Oracle® Communications

Cloud Native Core, Converged Policy User Guide



Release 26.1.201
G55574-01
August 2026

Oracle Communications Cloud Native Core, Converged Policy User Guide, Release 26.1.201

G55574-01

Copyright © 2019, 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

1 Introduction

1.1 Overview
1.2 References

2 CNC Policy Architecture

3 Policy Services

3.1 Audit Service
3.2 Access and Mobility Service
3.3 Authorization Service
3.4 Binding Service
3.5 Notifier Service
3.6 NWDAF Agent
3.7 PCRF Core Service
3.8 Policy Data Source (PDS) Service
3.9 Session Management Service
3.10 UE Policy Service
3.10.1 UE Policy Enhancements
3.11 Usage Monitoring Service

4 Policy Features

4.1 Security Context
4.2 Support for Handling DB Cluster Disconnect
4.3 Mutual Transport Layer Security
4.4 Diameter Gateway Connection Repaving
4.5 Optimizing Lookup in Binding Service Database
4.6 Support for QoS Monitoring
4.7 Optimize Database Lookup in SM Service
4.8 Support for SBI Message Priority Header
4.9 Disabling mTLS to Establish Communication between Policy and cnDBtier
4.10 Supports pcfIpEndPoints in pcfBinding- BSF Registration

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.11 Support for the 3gpp-Sbi-NF-Peer-Info Header
4.12 Support for DNN Replacement and Slice Support in AM Policy
4.13 Support for USER_LOCATION_CH Event Trigger
4.14 UE Policy Enhancements - Handling of AMF Updates with Change in AMF ID- Interaction with N1N2Commur and backoff
4.14.1 UE Policy Enhancements - Handling of AMF Updates with Change in AMF ID- Interaction with N1N2Co Retry and backoff, with retry-after Timer
4.15 Expiry Handling for Policy Data Subscriptions
4.16 Application Framework Change
4.17 Support to Display the Text Names of URSP and UPSI Rules in Logs
4.18 Support for Sponsored Data Connectivity When AF/NEF Provides the Support Over Policy Authorization Serv
4.19 Optimizing N7 Session Lookup for AAR messages in Rx Call flows
4.20 Conflict Resolution for URSP Rules N1N2 transfer to UE
4.21 Support for Immediate Report Handling for SM-Data, AM-Data, and UE-Policy-Set on N36 Interface
4.22 Support for Optimized POD Management Using maxSurge and maxUnavailable During Policy Upgrade
4.23 Optimizing PolicyDS Database Query With Configurable UE IDs
4.24 Support for Monitoring Migration Status of Database Records
4.25 Support for Signaling and DB Access Processing Latency Histogram Metrics
4.26 Support for NR vs EUTRA KPIs for N7 Interface
4.27 Support of Traffic Detection on SMF-N7 and TDF using Sd Interface
4.28 Handling Collision Between AAR and STR Messages During Update Notify Timeout
4.29 Supports Reattempt after Back-off during N1N2 Communication
4.30 Pod Congestion Control in Policy Services
4.30.1 AM Service Pod Congestion Control
4.30.2 Notifier Service Pod Congestion Control
4.30.3 User Service Pod Congestion Control
4.30.4 Diameter Connector Pod Congestion Control
4.30.5 UE Service Pod Congestion Control
4.30.6 SM Service Pod Congestion Control
4.30.7 PDS Pod Congestion Control
4.30.8 Usage Monitoring Pod Congestion Control
4.30.9 PCRF Core Pod Congestion Control
4.30.10 Binding Service Pod Congestion Control
4.30.11 Bulwark Pod Congestion Control
4.30.12 Congestion Control Discard Message Response Code
4.31 Stale Binding Detection Audit, Report and Recover
4.32 Congestion Control Resource Usage Calculation Using EMA Algorithm
4.33 Message Feed for SBI Monitoring
4.34 Support for Dual Stack
4.35 Handling of Multiple N1N2Transfer Messages
4.36 PCF support to not send ASR while Notify-Update fails
4.37 LDAP Timeout and Retry Mechanism

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.38 Logging Support for Error Response
4.39 Support for Burst rate limit modification and customization for logs
4.40 Concurrency Handling at Bulwark Service to Reduce Processing Latency of Service
4.41 Support for Stale Requests Cleanup
4.42 Support for Diameter Message Response Time Latency Metrics
4.43 Support for TLS
4.43.1 Support for TLS Using HTTPs
4.43.2 Support for TLS in Diameter Gateway
4.43.3 TLS 1.3 Support for Kubernetes API Server
4.44 Traffic Segregation
4.45 Support for Optimizing Database Encoding in PCRF Core
4.46 Support for policyDecFailureReports Attribute
4.47 Enhancements to Error Response
4.48 OAuth Access Token Based Authorization
4.49 Support for End-to-End Log Identifier Across Policy Services
4.50 Support for Automated Certificate Lifecycle Management
4.51 Support for Handling Requests From Reduced Capability Devices
4.52 PCF Support for ME-XX String in Server Header from CHF
4.53 Sy SLR Enhancements for Signaling Updates and UDR Notification
4.53.1 Handling N28 and N36 Interfaces Context Information during Subscription Failures
4.54 Enhancement to PRE Metrics
4.55 Enhancement to PCF Resiliency
4.56 Support for cnDBTier APIs in CNC Console
4.57 Support for Non-SUPI based On-Demand Discovery Caching of NF Profiles
4.58 Handling Race Condition Between Gx and Sy Sessions in two sites
4.59 Support for Policy Action to Send the Notify Terminate
4.60 Support for UDR Discovery Using Group ID
4.61 Network Policies
4.62 Support for SUPI based NRF Discovery Optimization and Response Caching from UDR
4.63 RAA Error Code Handling
4.64 IPv6 Support in Converged Policy Mode
4.65 Handling Rx Stale Sessions
4.66 Data Compression
4.67 Usage Monitoring on Gx Interface
4.67.1 Migrating Subscribers from OCPM to PCRF Deployment
4.67.2 Performance Considerations while Running Quota Management
4.68 Support for Autoenrollment of Subscribers
4.69 Support for Subscriber Notification Using SMPP
4.70 Support for Query on Update and Subscription to UDR
4.71 Support for Presence Reporting Area
4.72 Handling Install and Remove Conflict for Same Rule
4.73 Diameter Session Retry

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.74 Monitoring the Availability of SCP using HTTP2 OPTIONS
4.75 Supports 3gpp-Sbi-Correlation-Info Header
4.76 HTTP Error Codes
4.77 Diameter Error Codes
4.78 Configurations for Pre and Post Upgrade/Install Validations
4.79 Support Multiple Cluster Deployment at CNC Console
4.80 NetLoc Support
4.80.1 NetLoc Support in PCF
4.80.2 NetLoc Support in PCRF
4.81 Subscription to Notification Support for Signaling Path Status
4.82 Support for SessionRuleErrorHandling
4.83 3GPP-User-Location-Info AVP in Rx RAR
4.83.1 Support for Encoding of NCGI in 3GPP-User-Location-Info
4.84 Support for Server Header
4.85 SBI Timer Handling
4.86 Detection and Handling of Late Arrival Requests
4.86.1 PCF Support for Detection and Handling of Late Arrival Requests in BSF
4.87 Support for Session Retry and Alternate Route Service
4.88 Support for Honor retry-after Header in Egress Gateway
4.89 Stale Session Handling
4.90 Support for 3GPP NF Sets and Binding Headers
4.91 Georedundancy Support
4.92 Diameter Pod Congestion Control
4.93 Overload Control
4.93.1 Overload Control- Diameter
4.93.2 Overload Control- SBI
4.93.3 Enhancement to Overload Control Handling in SM Service
4.94 Load Shedding through Admission Control in PCRF-Core
4.95 Rate Limiting
4.96 Topology Hiding for Diameter Gateway
4.97 Two-phase Deployment of Policies
4.98 Binding Mechanism Support (Nbsf)
4.99 LDAP Support
4.100 SOAP Support
4.101 Support for Timer Configurations
4.102 Custom AVP to Support Third-Party Vendor Specific AVPs
4.103 Adding Subscription-ID AVPs to STR messages
4.104 Asynchronized Access to nCHF
4.105 Nudr to Support OperatorSpecificData
4.106 Support for Spending Limit Pending Counter
4.107 XFCC Header Validation
4.108 Policy Event Records

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.109 URSP Policy Support
4.110 AF Integration over Rx
4.111 IMS Emergency Session Support
4.112 IMS Restoration
4.113 Automated Test Suite Support
4.114 Notification Handling from PDS for PCRF-Core
4.115 Service mesh for intra-NF Communication
4.116 Turning off AccessToken signature Validation
4.117 Pending Transactions on N7 and N15 Interface
4.118 Pending Transactions on Gx Interface
4.119 NRF Client Retry and Health Check
4.120 Support for PCF Status on NRF on CNC Console
4.121 Support for Stale Binding Detection in BSF
4.122 Pod Protection at Ingress Gateway Using Rate Limiting
4.123 Support for Concurrency Handling using Bulwark Service in Policy
4.123.1 Support for Concurrency Handling using Bulwark Service in SM
4.123.2 Support for Concurrency Handling using Bulwark Service in AM
4.123.3 Support for Concurrency Handling using Bulwark Service in UE
4.123.4 Support for Concurrency Handling using Bulwark Service in PCRF
4.123.5 Support for Concurrency Handling using Bulwark Service in PDS
4.124 Support for Sd Interface in PCRF
4.125 Support for Retrying Binding Registration on BSF and generating Alarm to Operator
4.126 Controlled Shutdown of an Instance
4.127 Enhancement to use Cached NRF Discovery Responses
4.128 Limiting the Number of Sessions
4.129 Handling Stale Data in PDS
4.130 Support for User-Agent Header
4.131 Support for Spending Limit Status Reporting
4.132 NF Scoring for a Site
4.133 Consistent UDR Updates Using ETag
4.134 Support for Resource Allocation for PCC Rules
4.135 Subscriber State Variables in Policy
4.135.1 Local Subscriber State Variable
4.135.2 Remote Subscriber State Variable
4.135.3 Support to Write Remote Subscriber State Variables to Operator Specific Data (OSD)
4.136 AMF Selection for Namf-comm Subscription
4.137 Support for MCPTT Features
4.138 Support for Listing and Comparing UPSIs Received from UDR
4.139 Roaming Support in Policy
4.140 Wi-Fi Support using RAT-Type AVPs
4.141 Support for Database Slicing

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.142 Support for Interworking Between Evolved Packet Core (EPC) and CNC

5 Integrating Policy with Different Network Functions

6 Configuring Policy

7 Configuring Policy Using CNC Console

7.1 General Configurations
7.1.1 General Settings
7.1.2 Logging Configuration
7.1.2.1 Logging Level
7.1.2.2 Subscriber Activity Logging
7.1.3 SBI Ingress Error Code Profiles Collection
7.1.4 Policy Mated Region
7.1.5 Site Fallback
7.2 Error Handling
7.2.1 Error Configurations
7.3 Service Configurations
7.3.1 Common Data
7.3.1.1 Reattempts Profile
7.3.1.2 Retry Profiles
7.3.1.3 Timer Profiles
7.3.1.4 Site Takeover
7.3.1.5 NF Communication Profiles
7.3.1.6 Attribute Forwarding Profiles
7.3.1.7 Rx Reauth Profiles
7.3.1.8 Message Profiles
7.3.1.9 Message Attributes
7.3.1.10 Service Profiles
7.3.1.11 Default Processing Profiles
7.3.2 PCF Session Management
7.3.2.1 UDR Subscriber Delete Resource Support
7.3.3 PCF Access and Mobility
7.3.4 PCF UE Policy Service
7.3.5 PCF Policy Authorization
7.3.6 PCF User Connector
7.3.7 Timer Service
7.3.8 Configuring Usage Monitoring
7.3.9 PCRF Core Service Configurations

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.9.1 Settings
7.3.9.2 Serving Gateway
7.3.9.3 Network Element
7.3.10 Audit Service
7.3.11 Configuring Notifier Service
7.3.11.1 Notifier Configurations
7.3.11.2 Notification Server
7.3.12 PDS
7.3.12.1 PDS Settings
7.3.12.2 PDS Workflow
7.3.12.3 PDS UE ID Configuration
7.3.13 Binding Service
7.3.14 Policy Engine
7.3.15 Configuring NWDAF Agent
7.3.15.1 Settings
7.3.15.2 Slice Load Level
7.3.16 NRF Agent
7.3.17 IGW
7.3.18 Bulwark
7.3.18.1 Bulwark Settings
7.3.19 Diameter Connector
7.4 Policy Data Configurations
7.4.1 Common
7.4.1.1 Policy Table
7.4.1.2 Dropdown Blocks
7.4.1.3 PCF Presence Reporting Area
7.4.1.4 Policy Counter Id
7.4.1.5 Match Lists
7.4.1.6 Schemas
7.4.2 PCF Session Management
7.4.2.1 Session Rule
7.4.2.2 Session Rule Profile
7.4.2.3 QoS Information
7.4.2.4 PCC Rule
7.4.2.5 PCC Rule Profile
7.4.2.6 QoS Data
7.4.2.7 Traffic Profile
7.4.2.8 Charging Data
7.4.2.9 Traffic Control Data
7.4.2.10 Condition Data
7.4.3 PCF Access and Mobility
7.4.3.1 Service Area Restriction

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.4.4 PCF UE Policy
7.4.4.1 URSP Rule
7.4.4.2 UPSI
7.4.5 PCRF Core
7.4.5.1 Charging Server
7.4.5.2 Media Profile
7.4.5.3 Presence Reporting Area
7.4.5.4 Time Periods
7.4.5.5 Retry Profile
7.4.5.6 Traffic Profile
7.4.6 Usage Monitoring
7.4.6.1 Data Limit Profiles
7.4.6.2 Data Limit Selection Profiles
7.4.6.3 Data Limit Sorting Profiles
7.4.6.4 Data Rollover Profiles
7.5 Policy Management
7.5.1 Policy Projects
7.6 Diameter Configurations
7.6.1 Settings
7.6.2 Peer Nodes
7.6.3 Routing Table
7.6.4 Peer Node Sets
7.6.5 Diameter Error Configurations
7.6.6 Diameter Repaving
7.7 Data Source Configurations
7.7.1 Data Sources
7.8 Administration
7.8.1 Export & Import
7.8.1.1 Exporting Policy Data
7.8.1.2 Importing Policy Data
7.8.1.3 Using REST API for Policy Export & Import
7.9 Status and Query
7.9.1 Session Viewer
7.9.2 NF Data
7.9.2.1 PCF Registration Profile
7.9.2.2 NRF Status
7.9.2.3 Discovered NF Instances
7.9.3 Custom Query
7.10 Overload and Congestion Control Configurations
7.10.1 Diameter
7.10.1.1 Load Shedding Profiles
7.10.1.2 Message Priority Profiles

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.10.2 SBI
7.10.2.1 Overload Control
7.10.2.2 Route Level Mapping
7.10.2.3 Failure Count
7.10.3 Congestion Control
7.10.3.1 Settings
7.10.3.2 Thresholds
7.10.3.3 Load Shedding Rules
7.10.4 Overload Control Threshold
7.10.5 Advance Overload Control
7.10.5.1 Overload Configurations
7.11 Controlled Shutdown Configurations
7.11.1 Operational State
7.11.2 Diameter Error Mapping
7.11.3 SBI Ingress Error Mapping
7.12 NF Scoring Configurations
7.13 Viewing cnDBTier APIs in CNC Console
7.13.1 Backup List
7.13.2 Database Statistics Report
7.13.3 Georeplication Status
7.13.4 Georeplication Status Across All Sites
7.13.5 cnDBTier Health
7.13.6 Heartbeat Status
7.13.7 IP Family Reference
7.13.8 Georeplication Recovery
7.13.9 Local Cluster Status
7.13.10 On Demand Backup
7.13.11 Version
7.13.12 PCF Cluster DB State
7.13.13 Gracefully Stop and Start Georeplication

8 Alerts

8.1 List of Alerts
8.1.1 Common Alerts
8.1.1.1 POD_CONGESTION_L1
8.1.1.2 POD_CONGESTION_L2
8.1.1.3 POD_PENDING_REQUEST_CONGESTION_L1
8.1.1.4 POD_PENDING_REQUEST_CONGESTION_L2
8.1.1.5 POD_CPU_CONGESTION_L1
8.1.1.6 POD_CPU_CONGESTION_L2
8.1.1.7 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.8 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.9 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.10 ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.11 ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.12 ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.13 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.14 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.15 ASA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.16 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT
8.1.1.17 SCP_PEER_UNAVAILABLE
8.1.1.18 SCP_PEER_SET_UNAVAILABLE
8.1.1.19 POLICY_SERVICES_DOWN
8.1.1.20 DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD
8.1.1.21 DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT
8.1.1.22 DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT
8.1.1.23 UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD
8.1.1.24 UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT
8.1.1.25 POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD
8.1.1.26 POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT
8.1.1.27 POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT
8.1.1.28 UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD
8.1.1.29 DB_TIER_DOWN_ALERT
8.1.1.30 CPU_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD
8.1.1.31 CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD
8.1.1.32 CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD
8.1.1.33 MEMORY_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD
8.1.1.34 MEMORY_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD
8.1.1.35 MEMORY_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD
8.1.1.36 POD_CONGESTED
8.1.1.37 POD_DANGER_OF_CONGESTION
8.1.1.38 POD_PENDING_REQUEST_CONGESTED
8.1.1.39 POD_PENDING_REQUEST_DANGER_OF_CONGESTION
8.1.1.40 POD_CPU_CONGESTED
8.1.1.41 POD_CPU_DANGER_OF_CONGESTION
8.1.1.42 SERVICE_OVERLOADED
8.1.1.43 SERVICE_RESOURCE_OVERLOADED
8.1.1.44 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.45 SYSTEM_IMPAIRMENT_MAJOR
8.1.1.46 SYSTEM_IMPAIRMENT_CRITICAL
8.1.1.47 SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN
8.1.1.48 SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN
8.1.1.49 TDF_CONNECTION_DOWN

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.50 DIAM_CONN_PEER_DOWN
8.1.1.51 DIAM_CONN_NETWORK_DOWN
8.1.1.52 DIAM_CONN_BACKEND_DOWN
8.1.1.53 PERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED
8.1.1.54 SLA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.55 SLA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.56 SLA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.57 STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.58 STA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.59 STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.60 STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.61 STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.62 STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.63 SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.64 SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.65 SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.66 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR
8.1.1.67 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR
8.1.1.68 DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL
8.1.1.69 DGW_TLS_CONNECTION_FAILURE
8.1.1.70 POLICY_CONNECTION_FAILURE
8.1.1.71 AUDIT_NOT_RUNNING
8.1.1.72 DIAMETER_POD_ERROR_RESPONSE_MINOR
8.1.1.73 DIAMETER_POD_ERROR_RESPONSE_MAJOR
8.1.1.74 DIAMETER_POD_ERROR_RESPONSE_CRITICAL
8.1.1.75 CERTIFICATE_EXPIRY_MINOR
8.1.1.76 CERTIFICATE_EXPIRY_MAJOR
8.1.1.77 CERTIFICATE_EXPIRY_CRITICAL
8.1.1.78 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MINOR
8.1.1.79 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MAJOR
8.1.1.80 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_CRITICAL
8.1.1.81 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MINOR
8.1.1.82 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MAJOR
8.1.1.83 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_CRITICAL
8.1.1.84 STALE_BINDING_REQUEST_REJECTION_CRITICAL
8.1.1.85 STALE_BINDING_REQUEST_REJECTION_MAJOR
8.1.1.86 STALE_BINDING_REQUEST_REJECTION_MINOR
8.1.1.87 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MINOR
8.1.1.88 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MAJOR
8.1.1.89 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_CRITICAL
8.1.1.90 POLICYDS_EXPIRED_SUBSCRIPTION
8.1.1.91 LDAP_PEER_CONNECTION_LOST

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.92 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_MINOR
8.1.1.93 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_MAJOR
8.1.1.94 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_CRITICAL
8.1.1.95 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD
8.1.1.96 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD
8.1.1.97 RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.1.98 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.1.99 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.1.100 PCF_STATE_NON_FUNCTIONAL_CRITICAL
8.1.1.101 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST_EGW
8.1.1.102 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR
8.1.1.103 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR
8.1.1.104 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL
8.1.1.105 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
8.1.1.106 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
8.1.1.107 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL
8.1.1.108 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MINOR_PERCENT
8.1.1.109 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MAJOR_PERCENT
8.1.1.110 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_CRITICAL_PERCENT
8.1.1.111 QOS_MON_MISSING_ATTRIBUTES_ABOVE_CRITICAL_PERCENT
8.1.1.112 QOS_MON_MISSING_ATTRIBUTES_ABOVE_MAJOR_PERCENT
8.1.1.113 QOS_MON_MISSING_ATTRIBUTES_ABOVE_MINOR_PERCENT
8.1.1.114 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT
8.1.1.115 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MAJOR_PERCENT
8.1.1.116 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MINOR_PERCENT
8.1.1.117 QOS_MON_FAILED_AUTH_ABOVE_CRITICAL_PERCENT
8.1.1.118 QOS_MON_FAILED_AUTH_ABOVE_MAJOR_PERCENT
8.1.1.119 QOS_MON_FAILED_AUTH_ABOVE_MINOR_PERCENT
8.1.2 PCF Alerts
8.1.2.1 EGRESS_GATEWAY_DNS_RESOLUTION_FAILURE
8.1.2.2 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR
8.1.2.3 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR
8.1.2.4 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL
8.1.2.5 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
8.1.2.6 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
8.1.2.7 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL
8.1.2.8 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MINOR
8.1.2.9 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MAJOR
8.1.2.10 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL
8.1.2.11 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_CRITICAL_THRESHOLD
8.1.2.12 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MAJOR_THRESHOLD
8.1.2.13 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.14 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_CRITICAL_THRESHO
8.1.2.15 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MAJOR_THRESHOLD
8.1.2.16 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MINOR_THRESHOLD
8.1.2.17 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT
8.1.2.18 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT
8.1.2.19 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT
8.1.2.20 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MINOR
8.1.2.21 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR
8.1.2.22 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_CRITICAL
8.1.2.23 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MINOR
8.1.2.24 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MAJOR
8.1.2.25 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_CRITICAL
8.1.2.26 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_M
8.1.2.27 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_M
8.1.2.28 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_C
8.1.2.29 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD
8.1.2.30 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD
8.1.2.31 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD
8.1.2.32 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD
8.1.2.33 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD
8.1.2.34 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD
8.1.2.35 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD
8.1.2.36 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD
8.1.2.37 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD
8.1.2.38 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
8.1.2.39 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
8.1.2.40 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
8.1.2.41 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
8.1.2.42 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
8.1.2.43 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
8.1.2.44 SM_STALE_REQUEST_PROCESSING_REJECT_MINOR
8.1.2.45 SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR
8.1.2.46 SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL
8.1.2.47 UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR
8.1.2.48 UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL
8.1.2.49 UE_STALE_REQUEST_PROCESSING_REJECT_MINOR
8.1.2.50 UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR
8.1.2.51 UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR
8.1.2.52 UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL
8.1.2.53 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL
8.1.2.54 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_T
8.1.2.55 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_T

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.56 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
8.1.2.57 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
8.1.2.58 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
8.1.2.59 INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD
8.1.2.60 SM_TRAFFIC_RATE_ABOVE_THRESHOLD
8.1.2.61 SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT
8.1.2.62 SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT
8.1.2.63 PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD
8.1.2.64 PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT
8.1.2.65 PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD
8.1.2.66 PCF_PENDING_BINDING_SITE_TAKEOVER
8.1.2.67 PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED
8.1.2.68 PCF_PENDING_BINDING_RECORDS_COUNT
8.1.2.69 AUTONOMOUS_SUBSCRIPTION_FAILURE
8.1.2.70 AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT
8.1.2.71 AM_AR_ERROR_RATE_ABOVE_1_PERCENT
8.1.2.72 UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT
8.1.2.73 UE_AR_FAILURE_RATE_ABOVE_1_PERCENT
8.1.2.74 SMSC_CONNECTION_DOWN
8.1.2.75 LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD
8.1.2.76 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD
8.1.2.77 LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD
8.1.2.78 SM_UPDATE_NOTIFY_FAILED_ABOVE_50_PERCENT
8.1.2.79 SM_UPDATE_NOTIFY_FAILED_ABOVE_60_PERCENT
8.1.2.80 SM_UPDATE_NOTIFY_FAILED_ABOVE_70_PERCENT
8.1.2.81 UPDATE_NOTIFY_FAILURE_ABOVE_30_PERCENT
8.1.2.82 UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT
8.1.2.83 UPDATE_NOTIFY_FAILURE_ABOVE_70_PERCENT
8.1.2.84 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST
8.1.2.85 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD
8.1.2.86 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD
8.1.2.87 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD
8.1.2.88 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD
8.1.2.89 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD
8.1.2.90 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD
8.1.2.91 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD
8.1.2.92 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD
8.1.2.93 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD
8.1.2.94 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL
8.1.2.95 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_T
8.1.2.96 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_T
8.1.2.97 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHO

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.98 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD
8.1.2.99 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD
8.1.2.100 PCF_STATE_NON_FUNCTIONAL_CRITICAL
8.1.2.101 UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT
8.1.2.102 UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT
8.1.2.103 UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT
8.1.2.104 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT
8.1.2.105 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT
8.1.2.106 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT
8.1.2.107 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR
8.1.2.108 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR
8.1.2.109 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL
8.1.2.110 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
8.1.2.111 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
8.1.2.112 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL
8.1.2.113 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR
8.1.2.114 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR
8.1.2.115 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL
8.1.2.116 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
8.1.2.117 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
8.1.2.118 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL
8.1.2.119 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERC
8.1.2.120 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCE
8.1.2.121 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCE
8.1.2.122 AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT
8.1.2.123 AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT
8.1.2.124 AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT
8.1.2.125 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD
8.1.2.126 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD
8.1.2.127 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD
8.1.2.128 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MINOR_THRESHO
8.1.2.129 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MAJOR_THRESHO
8.1.2.130 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_CRITICAL_THRESH
8.1.2.131 IGW_POD_PROTECTION_CONGESTED_STATE
8.1.2.132 IGW_POD_PROTECTION_DOC_STATE
8.1.2.133 EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
8.1.2.134 INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
8.1.3 PCRF Alerts
8.1.3.1 PRE_UNREACHABLE_EXCEEDS_CRITICAL_THRESHOLD
8.1.3.2 PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD
8.1.3.3 PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD
8.1.3.4 PCRF_DOWN

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.5 CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.3.6 CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.3.7 CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.3.8 AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.3.9 AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.3.10 AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.3.11 RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.3.12 RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.3.13 RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.3.14 ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.3.15 ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.3.16 ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.3.17 ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.3.18 ASA_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.3.19 ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.3.20 RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD
8.1.3.21 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD
8.1.3.22 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD
8.1.3.23 RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT
8.1.3.24 RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT
8.1.3.25 RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT
8.1.3.26 Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT
8.1.3.27 Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT
8.1.3.28 Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT
8.1.3.29 Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT
8.1.3.30 Gx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT
8.1.3.31 Gx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT
8.1.3.32 STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL
8.1.3.33 STALE_DIAMETER_REQUEST_CLEANUP_MAJOR
8.1.3.34 STALE_DIAMETER_REQUEST_CLEANUP_MINOR

9 CNC Policy Metrics

9.1 TLS Metrics
9.2 Egress Gateway Metrics for SCP
9.3 Correlation-Info Header Metrics
9.4 Config Server Metrics
9.5 SM Service Metrics
9.6 AM Service Metrics
9.7 CM Service Metrics
9.8 PA Service Metrics
9.9 UE Service Metrics

Copyright © 2019, 2026, Oracle and/or its affiliates.

9.10 User Service Metrics
9.11 Diameter Connector Service Metrics
9.12 Diameter Gateway Metrics
9.13 Policy DS Metrics
9.14 LDAP Gateway
9.15 Binding Service Metrics
9.16 Audit Service Metrics
9.17 Query Service Metrics
9.18 AppInfo Metrics
9.19 PerfInfo Metrics
9.20 Pod Congestion Metrics
9.21 PCRF Core Metrics
9.22 Late Arrival Requests and Collision Detection Metrics
9.23 Notifier Metrics
9.24 Usage Monitoring Metrics
9.25 Bulwark Metrics
9.26 CHF Metrics
9.27 UDR Metrics
9.28 User-Agent Header Metrics
9.29 NWDAF Agent Metrics
9.30 PRE Metrics
9.31 NRF Client Metrics
9.32 Error Mapping Metrics
9.33 Metrics for Automated Certificate Lifecycle Management
9.34 Common Metrics
9.35 ASM Metrics
9.36 Sbi-NF-Peer-Info Header Metrics

10 CNC Policy KPIs

10.1 PCRF KPIs

A Ingress Gateway Metrics

B Egress Gateway Metrics

C HTTP Error Codes Supported by Policy

Copyright © 2019, 2026, Oracle and/or its affiliates.

D Error Code Dictionary

Copyright © 2019, 2026, Oracle and/or its affiliates.

Preface

- Documentation Accessibility
- Diversity and Inclusion

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which user supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that user enter.

Copyright © 2019, 2026, Oracle and/or its affiliates.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown in the following list on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Acronyms

The following table lists the acronyms and the terminologies used in the document:

Table Acronyms

Acronym	Description
3GPP	3rd Generation Partnership Project
AAA	Authorization Authentication Answer
AAR	Authorization Authentication Request
AF	Application Function
AMF	Access and Mobility Management Function
API	Application Programming Interface
ARS	Alternate Route Selection
ASM	Aspen Service Mesh
ASR	Abort-Session-Request
ATS	The core service sends the subscriber state variables to PDS only when there is an update to the variables.
AVP	Attribute Value Pair
BSF	Oracle Communications Cloud Native Core, Binding Support Function
CA	Certificate Authority
CDCS	Oracle Communications CD Control Server
CHF	Charging Function
CM	Configuration Management
CNC	Cloud Native Core
CNC Console	Oracle Communications Cloud Native Configuration Console
CNE	Oracle Communication Cloud Native Core, Cloud Native Environment
CNLB	Cloud Native Load Balancer
CNPCRF	Oracle Communications Cloud Native Core, Policy and Charging Rules Function
CUSTOMER_REPO	Docker registry address including the port number, if the docker registry has an associated port.
cnDBTier	Oracle Communications Cloud Native Core, cnDBTier
DNS	Domain Name System
DRA	Diameter Routing Agent
FQDN	Fully Qualified Domain Name
GUAMI	Globally Unique AMF Identifier
IMAGE_TAG	Image tag from release tar file. You can use any tag number. However, make sure that you use that specific tag number while pushing docker image to the docker registry.
IMS	IP Multimedia Subsystem
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol.
MCC	Mobile Country Code
MCPTT	Mission-critical push-to-talk
METALLB_ADDRESS_POOL	Address pool configured on metallb to provide external IPs

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table (Cont.) Acronyms

Acronym	Description
MNC	Mobile Network Code
NAD	Network Attachment Definitions
NEF	Oracle Communications Cloud Native Core, Network Exposure Function
NF	Network Function
NPLI	Network Provided Location Information
NRF	Oracle Communications Cloud Native Core, Network Repository Function
OSO	Oracle Communications Operations Services Overlay
P-CSCF	Proxy Call Session Control Function
PA Service	Policy Authorization Service
PCC	Policy and Charging Control
PDB	Pod Disruption Budget
PLMN	Public Land Mobile Network
PCF	Oracle Communications Cloud Native Core, Policy Control Function
PCRF	Oracle Communications Cloud Native Core, Policy and Charging Rules Function
PCEF	Policy and Charging Enforcement Function
PCSCF	Proxy Call Session Control Function
PDS	Policy Data Service
PRA	Presence Reporting Area
PRE	Policy Runtime Engine
PDU	Protocol Data Unit
Policy	Oracle Communications Cloud Native Core, Converged Policy
QoS	Quality of Service
RAA	Re-Auth-Answer
RAN	Radio Access Network
RAR	Re-Auth-Request
RedCap devices	Reduced Capability devices (Examples: Wearables, Wireless sensors, and Surveillance equipment)
SBI	Service Based Interface
SAN	Subject Alternate Name
SCP	Oracle Communications Cloud Native Core, Service Communication Proxy
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
UDR	Oracle Communications Cloud Native Core, Unified Data Repository
SRA	Successful Resource Allocation
STR	Session Termination Request
TTL	Time To Live
UE	User Equipment
UPF	User Plane Function
UPSI	UE Policy Section Identifier
URSP	UE Route Selection Policies
UPSC	UE Policy Section Code

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table (Cont.) Acronyms

Acronym	Description
URI	Uniform Resource Identifier
VoLTE	Voice over Long-Term Evolution
VoNR	Voice over New Radio
VSA	Vendor Specific Attributes

Copyright © 2019, 2026, Oracle and/or its affiliates.

What's New in This Guide

This section introduces the documentation updates for release 26.1.2xx.

Release 26.1.201 - G55574-01, August 2026

- **Feature Updates:**
  - **New Features:**
    - **Diameter Gateway Connection Repaving**
      - Added Diameter Gateway Connection Repaving to describe the Diameter Gateway Connection Repaving feature that provides a controlled mechanism to re-balance Diameter connections across the cluster without restarting services or causing a complete outage.
      - Added Diameter Repaving to describe Diameter Gateway connection repaving configuration.
      - Added the following advanced settings keys to Settings:
        - DGW_CONNECTION_REPAVING.MAX_STAGGER_JITTER_MS
        - DGW_CONNECTION_REPAVING.REINVOCATION_DELAY_MIN
        - DGW_CONNECTION_REPAVING.CONNECTION_DISCONNECT_INTERVAL_MS
        - DGW_CONNECTION_REPAVING.DPR_DELAY_MS
        - DGW_CONNECTION_REPAVING.DPR_DISCONNECT_CAUSE
      - Added `diam_repaving_disconnections_total` metric to Diameter Gateway Metrics that counts the total number of connections terminated by the "force disconnect" mechanism.
    - **Support for QoS Monitoring**
      - Added Support for QoS Monitoring to describe how Policy supports AF subscription to QoS Monitoring and notifies provides report to the AF about packet delay between the UPF and RAN.
      - Updated description of **Override Supported Features** field in PCF Session Management to mention support for **QoSMonitoring**.
      - Added **QosMon Notification Target** to PCF Session Management, which is used to configure QoS Monitoring functionality in SM service.
      - Updated description of **Override Supported Features** field in PCF Policy Authorization to mention support for **QoSMonitoring** and **EnhancedSubscriptionToNotification**.
      - Added the following fields to PCF Policy Authorization, which are used to configure QoS Monitoring in PA service:
        - Accept Request on Missing QoS Monitoring Attributes
        - Accept Request on QoS Monitoring Not Supported/Not Negotiated
      - Added the following metrics to PA Service Metrics:
        - occnp_pa_qosmon_request_total
        - occnp_pa_qosmon_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Added the following metrics to SM Service Metrics:
  - occnp_sm_qosmon_update_notify_sent_total
  - occnp_sm_qosmon_decs_error_total
- Added the following alerts to PCF Alerts:
  - QOS_MON_FAILED_AUTH_ABOVE_MINOR_PERCENT
  - QOS_MON_FAILED_AUTH_ABOVE_MAJOR_PERCENT
  - QOS_MON_FAILED_AUTH_ABOVE_CRITICAL_PERCENT
  - QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MINOR_PERCENT
  - QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MAJOR_PERCENT
  - QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT
  - QOS_MON_MISSING_ATTRIBUTES_ABOVE_MINOR_PERCENT
  - QOS_MON_MISSING_ATTRIBUTES_ABOVE_MAJOR_PERCENT
  - QOS_MON_MISSING_ATTRIBUTES_ABOVE_CRITICAL_PERCENT

- **Support for 3GPP-SBI-Message-Priority Support**
  - Added Support for SBI Message Priority Header to describe how Policy supports assigning priority to messages using `3GPP-SBI-Message-Priority` header.
  - Updated the description of **Interface Type** and **Message Type** fields in Message Profiles.
  - Added **Message Priority Profile** to PCF Session Management.
  - Added **Message Priority Profile** for UDR Connector and CHF Connector in PCF User Connector.
  - Added **Message Priority Profile** to Binding Service.
  - Added the following metrics to Common Metrics:
    - occnp_http_message_priority_request_count_total
    - occnp_http_message_priority_response_count_total
- **Support for 3gpp-Sbi-NF-Peer-Info Header**
  - Added Support for the 3gpp-Sbi-NF-Peer-Info Header section, which enables network elements to obtain source and destination information for messages exchanged between a specified pair of NF (service) instances.
  - Added the following fields under `NF Peer Info Settings` in the NF Communication Profiles section:
    - `Send NF-Peer-Info Header`
    - `Include NF Service Instance ID`
  - Added the following metrics in the Sbi-NF-Peer-Info Header Metrics section:
    - `occnp_nf_peer_info_header_received_total`
    - `occnp_nf_peer_info_header_sent_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

    - Added `SAVE_SRC_SERV_INST` parameter in the advanced settings for the following sections:
        - PCF Session Management
        - Binding Service
        - PCF User Connector
    - Added `NF_PEER_INFO_FIND_OPTIMIZE_SRC` parameter to the advanced settings in the PDS Settings section.
- **Supports pcfIpEndPoints in pcfBinding- BSF Registration**
    - Added Supports pcfIpEndPoints in pcfBinding- BSF Registration section to enable SM Service to send the information present in the ipEndPoints of the NF Profile in its Binding Registration request.
    - Added the following fields in the PCF Session Management section:
        - `Service FQDN and IP Endpoints Configuration`
        - `NF Profile for Service FQDN and IP Endpoints`
    - Removed the following Advance Settings from the PCF Session Management section:
        - `BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS`
        - `BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS.SERVICE_NAME`
- **Optimize Database Lookup in SM Service**
    - Added Optimize Database Lookup in SM Service section, which improves PCF capacity per instance by reducing the storage footprint, database load, database replication, and latency in the SM Service.
    - Added `BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` parameter in the advanced settings in the PCF Session Management section.
    - Added `occnp_dependentContextBinding_processing_total` metrics in the Binding Service Metrics section.
- Added the Disabling mTLS to Establish Communication between Policy and cnDBtier section with information to disable mTLS to establish communication between Policy and cnDBtier.
- **Security Context**
    - Added Security Context section, which improves the security posture of deployed workloads Policy by applying Kubernetes pod and container security context settings.

– **Enhancements:**

- **Assume Positive Support for SM Service During Overload Condition**
    - Updated Enhancement to Overload Control Handling in SM Service section with description of Assume Positive support for handling Overload Control at SM Service.
    - Added Default Processing Profiles to describe creating and configuring Default Processing Profiles.
    - Added Service Profiles to describe creating and configuring service profiles.
    - Added **Default Processing** to PCF Session Management, which is used to configure Default Processing Profile for SM service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Added `MSG_PROCESSING_DEFAULTS.ENABLED_ON_PRE_FAILURE` advanced settings key to PCF Session Management, which is used to indicate if the default PCC rules and session rules configured using Default Processing Profile must be applied on Session creation in case of PRE failure.
- Added the following new fields to Overload Configurations:
  - Service Profile
  - Service Profile Apply Percentage
- Updated Overload Control Threshold to describe support for additional load levels up to L10 for configuring overload control for SM service and Diameter Connector service.
- Updated Discard Policy to describe support for additional load levels up to L10 for configuring overload control for SM service and Diameter Connector service.
- Updated Load Shedding Profiles to describe support for additional load levels up to L10 for configuring overload control for SM service and Diameter Connector service.
- Added the following metrics to SM Service Metrics:
  - occnp_enhanced_overload_service_interaction_total
  - occnp_enhanced_overload_ssv_update_skipped_total
- Added the following alerts to PCF Alerts:
  - SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED _MINOR
  - SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED _MAJOR
  - SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED _CRITICAL

- **Support to Write Remote Subscriber State Variables to Operator Specific Data (OSD)**
  - Added Support to Write Remote Subscriber State Variables to Operator Specific Data (OSD) section to write values received from Online Charging System (OCS) provided counters into Operator Specific Data (OSD) in the UDR using Remote State Variables.
  - Added `Operator Specific Data` field to enable the operator to specify the paths in OSD in PDS Settings section.
  - Added `ENABLE_OCS_ERROR_HANDLING` parameter in the advanced settings in the PDS Settings section.
- Updated the examples to add method dimension for the following metrics in the Policy DS Metrics section:
  - server_request_total
  - server_response_total
- Updated the examples for the following metrics in the UDR Metrics section:
  - ocpm_udr_tracking_request_total
  - ocpm_udr_tracking_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

* **Support for DNN Replacement and Slice Support in AM Policy - Multiple Slice and DNN, updates UDR and AMF**:
  * Updated Support for DNN Replacement and Slice Support in AM Policy section to describe support for multiple S-NSSAI and DNNs in `SmfSelectionData` to AMF for a UE and its respective AM Policy Association.
  * Added the following alerts to PCF Alerts:
    * DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MINOR_PERCENT
    * DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MAJOR_PERCENT
    * DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_CRITICAL_PERCENT
* **UE Policy Enhancements - Handling N1N2MessageTransferError Responses with "retryAfter"**
  * Updated UE Policy Enhancements - Handling of AMF Updates with Change in AMF ID- Interaction with N1N2Communication Session Retry and backoff.
  * Added **Enable Retry-After IE** to Retry Profiles section.
  * Added the following advanced settings key to PCF UE Policy Service:
    * CANCEL.ON.NEW.TRIGGER.ENABLED
    * CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.ENABLED
    * CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_LEASE_DURATION
    * CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_BACKOFF
    * CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_COUNT
    * CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_WAIT_DURATION
    * RETRY.AFTER.IE.MAX.SECONDS
    * RETRY.AFTER.IE.TIMER.CAPACITY
    * RETRY.AFTER.IE.TIMER.RATE
    * TIMER_EXP_RANGE_MIN_SEC
  * Added the following new metrics to UE Service Metrics:
    * occnp_ue_update_guami_change_during_retryafter_cancelled_total
    * occnp_ue_delete_during_retryafter_total
    * occnp_ue_http_in_request_during_retryafter_total
    * occnp_n1n2transfer_error_with_retryafter_seconds
    * occnp_n1n2transfer_error_retryafter_invalid_total
  * Added the following alerts to PCF Alerts:
    * UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD

Copyright © 2019, 2026, Oracle and/or its affiliates.

        - UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD
        - UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD
        - UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MINOR_THRESHOLD
        - UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MAJOR_THRESHOLD
        - UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_CRITICAL_THRESHOLD
    - **Support for cnDBTier APIs in CNC Console**
        - Updated the Support for cnDBTier APIs in CNC Console section with details of the APIs IP Family Reference and Gracefully Start and Stop Georeplication.
        - Added the APIs IP Family Reference and Gracefully Stop and Start Georeplication to the section Viewing cnDBTier APIs in CNC Console.
  - **Binding - Remove Index-Based Lookup**
    - Added Optimizing Lookup in Binding Service Database section to describe how Policy supports to optimize lookup in Binding service database by replacing index-based queries with primary-key searches and dedicated lookup tables.
    - Added the following fields to Binding Service, which are used to enable and configure query optimization:
        - Enable Indexing
        - Enable Query Optimization
        - Preferred Subscriber ID for Session Limit
    - Added the following metrics to Binding Service Metrics:
        - occnp_binding_index_restore_total
        - occnp_binding_index_total
  - **Enhanced logging (at WARN level) for microservices involved in PCRF & Diameter**: Updated Logging Support for Error Response with the details of enhanced logging support for microservices involved in SM call flows.
- **General Updates:**
  - Added HTTP Error Codes supported for Policy as a consumer of AMF - UE Policy in HTTP Error Codes Supported by Policy section.
  - Added the following procedure in the Diameter Pod Congestion Control section:
    - Load-Shedding Profile Storage and Validation
    - Unified Message Priority Profile Behavior
    - Conversion of Legacy Diameter Gateway Load Shedding Profiles
- Updated the default value of the following Advance Settings from 50ms to 200ms:
  - QUEUE_CONGESTION_RESOURCE_CALC_INTERVAL_MS
  - CPU_CONGESTION_RESOURCE_CALC_INTERVAL_MS
- Removed `USER.ocsSpendingLimit.resetContextOnGxCreate` parameter from PDS Settings section.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Added EGRESS_GATEWAY_DNS_RESOLUTION_FAILURE alert in the PCF Alerts section to detect DNS lookup failure.
- Added `SY.OptimizationType` advanced settings key in the **PCF Core Service Configurations** section. This key is used for optimization handling of reauthorization flows triggered by OCS notifications .
- Added GxSession table slicing configuration steps in the Support for Database Slicing section.
- Added `OPTIMISTIC_RETRY_BACKOFF_TIME_MS` and `DBEXCEPTION_RETRY_BACKOFF_TIME_MS` advanced settings keys, which are used to configure the initial backoff delay before retrying a DB operation, and removed `INTEGRITY_CONSTRAINT_RETRY_MAX_ATTEMPT` from PDS Settings as `OPTIMISTIC_RETRY_MAX_ATTEMPT` key is used to set the retry count for all concurrency related exception thrown from DB.
- Updated the Table D-7 and Table D-8 error code details in the Error Code Dictionary section.

Copyright © 2019, 2026, Oracle and/or its affiliates.

1 Introduction

This document provides information about the role of Oracle Communications Cloud Native Core, Converged Policy (Policy) in 5G Service Based Architecture and how to configure and use Policy services and managed objects.

1.1 Overview

Policy is a key component of the 5G Service Based Architecture(SBA). It provides a flexible, secure, and scalable policy designing solution. Policy interacts with other network functions to perform usage monitoring, network behavior management, and governance. It helps operators to design, test, and deploy different network policies supporting 5G deployments. Policy is designed and built with a microservice based architecture on cloud native principles. It uses network, subscriber, and service information to help service providers create policies and determine how and under what conditions subscribers and applications use network resources. It helps in minimizing network utilization while maximizing the quality of experience for operators. Policy solution supports deployments into any cloud, including containers on Bare Metal managed by Kubernetes or VMs managed by OpenStack.

> **Note**
>
> The performance and capacity of the Policy system may vary based on the Call model, Feature/Interface configuration, underlying CNE and hardware environment, including but not limited to the complexity of deployed policies, policy table size, object expression and custom JSON usage in Policy design.

Policy is a network function for policy control decision and flow based charging control. It consists of the following functions:

- Policy rules for application and service data flow detection, gating, QoS, and flow based charging to the Session Management Function (SMF)
- Access and Mobility Management related policies to the Access and Mobility Management Function (AMF)
- UE Route Selection Policies (URSP) rules to User Equipment (UE) through AMF
- Access to subscription information relevant for policy decisions in a Unified Data Repository (UDR)
- Network control for service data flow detection, gating, and Quality of Service (QoS)
- Flow based charging towards the Policy and Charging Enforcement Function (PCEF)
- Receiving session and media related information from Application Function (AF) and informing AF of traffic plane events
- Provision of Policy and Charging Control (PCC) Rules to Policy and Charging Enforcement Function (PCEF) through the Gx reference point

Policy supports the above functions through the following services:

- Session Management Service

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Access and Mobility Service
- Policy Authorization Service
- User Equipment (UE) Policy Service
- PCRF Core Service
- Binding Service
- Policy Data Source Service
- Usage Monitoring Service
- Notifier Service
- NWDAF Agent

1.2 References

You can refer to the following documents for more information.

- *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Document*
- *Oracle Communications Cloud Native Core, Converged Policy Design Guide*
- Visual Programming Editor: https://developers.google.com/blockly
- 3GPP Technical Specification 29.512 v15.3.0, Session Management Policy Control Service, Stage 3, Release 15
- 3GPP Technical Specification 29.514 v15.3.0, Policy Authorization Service, Stage 3, Release 15
- 3GPP Technical Specification 29.507 v15.3.0, Access and Mobility Policy Control Service, Stage 3, Release 15
- 3GPP Technical Specification 29.525 v15.5.1, UE Policy Control Service, Stage 3, Release 15
- 3GPP Technical Specification 29.518 v15.5.1, Access and Mobility Management Services, Stage 3, Release 15

Copyright © 2019, 2026, Oracle and/or its affiliates.

2
CNC Policy Architecture

Oracle Communications Cloud Native Core, Converged Policy (Policy) is developed as a cloud native application that is composed of a collection of microservices that run in a cloud native environment. It separates the processing or business logic into the logical grouping of microservices and components:

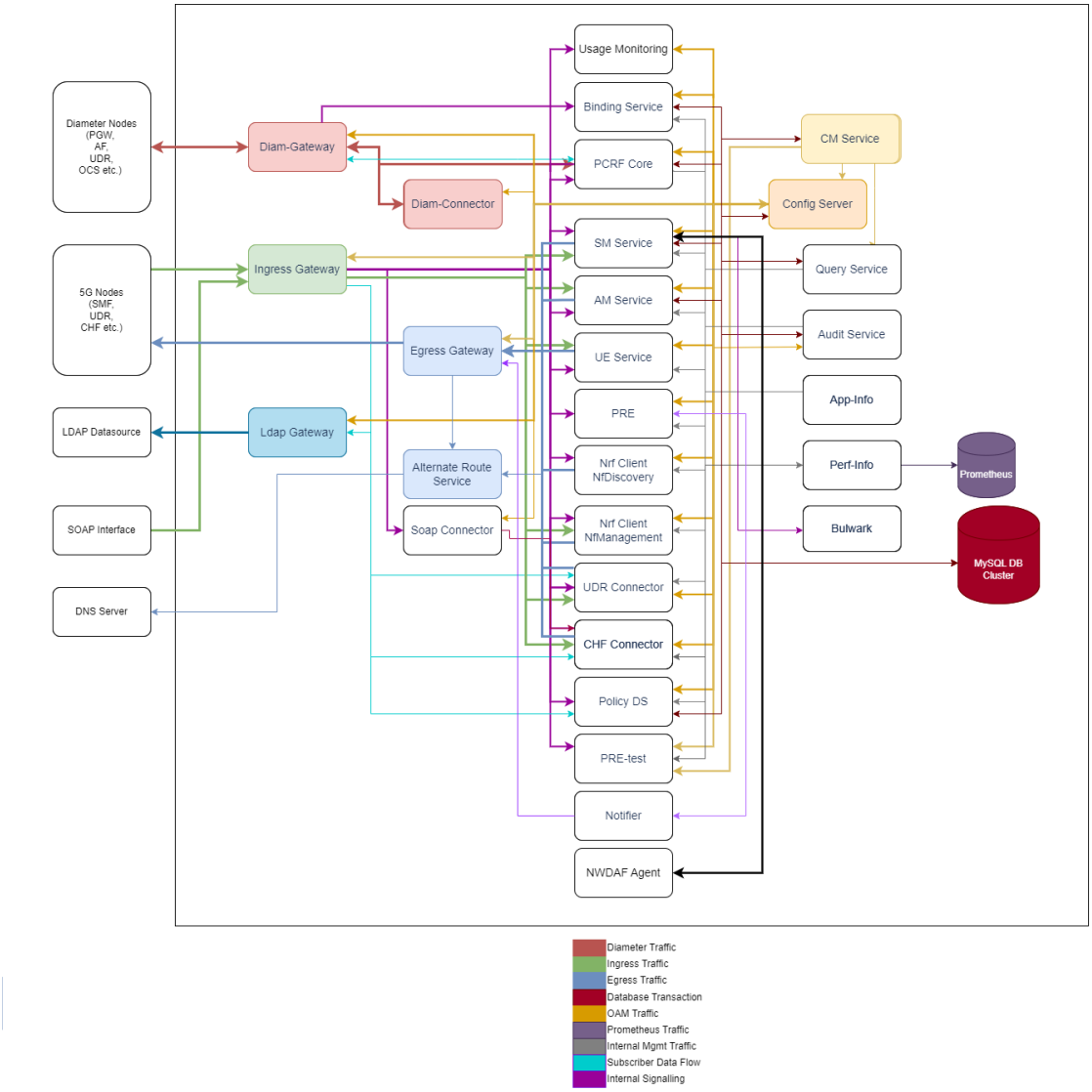
- **Connectivity**: Components interfacing with external entities. This is where an API gateway is utilized to interface with external traffic to the PCF. These are stateless sets of components.
- **Business logic**: Application layer running the PCRF or PCF business logic, policy engine, and various services that can be enabled based on deployment requirements. These are stateless sets of components.
- **Data Management**: Data layer responsible for storing various types of persistent data. PCF is developed to be able to plug in different types of back-end data layers that could be internal or external.

The Policy solution provides a flexible and modular policy designing framework. It offers, rapid and secure deployment of new policies and supports the existing use cases. The Converged policy solution supports both 4G and 5G networks, thereby helping operators to manage their heterogeneous network in an intuitive and consistent manner while enabling seamless inter-working and migration between 4G and 5G networks.

The following diagram represents the Policy architecture:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 2-1 Policy Architecture Diagram



Components of the Policy Architecture

- Kubernetes cluster hosting Docker containers and Calico networking
- Optional CNE services to support operation of PCF
- Connectivity
  - **Diameter Gateway/Connector** – Enables the policy solution functions as a Diameter server and offers integration over Gx, Rx, Sy and other legacy Diameter services. The Diameter server also implements routing, load balancing and overload control services. The Diameter Gateway acts as a gateway for all Diameter traffic to Policy Solution. It also performs round-robin load balancing across its back-end peers (Diameter connector and PCRF-Core).

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> For the Diameter Gateway, minimum and maximum replica settings cannot be configured because it is stateful. For StatefulSets (STS), only the total number of replicas can be set.

  - **Ingress Gateway** – Acts as a Gateway for all ingress HTTP traffic to Policy Solution.
  - **Egress Gateway** – Acts as a gateway for all egress HTTP traffic originating from Policy Solution to outside the network.
  - **LDAP Gateway** – Acts as a gateway for all egress LDAP traffic towards Directory Services.
  - **Diameter Connector** – Accepts Diameter messages from Diameter Gateway and converts the message to HTTP message format and sends to PCF components.
  - **Soap Connector** – Accepts the SOAP messages from ingress gateway, converts to JSON format and forwards the message to Policy Data Service for processing.
  - **NRF Client Service** – Integrates with NRF for service registration, discovery, and service status or load related information, along with application and performance information services. NRF discovery helps in on-demand discovery of network functions. NRF management helps in autonomous discovery of network functions.
- Policy Business Logic
  - **SM Service (includes PA Service)** - Provides the SMF session and application or flow based policies. The Policy Authorization (PA) service, such as Rx like interface in SBA authorizes an AF request and creates policies as requested by the NF consumer service for the PDU session to which the AF session is bound. This service implements policy control for session management for service data flows. This service implements the N7 interface to trigger session management policies towards the SMF function.
  - **AM Service** - Implements access management service-related policies over the N15 interface towards the AMF.
  - **PCRF Core Service** – Implements the legacy handling of PCRF core business logic, interactions with other microservices, and triggers for policy enforcement over the Gx interface. PCRF is a node that determines policy rules in a multimedia network in real-time.
  - **Binding Service** - Stores binding information related to 4G/5G subscribers and helps Diameter Gateway in forwarding AF messages.
  - **UE Policy Service** - Provides UE policy, includes UE Route Selection Policy (URSP) through AMF transparently to the UE. Implements UE management service-related policies over the N15 interface towards the AMF.
  - **UDR Connector** – UDR Connector layer interfaces the application with the UDR.
  - **CHF Connector** – CHF Connector layer interfaces with the CHF.
  - **Policy Data Service**– Policy DS interfaces 4G/5G Signaling components with Protocol specific connectors (UDR Connector/CHF Connector/LDAP Gateway) to have a unified data source layer.
  - **Policy Runtime Engine** – Policy Runtime Engine (PRE) service runs the Policy Decision Engine. The policies can be configured using the configuration management service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - **PRE Test Engine** – The PRE Test Engine runs the Policy Decision Engine for test messages. Test message can be triggered from the configuration management service.
  - **Configuration Management** – This service provides the OAM interfaces that includes GUI and REST interfaces, for Policy and Service provisioning. Configuration Service and CM GUI offers graphical interface for all policy-related configurations and design of policies.
  - **Configuration Server** – This service performs the database abstraction for storage and retrieval of policy configuration.
  - **Query** – The Query microservice processes session viewer queries triggered by the configuration management service.
  - **Audit** – The Audit microservice runs the Audit engine to detect and process stale session records.
  - **App-Info** – This microservice monitors application (microservice) health and status.
  - **Perf-Info** – This microservice monitors application (microservice) capacity and load status.
  - **Bulwark** - This microservice facilitates the concurrency support for other internal services, such as SM service, AM service, Policy DS, etc.
  - **Notifier** - This microservice notifies subscribers about their data usage at different threshold levels.
  - **Usage Monitoring** - This microservice implements the usage monitoring procedures like usage accumulation, grant calculation, etc. for session and PCC flows.
  - **NWDAF Agent** - This microservice integrates Policy with Network Data Analytics Function (NWDAF) service to get analytics information.
- Data Tier
  - **Dynamic state** – Stores the session information relevant for policy context.
  - **Configuration store** – Stores the configuration related data.
- Ingress and Egress Gateway Traffic Management
  For more information on Ingress and Egress Gateway Traffic Management, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide.*

Copyright © 2019, 2026, Oracle and/or its affiliates.

3
Policy Services

This chapter explains the Policy services.

> **Note**
>
> The performance and capacity of the Policy system may vary based on the Call model, Feature/Interface configuration, underlying CNE and hardware environment, including but not limited to the complexity of deployed policies, policy table size , object expression and custom json usage in Policy design.

3.1 Audit Service

Policy signaling services like SM service, AM service, UE service, Binding Management service etc are stateless, thereby making the centralized DB tier to store the session states. The policy microservices session processing and DB tier transactions happen over network. The transactions that fail due to varied reasons get stored in the database as stale records. These stale records grows indefinitely over a period of time. The Audit Service is responsible for auditing the database to monitor for stale records, and either notify or clean up these stale records. The service that needs to use the Audit service to audit its tables, must register with the Audit service.

Figure 3-1 Audit Service Registration



Audit service is mainly responsible for:

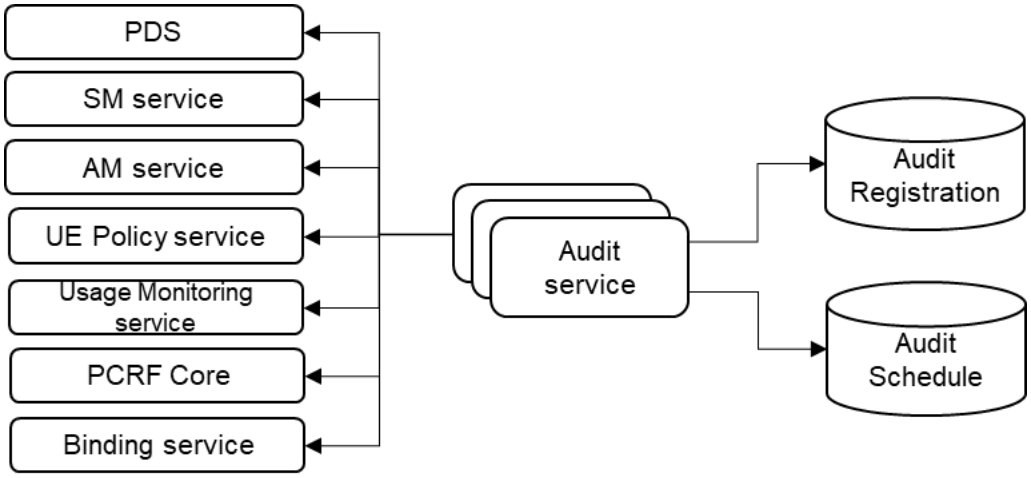
- allows core services to dynamically register or de-register the tables for auditing process
- core services can change other attributes at run time by using the Audit service restful interface
- notifying the context owners about the expired records in the registered table for auditing
- provide flow control of notifications towards the context owners
- perform forceful deletion of stale records, in case no corrective action is taken by context owners
- publish total count of records in the registered table for auditing

Audit service is not only responsible for stale session cleanup but has increased scope in other signaling features as well e.g., notifying core service for binding retry attempts.

Audit service with single pod deployment makes it neither scalable nor highly available. Audit service supports multiple pods, by using Audit Schedule. Audit Schedule helps to effectively manage and plan the audit service on the registered services.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 3-2 Multiple Pod Audit Service



Exception tables for the following services are maintained in an NDB Cluster to capture conflicting data.

- Binding Service
- SM Service
- AM Service
- UE Policy Service
- PCRF Core
- PDS
- Usage Monitoring

These exception tables are used to detect occurrences of conflict between sites and records/keys in tables for which conflict happens.

Records in exception tables can grow rapidly due to frequent collision that can happen. Audit service is used to cleanup these exception tables in scheduled manner. The Audit service configuration for cleaning up these exception tables are predefined using Helm parameters at the time of installation with a default 24hr frequency for auditing.

To enable auditing on the exception tables, add `exceptionTableAuditEnabled` parameter to custom-values.yaml file while upgrading to latest version and set the value of this parameter to true. After the upgrade procedure is complete, enable or disable the audit for the above mentioned services using CNC Console. For more details on enabling the audit, see *Enabling/Disabling Services Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

For information on how to configure Policy Audit Service, see Audit Service

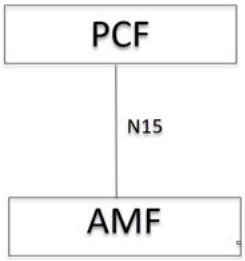
3.2 Access and Mobility Service

Policy implements Access and Mobility (AM) management service related policies over the N15 interface towards Access and Mobility Management Function (AMF).

The following figure describes the communication between PCF and AMF over the N15 interface:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 3-3 Communication between PCF and AMF over N15



AMF can perform the following functions:

- Enforcing control of policy decisions related to Radio Access Technology (RAT) or Frequency Selection Priority.
- Enforcing Service Area Restrictions. It is executed in User Equipment (UE).
- Enabling location tracking for a UE to get periodic updates on the current location of a subscriber.

Policy supports the following 3GPP defined services for AM Management:

Table 3-1 Access and Mobility Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_AMPolicyControl_Create	Creates an AM Policy Association and provides corresponding policies to the Network Function (NF) consumer	AMF	{apiRoot}/npcf-am-policy-control/v1/policies/	POST
Npcf_AMPolicyControl_Update	Updates an AM Policy Association and provides corresponding policies to the NF consumer when the policy control request trigger is met or the AMF is relocated due to the UE mobility and the old PCF is selected	AMF	{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}/update	POST
Npcf_AMPolicyControl_UpdateNotify	Provides updated policies to the NF consumer	PCF	{{Notification URI}/update {Notification URI}/terminate	POST

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-1 (Cont.) Access and Mobility Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_AMPolicyControl_Delete	Provides means for the NF consumer to delete the AM Policy Association	AMF	{apiRoot}/npcf-am-policy-control/v1/policies/{polAssoId}	DELETE
Npcf_AMPolicyControl_TerminateNotify	Requests termination of policies to the NF consumer	PCF	{apiRoot}/npcf-am-policy-control/v1/policies/{Notification URI}/terminate	POST

For information on how to configure PCF Access and Mobility service, see PCF Access and Mobility.

3.3 Authorization Service

PCF implements policy authorization service that authorizes Application Function (AF) request over the N5 interface.

Policy Authorization service supports the creation of policies as requested by AF for Packet Data Unit (PDU) session. Policy authorization service is a critical function for IP Multimedia Subsystem (IMS) integration and dynamic Policy and Charging Control (PCC) rule creation.

Oracle Communications PCF supports the following 3GPP defined services for Policy Authorization:

Table 3-2 Policy Authorization Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_PolicyAuthorization_Create	Determines and installs the policy according to the service information provided by an authorized NF service consumer.	AF, Network Exposure Function (NEF)	{apiRoot}/npcf-policyauthorization/v1/app-sessions	POST
Npcf_PolicyAuthorization_Update	Determines and updates the policy according to the modified service information provided by an authorized NF service consumer.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}	PATCH

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-2 (Cont.) Policy Authorization Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_PolicyAuthorization_Delete	Provides means to delete the application session context of the NF service consumer.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/delete	POST
Npcf_PolicyAuthorization_Notify	Notifies NF service consumer of the subscribed events.	PCF	{notifUri}/notify {notifUri}/terminate	POST
Npcf_PolicyAuthorization_Subscribe	Allows NF service consumers to subscribe to the notification of events.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription	PUT
Npcf_PolicyAuthorization_Unsubscribe	Allows NF service consumers to unsubscribe to the notification of events.	AF, NEF	{apiRoot}/npcf-policyauthorization/v1/app-sessions/{appSessionId}/events-subscription	DELETE

Policy authorization for PCF interaction with NEF

The `Npcf_PolicyAuthorization` on N5 and N30 interfaces act as the main integration point between PCF and NEF. The `Npcf_PolicyAuthorization` ensures that the services and applications utilizing the 5G network, especially those accessed externally through the NEF, are governed by appropriate policies established by the PCF.

The `Npcf_PolicyAuthorization` service operation authorizes the request from the NF service consumer NEF, and optionally communicates with `Npcf_SMPolicyControl` service to determine and install the policy according to the information provided by the NF service consumer.

PCF complies with 3GPP 23.502 and 29.514 Rel 15.4. For details on the message format, procedures followed, and the other aspects of `Npcf_PolicyAuthorization` over N5 interface that PCF complies with, see the *Compliance Matrix*.

For configuring Policy Authorization service, see PCF Policy Authorization.

3.4 Binding Service

Binding service stores binding information related to 4G and 5G subscribers and help Diameter Gateway in forwarding Application Function (AF) requests. It also queries Oracle Communications Cloud Native Core, Network Repository Function (NRF) client for fetching Oracle Communications Cloud Native Core, Binding Support Function (BSF) information (One time Query and subscribe for notifications). For BSF, autonomous NRF discovery and static configuration is only supported, on-demand is not yet supported. Session Management service and PCRF- Core service send all the relevant information to Binding service asynchronously.

In Policy, Diameter Gateway should have a converged mode, where:

- Diameter Gateway connects to PCRF-Core
- Diameter Gateway also accepts a connection from Diameter Connector

Copyright © 2019, 2026, Oracle and/or its affiliates.

In Converged mode of Diameter Gateway,

- All Diameter Applications except Rx are routed to PCRF-Core.
- For Rx messages, Diameter Gateway queries (asynchronously) Binding Service and based on the response, it forwards AF requests to either PCRF-Core or SM Service (via. Diameter Connector).

Configuration

In Helm Charts, you must configure **diamgateway.envGatewayMode** as **converged** in custom-values.yaml file, and the child helm files for Diameter-Gateway, Query-Service, and so on need to refer to this environment variable. This is mainly for performance considerations so that Diameter-Gateway and Query Service need not to query Binding service for the binding information. For more information on **diamgateway.envGatewayMode**, see *Oracle Communications Cloud Native Core Policy Installation, Upgrade and Fault Recovery Guide*.

Based on the value of the following parameters, either the Binding service or BSF is queried:

- **bindingSvcEnabled** in custom-values.yaml file under the sm-service section
- **Binding Operation** in Oracle Communications Cloud Native Core, Cloud Native Configuration Console (CNC Console under Policy → Service Configurations → PCF Session Management → Binding Configurations)

The behavior is as follows:

- If both the configuration variables are set to true, the Binding service is queried.
- If the **bindingSvcEnabled** parameter is true and the **Binding Operation** is false, the Binding service is queried.
- If the **bindingSvcEnabled** parameter is false and the **Binding Operation** is true, BSF is queried.
- If both the configuration variables are set to false, neither BSF nor the Binding service is queried.

Binding Service Truth table when receiving AAR-I

Following truth table is considered by Binding Service for finding the context owner of a session.

Priority: Priority indicates that attributes if specified in the message is considered as per the following priority from high to low. For example, IPv6 has higher priority indicates that if IPv6 is present, then only IPv6 binding is considered and corresponding context-owner information is returned otherwise next attribute priority is considered.

- IPv6
- IPv4 + APN/DNN+S-NSSAI
- IPv4
- IMSI
- MSISDN

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-3 Binding Service Truth table when receiving AAR-I

S.No.	Message	IPv6	IPv4	APN/ DNN+S-NSSAI	IP Domain ID	GPSI/ MSISDN	SUPI/ IMSI	Binding Lookup Query
1	Gx-CCRI/SM Association	P (Present in Gx CCR-I/N7 Sm create message)	P	P	P	P	P	IPv6
	AAR - I	P (Present in Rx AAR-I message)	P	P	P			
2	Gx-CCRI/SM Association	P	P	P	P	P	P	IPv4 + APN/ (DNN+S-NSSAI) + IP Domain ID
	AAR - I		P	P	P			
3	Gx-CCRI/SM Association	P	P	P	P	P	P	IPv4 (DNN and IP Domain ID won't be considered)
	AAR - I		P			P	P	
4	Gx-CCRI/SM Association	P	P	P		P	P	IPv4 + APN/ (DNN+S-NSSAI) + IP Domain IDIF No Records found (Would consider IP Domain ID as BLANK in Gx Session) => Not in the scope of PI-C (Need to enhance DB API for the same)
	AAR - I		P	P	P			

Copyright © 2019, 2026, Oracle and/or its affiliates.

Binding Service Truth table when receiving AAR-U

Table 3-4 Binding Service Truth table when receiving AAR-U

S.No.	Message	IPv6/IPv4	APN/DNN+ S-NSSAI	Session ID	Binding Lookup Query
1	AAR-U	P	P	P	Session-ID
2	AAR-U	P	P	P	IP Address + APN/DNN+S-NSSAI (If Rx Session Id not Found in Binding DB)
3	AAR-U	P		P	IP Address (If Rx Session Id not Found in Binding DB)

Note

- By default, only IPv6 prefixes with a /64-bit length are supported, and that this value is configurable using the binding.defaultIpv6PrefixLength helm parameter. For more information about this parameter, see Binding Service Configuration in *Oracle Communications Cloud Native Core Policy Installation, Upgrade and Fault Recovery Guide*.
- IP-CAN-Session Not available message is displayed when there is no suitable binding found in the binding service.
- UNABLE-TO-COMPLY message is displayed when request times out at Diameter Gateway.

Remote Cleanup of PDU Sessions when PDU Session Exceeds Limiting Number

In the event where the number of SM sessions per DNN exceeds the configured "Max sessions per DNN" value for a Binding service, Binding service triggers remote or local cleanup request towards SM service when the number of SM session per DNN exceeds the configured `Max sessions per DNN` value.

The deletion of stale binding session is controlled by a configurable binding flag. The binding flag "Max Session Cleanup Mode" can be set to either "Local" or "Remote" value.

- If the flag is set to "Local" PCF does not send terminate notification to SMF and deletes the session locally.
- If the flag is set to "Remote" PCF initiates terminate notification request toward SMF. PCF starts a timer to wait for SMF to send delete request to PCF based on `Force Delete On Expiry of Wait Timer` flag.
  - If delete request is received before timer expiry then deletes the session
  - If timer expires and delete request is not received PCF deletes the session

The timer value is configured in the PCF SM service Advanced setting page in CNC Console. Its default value is 30000 millisecond. This is considered only if "Remote" is selected in Binding service configuration.

Copyright © 2019, 2026, Oracle and/or its affiliates.

On failure of PCF terminate notification request to SMF, PCF deletes the session based on the "Force delete on Error" flag.

3.5 Notifier Service

Policy Notifier service is an optional service that allows Policy to send notifications to the subscribers about their current data usage. This service is independent of deployment mode and can be enabled in all the supported deployment modes.

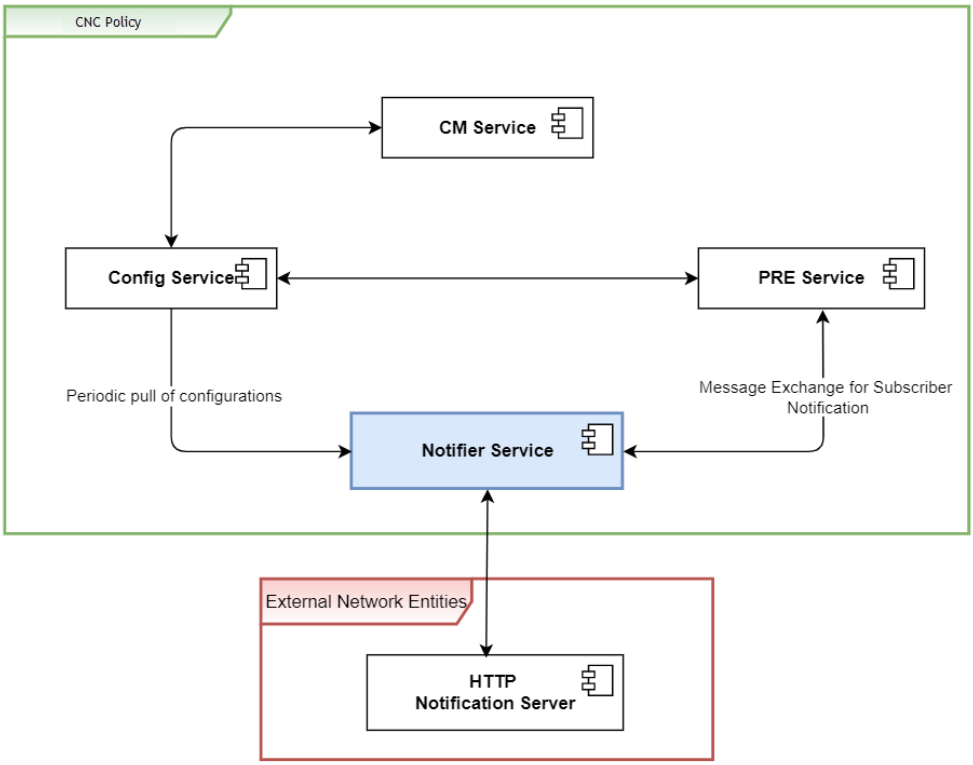
As part of subscriber quota management and based on the defined policies, the user is notified about their current usage at various levels. For example, when a user consumes 80% of the granted quota, a notification must be sent to notify the user about its usage. Similarly, when they reach or exceed the threshold, a notification must be sent informing the user about reduced quality of service or even suspension of service. With the Notifier service, Policy can send either HTTP notification or short messages (SMS) using SMPP to subscribers, based on the policies configured by operators, through an external notification server.

> **Note**
>
> In the current release, Policy supports subscriber notification only using HTTP and SMPP protocols.
> This feature is supported only for PCRF-Core call flows.

The following diagram shows how Notifier Service fetches configurations from Config service and on receiving notification request from PRE, sends out the notification to the subscriber via external notification server:

Copyright © 2019, 2026, Oracle and/or its affiliates.

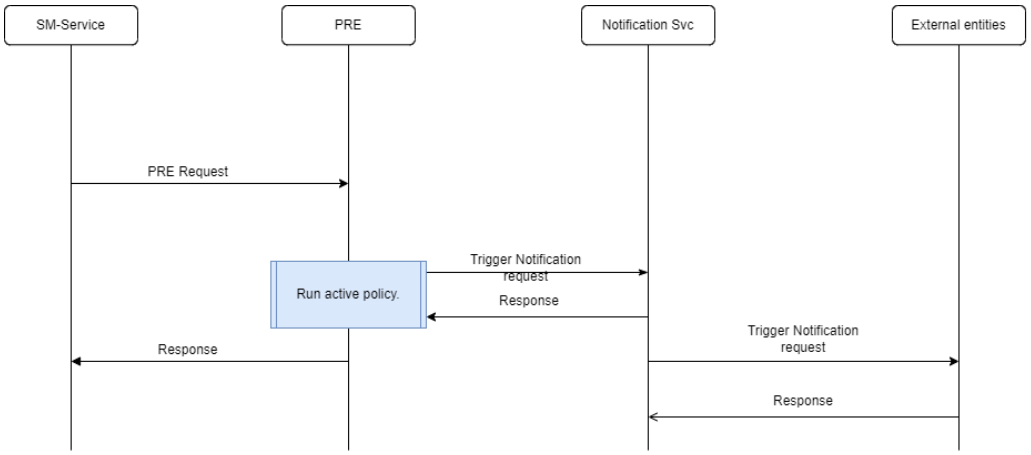
Figure 3-4 High Level Notifier Service Diagram



Call Flow

The following call flow diagram describes the notification call flow for SM service. As seen in the diagram, SM service sends a request to PRE that runs any given active policy and as a result triggers notification request to Notifier Service. Then, Notifier service sends a notification request towards the configured external server. On receiving success response, Notifier service sends the response to PRE, which in turn sends it to SM service.

Figure 3-5 Notifier Call Flow for SM Service



Copyright © 2019, 2026, Oracle and/or its affiliates.

Enable

By default, the Notifier service is disabled. Thus, the user cannot access the configurations from GUI.

To enable the service, set the following parameter to true at the time of installing or upgrading Policy:

```
notifierServiceEnable
```

For information on how to set the parameter value, see *Oracle Communications Cloud Native Core Policy Installation, Upgrade and Fault Recovery Guide*.

Configure

Once the service is enabled, you should be able to see **Notifier** service menu under the **Service Configurations** on CNC Console for Policy.

To allow flexibility, operators can configure an HTTP request message including the destination, content, and other attributes. The static content of the notification is retrieved from Policy variables and Policy table.

For information on how to configure Notifier service, see Configuring Notifier Service.

Logs

Policy publishes logs for all Hypertext Transfer Protocol (HTTP) messages sent via Policy action.

3.6 NWDAF Agent

Policy integrates with Network Data Analytics Function (NWDAF) service to get analytics information. NWDAF can provide various analytics data, which PCF can consume and use to make policy decisions. For more information analytics data, see Oracle Communications Networks Data Analytics Function User Guide.

> **Note**
>
> Policy 22.4.0 includes phase one implementation of Policy integration with NWDAF for testing purposes.

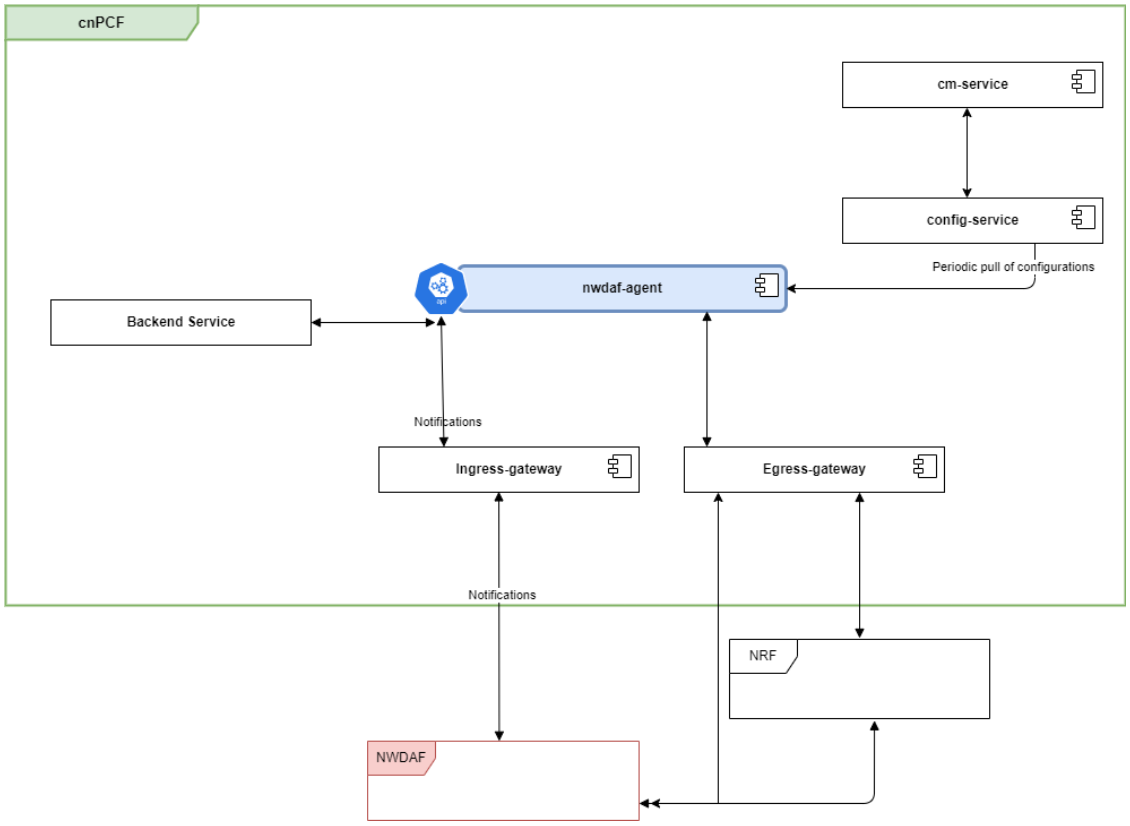
It also queries Network Repository Function (NRF) client for fetching NWDAF information. For NWDAF, autonomous NRF discovery and static configuration is only supported, on-demand is not yet supported. For more information on autonomously discovered NF profiles for NWDAF, see Discovered NF Instances.

A 5G network contains a vast number of devices and sensors generating an enormous amount of data. The NWDAF Agent allows the Communications Service Providers (CSPs) to efficiently monitor, manage, automate, and optimize their network operations by the data collected and analytics generated across the network. It also helps the CSPs in achieving the operational efficiency and provides an enhanced service experience. Currently, NWDAF Agent supports slice load level analytics as part of the analytics data that is provided from NWDAF.

The following diagram describes the interaction with NWDAF Agent and Policy:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 3-6 Interaction between Policy and NWDAF Agent



PCF supports the following 3GPP defined services for NWDAF Agent:

Table 3-5 3GPP defined services for NWDAF Agent

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method or Custom Operation
GET	Get NWDAF Agent Service configuration	AM	{apiRoot}/oc-cnpolicy-configuration/v1/services/nwdafAgent	GET
PUT	Update NWDAF Agent Service configuration	AM	{apiRoot}/oc-cnpolicy-configuration/v1/services/nwdafAgent	PUT
GET	Export NWDAF Agent Service configuration	AM	{apiRoot}/oc-cnpolicy-configuration/v1/services/nwdafAgent/export	GET

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-5 (Cont.) 3GPP defined services for NWDAF Agent

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method or Custom Operation
POST	Import NWDAF Agent Service configuration	AM	{apiRoot}/oc-cnpolicy-configuration/v1/services/nwdafAgent/import	POST

For information on parameters of the 3GPP defined services for NWDAF Agent , see *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide*.

Enable

By default, the NWDAF Agent is disabled. Thus, the user cannot access the configurations from GUI.

To enable the service, set the following parameter to true at the time of installing or upgrading Policy:

```
nwdafAgentServiceEnable
```

For information on how to set the parameter value, see *Oracle Communications Cloud Native Core Policy Installation, Upgrade and Fault Recovery Guide*.

Configure

Once the service is enabled, you should be able to see **NWDAF Agent** service menu under the **Service Configurations** on CNC Console for Policy.

For information on how to configure NWDAF Agent, see Configuring NWDAF Agent.

After the configuration you can use blockly to see the analytics data. For more information, see "Public Category" section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

3.7 PCRF Core Service

The Policy solution supports the Gx reference point for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from PCEF to PCRF.

PCRF Core Service supports the following:

- IP-CAN session Establishment, Modification, and Termination Support
- Install, Modify, or Remove Predefined PCC rules
- Install, Modify, or Remove Dynamic PCC rules
- Gate function
- Charging related information support
- Integration with AF (over Rx)
- Presence Area Reporting (PRA) Support

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Time of the day procedures
- Sponsored data connectivity support
- NSA related enhancements for QoS (Quality of Service)
- UE IPv4, IPv6, and IPv4v6 support

For information about configuring PCRF Core service, see Settings.

Configurations to route messages to OCS or UDR through Diameter Gateway

> **Note**
>
> Configurations described in this section are required when PCRF Core uses UDR or OCS as a datasource.

When CNC Policy is deployed in cnPCRF or converged mode, PCRF Core service does not connect directly to OCS or UDR. Instead, PCRF Core establishes a connection with Diameter gateway - the front end for any Diameter traffic, and routing of messages destined for OCS/UDR has to go through the latter.

To allow PCRF Core to communicate with UDR and OCS through Diameter gateway, perform the following Diameter peer configurations:

1. Configure the OCS as OCS peer by putting the following values on the **Create Peer Node** page:

Table 3-6 Peer Node Configuration

Field Name	Description
Name	Name of the peer node. Example value: `ocs`
Type	Type of the peer node. Example value: `ocs`
Reconnect Limit (sec)	The reconnect limit. This value must be configured as the Diameter peer configuration. Example value: `10`
Initiate Connection	Set to **true** to initiate the connection with peer node.
Port	OCS peer port detail. Example value: `8007`
Host	The OCS host IP/FQDN.
Realm	The realm detail of the OCS peer. Example value: `oracle.com`
Identity	The identity detail of the OCS peer. Example value: `ocs`

For more information, see Peer Nodes.

2. Configure the DataSource by providing the following values on Create Data Source page:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-7 Data Source Configuration

Field Name	Description
Name	Data source name. Example value: `ocs`
Description	Details about the data source.
Type	Data source type. Example value: `Sy`
admin state	Enable this switch.
Realm	The realm detail of the data source.
Role	Role of the data source. Example value: `Primary`
Timer Profile	Timer profile for the data source.
Primary Server	The primary data source server details. For Primary data source server, enter the following values: • **Identity**: Primary server identity. Example value: `oc-diam-gateway` • **Addr**: Load balancer IP of Diameter gateway. • **Port**: Port detail.

For more information, see Data Sources.

3. Configure the static routing table, using the configurations given in the following table:

Table 3-8 Diameter Route Table Configuration

Field Name	Description
Priority	Set the priority value. Example value: `1`
Name	Name of the route. Example value: `ocsroute`
Type	Route type Example value: `Realm`
Realms	The realm detail of the route. Example value: `oracle.com`
Application ID	Example value: `Sy`
Server Identifier	The value of this field is reference of Diameter peer configuration name. Example value: `ocs`

For more information, see Routing Table.

3.8 Policy Data Source (PDS) Service

Policy Data Source (PDS) Service

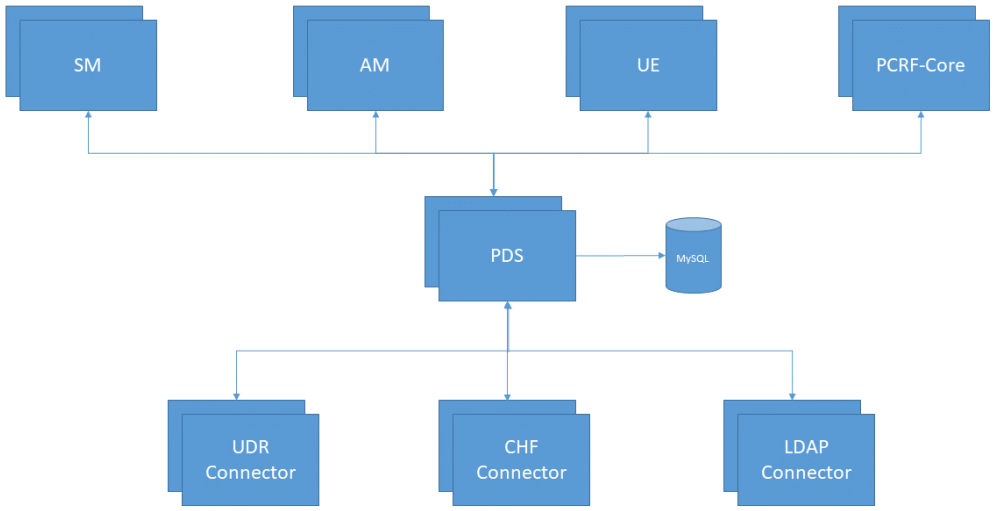
Policy Data Source Service (PDS) is an intermediate layer which interfaces Core Services (SM/AM/UE/PCRF-Core) with the protocol specific connector layers (UDR/CHF/LDAP Connectors). PDS also holds the subscriber information in its database when a new session

Copyright © 2019, 2026, Oracle and/or its affiliates.

gets established for a given subscriber and cleans-up the information when the last session termination happens. PDS is also responsible for storing the Subscriber State Variables except session level in its database and provides these variable information across multiple core services which requests the information.

You could define the workflows for PDS and the workflow would define the flow of request processing. This workflow is internal to the PDS project and should consult with engineering team for any update.

The following figure depicts the PDS architecture:



For configuring PDS service, see PDS Settings.

> **Note**
>
> Currently, PDS supports SUPI/GPSI as the search key. It does not support NAI as the search key.

UDR Connector- UDR Connector is a protocol specific layer which converts the request send by PDS to nUDR specific format and forwards to real UDR for subscription information. It also provides an ability to subscribe for profile change at UDR.

CHF Connector – CHF Connector is a protocol specific layer which converts the request send by PDS to nCHF specific format and forwards to actual CHF for fetching PolicyCounter Information. As per the standards, it automatically subscribes for profile change at CHF.
For configuring the UDR or CHF connector, see PCF User Connector.

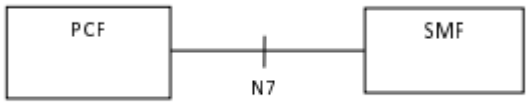
3.9 Session Management Service

Oracle Communications Policy Control Function (PCF) implements policy control for session management for service data flows. PCF implements the N7 interface to trigger the Session Management (SM) policies towards Session Management Function (SMF). SMF controls the User Plane Function (UPF) . It translates policies received from PCF to a set of directives or information that can be understood by UPF and then forwards it to the UPF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following figure illustrates the communication between PCF and SMF over the N7 interface.

Figure 3-7 Communication between PCF and SMF over N7



Session Management Service supports the following:

- Enforcement control of policy decisions related to QoS, charging, gating, service flow detection, packet routing and forwarding, and traffic usage reporting.
- Enforcement of QoS, charging, gating, service flow detection, packet routing and forwarding, and traffic accounting and reporting policy decisions can be distributed among the UPF, Radio Access Network (RAN), and User Equipment (UE) depending on the policy type.
- Support for UE IPv4, IPv6, and IPv4v6

Oracle Communications PCF supports the following 3GPP defined services for Session Management:

Table 3-9 Session Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_SMPolicyControl_Create	Request to create an SM Policy Association with the PCF to receive the policy for a PDU session	SMF	{apiRoot}/npcf-smpolicycontrol/v1/sm-policies	POST
Npcf_SMPolicyControl_Delete	Request to delete the SM Policy Association and the associated resources	SMF	{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/delete	POST
Npcf_SMPolicyControl_Update	Request to update the SM Policy association with the PCF to receive the updated policy when Policy Control Request Trigger condition is met	SMF	{apiRoot}/npcf-smpolicycontrol/v1/sm-policies/{smPolicyId}/update	POST

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-9 (Cont.) Session Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_SMPolicyControl_UpdateNotify	Update and/or delete the PCC rule(s) PDU session related policy context at the SMF and Policy Control Request Trigger information	PCF	{Notification URI}/update {Notification URI}/terminate	POST

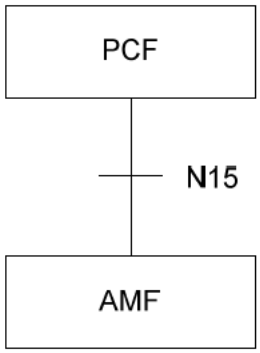
For configuring PCF Session Management service, see PCF Session Management.

3.10 UE Policy Service

Policy implements **PCF UE Policy** service to provision the UE policies, determined by PCF, to UE through AMF over the N15 interface.

The following figure describes the communication between PCF and AMF over the N15 interface:

Figure 3-8 PCF-AMF communication



PCF UE Policy service performs the following functions:

- Transferring UE Route Selection Policies (URSP) rules to UE
- Establishing the UE Policy Association requested by the NF service consumer
- Deleting the UE Policy Association requested by the NF service consumer
- Defining and delivering URSP message to UE via AMF using N1N2 message

Policy supports the following 3GPP defined service operations for the PCF UE Policy service:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-10 PCF UE Policy Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_UEPolicyControl_Create	Creates a UE Policy Association	AMF	{apiRoot}/npcf-ue-policy-control/v1/policies/	POST
Npcf_UEPolicyControl_Update	Provides means for the NF consumer, that is, AMF to update an existing UE Policy association. AMF invokes this procedure only if PCF has subscribed to location change trigger.	AMF	{apiRoot}/npcf-ue-policy-control/v1/policies/{polAssoId}	POST
Npcf_UEPolicyControl_UpdateNotify	Notifies NF consumer about the update made to policy control request trigger(s) by PCF	PCF	{Notification URI}	POST
Npcf_UEPolicyControl_Delete	Provides means for the NF consumer to delete the UE Policy Association	AMF	{apiRoot}/npcf-ue-policy-control/v1/policies/{polAssoId}	DELETE
N1N2MessageSubscribe	Creates a subscription for N1 Message Transfer	AMF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages/subscriptions	POST
N1N2MessageUnSubscribe	Deletes an existing subscription for N1 Message Transfer	AMF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages/subscriptions/{subscriptionId}	DELETE
N1N2MessageTransfer	Transfers an N1 message (NAS message) to be delivered to the UE	PCF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages	POST
N1N2MessageNotify	Indicates status of an N1N2 Message Transfer	AMF	{apiRoot}/v1/ue-contexts/{ueContextId}/n1-n2-messages/notify	POST

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 3-10 (Cont.) PCF UE Policy Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
N1N2MessageFailureNotify	Indicates that N1N2 message has failed to deliver to UE	AMF	{apiRoot}/v1/ue-contexts/{ueContextId}/n1-n2-messages/txfailure-notify	POST

For information on how to configure PCF UE Policy, see PCF UE Policy Service.

3.10.1 UE Policy Enhancements

UE Service in PCF is responsible for handling the User Equipment (UE) related procedures as described in 3GPP TS 29.525. This primarily includes delivery of UE Route Selection Policy (URSP) rules to the UE. URSP rules can be locally configured at PCF. The current implementation of PCF only supports local configuration of URSP rules, however UDR may send the UPSI codes to indicate to PCF which rules to deliver. PCF delivers URSP rules to UE via AMF on the N15 interface. PCF consumes the Namf-comm service provided (produced) by AMF on the N15 Namf interface.

AMF Selection for Namf-comm Subscription

Policy discovers the producer AMFs from NRF either using GUAMI or using the **AMF Set ID** and the **AMF Region ID**.

You can set the **AMF Discovery criteria** using CNC console.

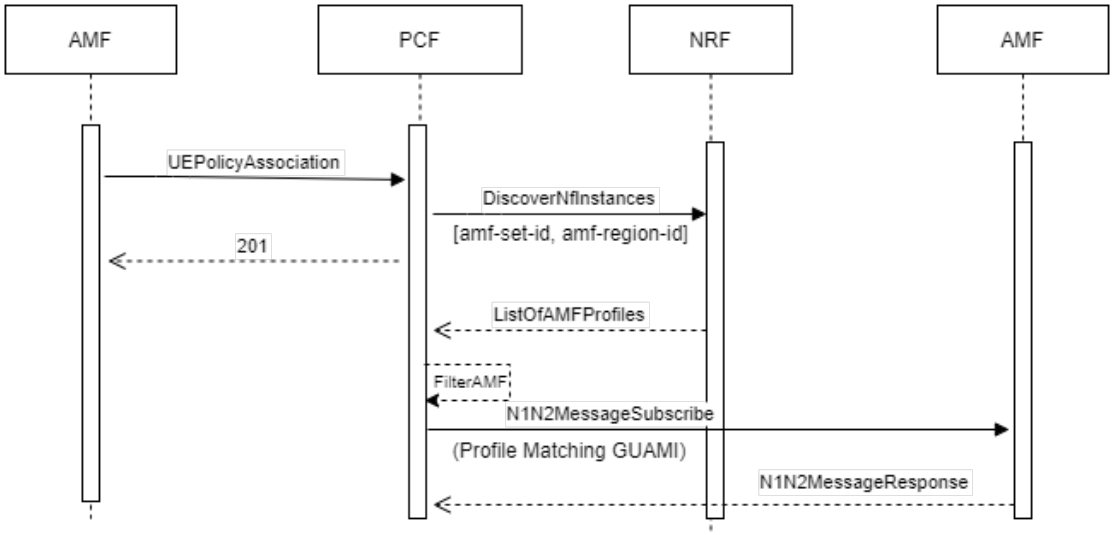
1. Log in to CNC Console as an Administrator.
2. Navigate to **PCF UE Policy page** under **Policy**.
3. Under **AMF** section, set the value of **AMF Discovery criteria** to either **GUAMI** or **SetID and RegionID**.
   - By default, the value of **AMF Discovery criteria** parameter is set to **GUAMI**.

     With this default configuration, Policy sends GUAMI to NRF to receive the list of AMF profiles. From the list of AMF profiles received from NRF, Policy selects one of the AMFs as the producer AMF.
   - If the value of **AMF Discovery criteria** parameter is set to **SetID and RegionID**, Policy extracts the AMF SetID and AMF RegionID from GUAMI and uses these IDs to discover the producer AMF as explained below.

> **Note**
>
> GUAMI is the default configuration for all existing deployments. With this default configuration, the upgrade support for existing customers will also be achieved and any new UEPolicyAssociation Request will not impact the existing behavior of AMF discovery based on **GUAMI**.

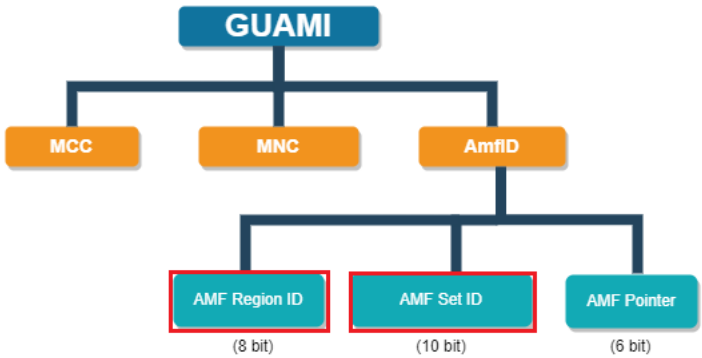
Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 3-9 Selecting Producer AMF using AMF SetID and AMF Region ID



1. Policy receives UEPolicyAssociationRequest from Consumer AMF.
2. If **AMF Discovery criteria** is set to **SetID and RegionID**, Policy parses the GUAMI to fetch the `AMF SetID` and `AMF RegionID`.

Figure 3-10 Parsing GUAMI



Sample GUAMI:

```
"guami": {
        "plmnId": {
            "mcc": "450",
            "mnc": "05"
        },
        "amfId": "010041"
    }
```

In the above example, Policy extracts the following details from GUAMI:

`amfid` = 010041

Copyright © 2019, 2026, Oracle and/or its affiliates.

`AMF RegionID` (first 8 bits): 01

`AMF SetID` (next 10 bits): 001

3. Policy includes the extracted **AMF SetID** and **AMF RegionID** in a query parameter (`amf-set-id, amf-region-id`) and queries the NrfClientConnector through NRF discovery URI `/nnrf-disc/v1/nf-instances`.
4. Policy receives a list of AMF Profiles as a response from NRF.
5. Policy selects the target AMF from the list of AMF Profiles by matching GUAMI received in UEPolicyAssociationRequest with the GUAMI(s) present in the list of AMFProfiles returned from NRF.
   a. If the above match results in a single AMF instance, Policy uses that AMF for the Subscription Request required for UE Policy Transfer.
   b. If there is no match, Policy applies the filter for Priority/Capacity Load to all the GUAMI's received in AMFProfile to identify the relevant AMF.
   c. If there are more than one AMF profiles, Policy applies the filter for Priority/Capacity Load to select the relevant AMF.
6. Policy sends a N1N2MessageSubscribe to the selected producer AMF and receives a response.
7. Policy responds the consumer AMF with a 201 message.

UE Policy Delivery Rules

The following rules are defined in 3GPP TS 29.525 with respect to UE Policy (URSP) delivery:

- The PCF shall only send "MANAGE UE POLICY COMMAND" messages below a predefined size limit.
- The PCF may deliver the UE policy to the UE in several "MANAGE UE POLICY COMMAND" messages.

The UE policy is divided into policy sections for fragmented delivery and subsequent partial updates of UE policies. Such policy sections may be predefined in the PCF, may be retrieved by the PCF from the UDR as specified in 3GPP TS 29.519, or maybe dynamically generated by the PCF, but shall comply with the rules below. If the predefined size limit is observed, the PCF may combine several policy sections into one "MANAGE UE POLICY COMMAND" message.

The following rules apply for policy sections:

- The size must be below the predefined size limit.
- The policy section must contain complete URSP rule(s), and no fractions of such rules.
- The policy section may contain a small number of policies, for example, URSP rule(s), to ease a subsequent partial update of UE policies.
- A single PLMN should provide the entire content of a policy section.

Each UE policy section is identified by a UE policy section identifier (UPSI). The UPSI is composed of two parts:

1. The PLMN ID part containing the PLMN ID for the PLMN of the PCF which provides the UE policies.
2. An UE policy section code (UPSC) containing a unique value within the PLMN selected by the PCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Fragmented URSP Delivery

The PCF may deliver the UE policy to the UE in several "MANAGE UE POLICY COMMAND" messages.

After sending a "MANAGE UE POLICY COMMAND" message, the PCF shall wait for a related confirmation in a "MANAGE UE POLICY COMPLETE" message or failure indication in a "MANAGE UE POLICY COMMAND REJECT" message. When no such message is received until the expiry of a supervision timer specified in Annexure D of 3GPP TS 24.501, or when a failure indication is received, the PCF should resend related instructions for the policy sections.

When UE Policy is installed with fragmentation, policy table do not support URSPs installation. Policy supports this feature implementation, by providing URSP data type and URSP List data type as column in the policy table. On the Policy Console, this column data types is added in the Create Policy Table page. Two Blocklys namely, URSP List data type and URSP data type is used by the create Policy table blocks.

For detailed information about configuring the policy blocks for UE Policy service type, see *Oracle Communication Cloud Native Core, Converged Policy Design Guide*.

Manage UE Policy Command Reject

In case of PCF receiving "MANAGE UE POLICY COMMAND REJECT", policy tries to re-transmit the N1N2Message for all the rejected UPSIs only. PCF will decode UE Policy Manage Command Reject and will resend the UPSIs as part of UE Policy Manage Command which were rejected by UE. This is done by setting the label `On UE Policy Command Reject` to **Re-Transmit Rejected UPSIs** value from the drop down list in the CNC Console.

> **Note**
>
> AMF notifying REJECT messages to PCF-UE with encoded rejected UPSIs should adhere to specification specified under Annexure D of 3GPP TS 24.501.

PCF handles the following N1N2Message transfer failures:

- On T 3501 Timer Expiry
- On Transaction Failure Notification
- On UE Policy Command Reject

Using CNC Console `N1 Message Retransmission Settings` group in `PCF UE Policy` page, the user can configure the UEPolicy `maximum number of retransmissions` and the actions to be taken to handle each failures separately.

For UE Policy configurations on CNC Console, see PCF UE Policy Service

Support of policy evaluation on AMF Notification on N1Notify and N1N2NotifyFailure

Currently, PCF does not evaluate Policies after N1 message notify or N1N2Transfer failure notification flow in PCF UE service. Thus PCF does not allow the user to take action dynamically and allows only static action such as retransmit, skip the fragment, or ignore.

This feature enables the PCF user to write policies using Policy blockly. PCF evaluates the policies and takes actions after receiving N1Message Notify messages with MANAGE UE POLICY COMPLETE or MANAGE UE POLICY COMMAND REJECT messages from AMF ,

Copyright © 2019, 2026, Oracle and/or its affiliates.

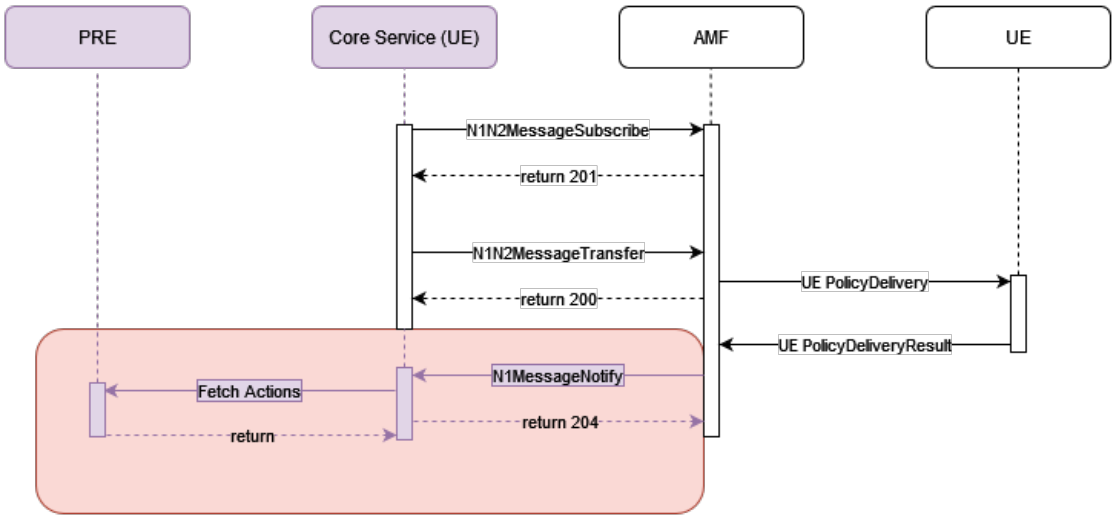
when UPSI's are installed. PCF UE service decodes the N1 Notify message that it receives from AMF during the rejection of URSP's by UE.

The subscription and transfer process are managed by the retry mechanism. In the notification flow, when the UE service receives a notification from AMF (N1MessageNotification), PRE is included both in the event of success or failure, allowing for subsequent installation attempts.

- In case of `MANAGE UE POLICY COMPLETE` message, PCF UE does not send the list of rejected UPSIs or URSPs since the transaction was completed successfully.
- In case of `MANAGE UE POLICY COMMAND REJECT` message, PCF UE sends the list of rejected UPSIs and URSPs to the PRE so that policy evaluation can be done using this information.
- In case of `N1N2MessageTransferFailure` message, PCF UE does not send the list of rejected UPSIs or URSPs as this is the a HTTP error with AMF and there is no information about rejected UPSIs or URSPS. PCF UE sends the cause of the failure to PRE.

> **Note**
>
> The blockly Policy created by considering the course of action that needs to be taken in the event of an error, supersedes any configurations set in `N1 Message Retransmission Settings` of the `PCF UE Policy` page in CNC Console.

Figure 3-11 UE and PRE interaction



The policy writer can check if the message is "MANAGE UE POLICY COMPLETE" and then take actions like:

- Write successfully the installed UPSI as a string value in VSA and update it to UDR.
- Define remote state variables, set values to variables and write in VSA and update it to UDR.

The policy writer can check if the message is "MANAGE UE POLICY COMMAND REJECT" and then take actions like:

- – Write successfully the installed UPSI as a string value in VSA and update it to UDR.
  - – Retransmit the failed UPSIs or new UPSIs, based on conditions like PLMN, SUPI, the failed UPSIs.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Skip the retransmit of UPSIs, based on conditions like PLMN, SUPI, the failed UPSIs.
- Abort the transaction of transferring the UEPolicy in N1N2Message based on conditions like PLMN, SUPI, the failed UPSIs.
- Define remote variables other than UPSI, set values to variables and write in VSA and update it to UDR.

Support of policy evaluation on T3501 Timer Expiry

Currently, PCF does not evaluate Policies after T 3501 timer expiry in PCF UE service. Thus PCF does not allow the user to take action dynamically and allows only static action present at CNC Console such as retransmit, skip the fragment, or abort. This feature enables the PCF user to write policies using Policy blockly on T3501 Timer Expiry. For more information, see "PCF UE Policy" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.

Deletion of URSP Rules

UE service allows deletion of URSP rule(s) in subsequent call flows that were previously sent over N1N2 NAS message delivery. The UPSI containers are updated and resent with the same UE Policy Section Code (UPSC) code and PLMN ID. An UPSI if being retransmitted because of URSP deletion will not further fragment the remaining URSPs within that UPSI as there is change in the size of the UPSI. The UPSI container honors the precedence of URSP rules while delivering in multiple fragments.

> **Note**
>
> The operator can perform Install and Remove URSP rules in the same policy execution cycle.

Managing UE Policy Enhancements

This section explains the procedure to enable and configure the feature.

Enable

This forms Policy applications core feature functionality. You do not need to enable or disable this feature.

Configure Using CNC Console

Perform the feature configurations in CNC Console as described in PCF UE Policy Service section.

Configure Using REST API

Perform the feature configurations as described in "UE Policy" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Document*

Configure Using Blockly

PCF UE services blockly's are described "UE Policy Blocks" section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Observability

Metrics:

Policy provides UE Policy metrics as described in UE Service Metrics section.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Maintain
If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support for more information on how to raise a service request.

3.11 Usage Monitoring Service

Policy Usage Monitoring is an internal service that interacts with Policy PRE service to get usage monitoring related Policy decisions and sends notifications to the subscribers about their current data usage. This service is independent of deployment mode and can be enabled in all the supported deployment modes.

With the introduction of Usage Monitoring service, Policy can control usage monitoring support for a PDU Session. Usage is defined as either volume or time of user plane traffic.

Policy receives usage monitoring related information per APN and UE from the UDR, i.e. the overall amount of allowed resources (based either on traffic volume and/or traffic time) that are to be monitored for the sessions of a user, together with the corresponding remaining allowed usage related information. In addition, usage monitoring related information for Monitoring key(s) per APN and UE may also be received from the UDR, together with the corresponding remaining allowed usage related information. For the purpose of usage monitoring control Policy requests the Usage report trigger and provides the necessary usage threshold(s), either volume threshold, time threshold, or both volume threshold and time threshold, upon which the PGW reports to Policy. Policy may request a usage report from the PGW.

Once Policy receives a usage report from the PGW, it deducts the value of the usage report from the remaining allowed usage for that APN.

Enable

By default, the Usage Monitoring service is disabled.

To enable the service, set the following parameter to true at the time of installing or upgrading Policy:

```
usageMonEnable
```

For information on how to set the parameter value, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

> **Note**
>
> To enable Usage Monitoring for PCRF, the deployment must have a 5G UDR as user data for Usage Monitoring is read from 5G UDR only.

Configure

Once the service is enabled, you can configure the Usage Monitoring service under the **Service Configurations** on CNC Console for Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For information on how to configure Usage Monitoring service, see Configuring Usage Monitoring.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4 Policy Features

These section explains Oracle Communications Cloud Native Core, Converged Policy features.

> **Note**
>
> The performance and capacity of the Policy system may vary based on the Call model, Feature/Interface configuration, underlying CNE, and hardware environment, including but not limited to the complexity of deployed policies, policy table size, object expression and custom json usage in Policy design.

4.1 Security Context

The Security Context Feature improves the security posture of deployed workloads in Oracle Communications Cloud Native Core, Converged Policy by applying Kubernetes pod and container security context settings.

A security context defines privilege and access control settings for a pod or container. These settings control how containers run, which user and group IDs are used, whether privilege escalation is allowed, which Linux capabilities are available, and whether the root filesystem is writable.

This feature applies the SA-approved deployment security context recommendations to Converged Policy services, Common Services consumed by Policy, and one-click deployment values. The implementation supports the following deployment models:

- OC-CNE based deployments.
- Non-OC-CNE deployments where the customer has no sidecar injections, or sidecars do not require special or elevated privileges.
- Non-OC-CNE deployments where the customer requires sidecar injections with different or elevated privileges.

The Security Context feature is supported for Converged Policy services and related services, including:

- `binding-service`
- `bulwark`
- `cmservice`
- `config-server`
- `diam-connector`
- `diam-gateway`
- `ldap-gateway`
- `notifier`
- `nwdaf-agent`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- pcf-amservice
- pcf-smservice
- pcf-ueservice
- pcf-userservice
- pcrf-core
- perf-info
- policy-runtime
- policyds
- queryservice
- session-state-audit
- soapconnector
- usage-mon
- app_info

The Security Context feature supports the following default configuration:

```
enableContainerSecurityContext: true
enablePodSecurityContext: false

podSecurityContext:
  runAsNonRoot: true
  runAsGroup: 25
  runAsUser: 25

containerSecurityContext:
  runAsNonRoot: true
  readOnlyRootFilesystem: true
  allowPrivilegeEscalation: false
  privileged: false
  capabilities:
    drop:
      - ALL
```

The container security context is enabled by default. The pod security context is available but disabled by default to avoid compatibility issues with deployments that use sidecar containers or other pod-level requirements.

Managing Security Context Feature

Enable

You can enable the Security Context Feature using Helm Configuration:

Enable Container Security Context:

You can enable or disable the feature by setting the `enableContainerSecurityContext` parameter to true or false in the custom-values.yaml file. The container security context is enabled by default.

Enable Pod Security Context:

Copyright © 2019, 2026, Oracle and/or its affiliates.

You can enable or disable the feature by setting the `enablePodSecurityContext` parameter to true or false in the custom-values.yaml file. The pod security context is disabled by default.

Service-Specific Configuration:

Use service-specific configuration when a service requires a different user ID, group ID, or security context value. For example:

```
bulwark:
  podSecurityContext:
    runAsNonRoot: true
    runAsUser: 5000
    runAsGroup: 5000
  containerSecurityContext:
    runAsNonRoot: true
    allowPrivilegeEscalation: false
    privileged: false
    readOnlyRootFilesystem: true
    capabilities:
      drop:
        - "ALL"
```

Deployment Template:

The deployment template applies the pod and container security context settings when the corresponding values are enabled.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  ...
spec:
  ...
  template:
    spec:
      ...
      {{- if .Values.global.setHostUsers }}
      hostUsers: false
      {{- end }}
      {{- if .Values.enablePodSecurityContext }}
      securityContext:
        {{- toYaml .Values.podSecurityContext | nindent 8 }}
      {{- end }}
      containers:
        - name: {{ .Chart.Name }}
          ...
          {{- if .Values.enableContainerSecurityContext }}
          securityContext:
            {{- toYaml .Values.containerSecurityContext | nindent 12 }}
          {{- end }}
```

Observability

There are no new Metrics, KPIs or alerts available for this feature.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.2 Support for Handling DB Cluster Disconnect

The Handling DB Cluster Disconnect feature enables PCF to detect DBTier cluster failure or disconnect events and adjust signaling behavior accordingly.

A DB cluster disconnect can occur because of software or infrastructure failures, multiple worker node restarts, network failure or latency across worker nodes, or operational activity such as manually restarting multiple DbTier data pods.

When a NodeGroup loses its in-memory data, the DB cluster can reform with empty in-memory tables and begin accepting new traffic. If the NF continues processing in this state, session data can become inconsistent across sites and session continuity can be affected. This feature enables to detect that condition and either suspend or continue signaling based on the configured cluster state policy.

With this feature, PCF enables to:

- Detect DB cluster disconnect or failure events through AppInfo polling of DB Monitor.
- Prevent the NF from accepting traffic when DB state is not suitable for session persistence.
- Support recovery in single-site deployments by allowing operators to restore NF sessions from backed-up data.
- Support multi-site recovery by allowing session restoration through GRR from a mate site.
- Provide an operator-controlled option to continue processing without backup-store recovery after a cluster disconnect.
- Expose the current DB cluster state and NF DB functional state through GUI and REST API surfaces.

The feature distinguishes between cluster states where NF signaling can continue and states where signaling should be suspended.

Functional states by default:

- `START`
- `CHECKPOINT`
- `RE_SYNC`

Non-functional or suspended states by default:

- `FAILURE`
- `RESTART`
- `RESTORE`

The default functional event list is operator configurable. For example, in a single-site deployment where the NF can resume without restoring from backup, `RESTART` can be added to the functional event list.

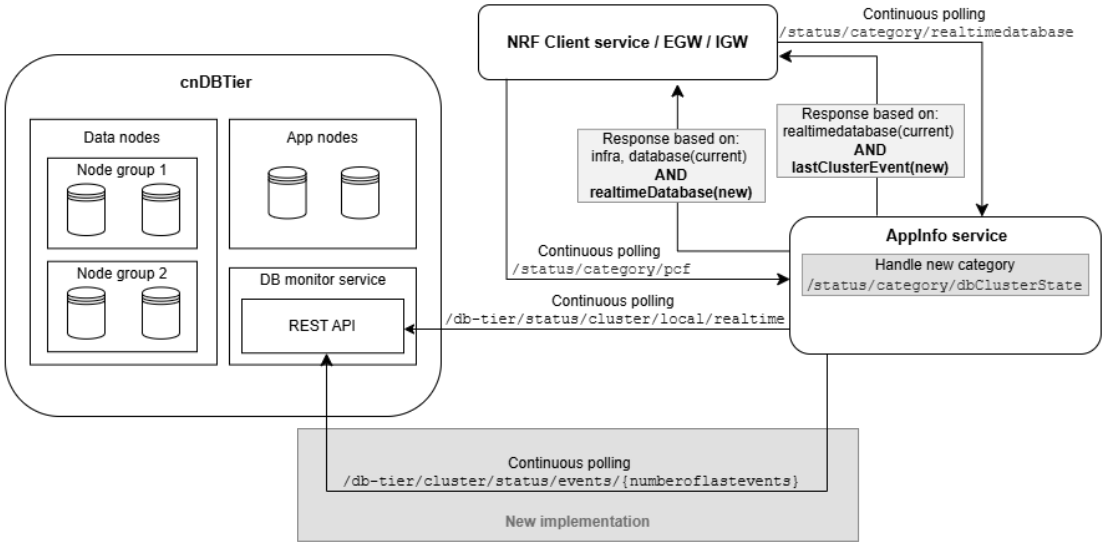
Architecture and Behavior

AppInfo runs as a multi-pod deployment. Unlike services that share a common database, each AppInfo pod stores its own data in a local text file, with no replication between AppInfo pods.

With cluster event tracking enabled, AppInfo runs a background process that continuously polls DB Monitor for cluster events using the configured DBTier cluster event URL. AppInfo stores the latest cluster state and derives an NF DB functional state from it.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-1 Architecture



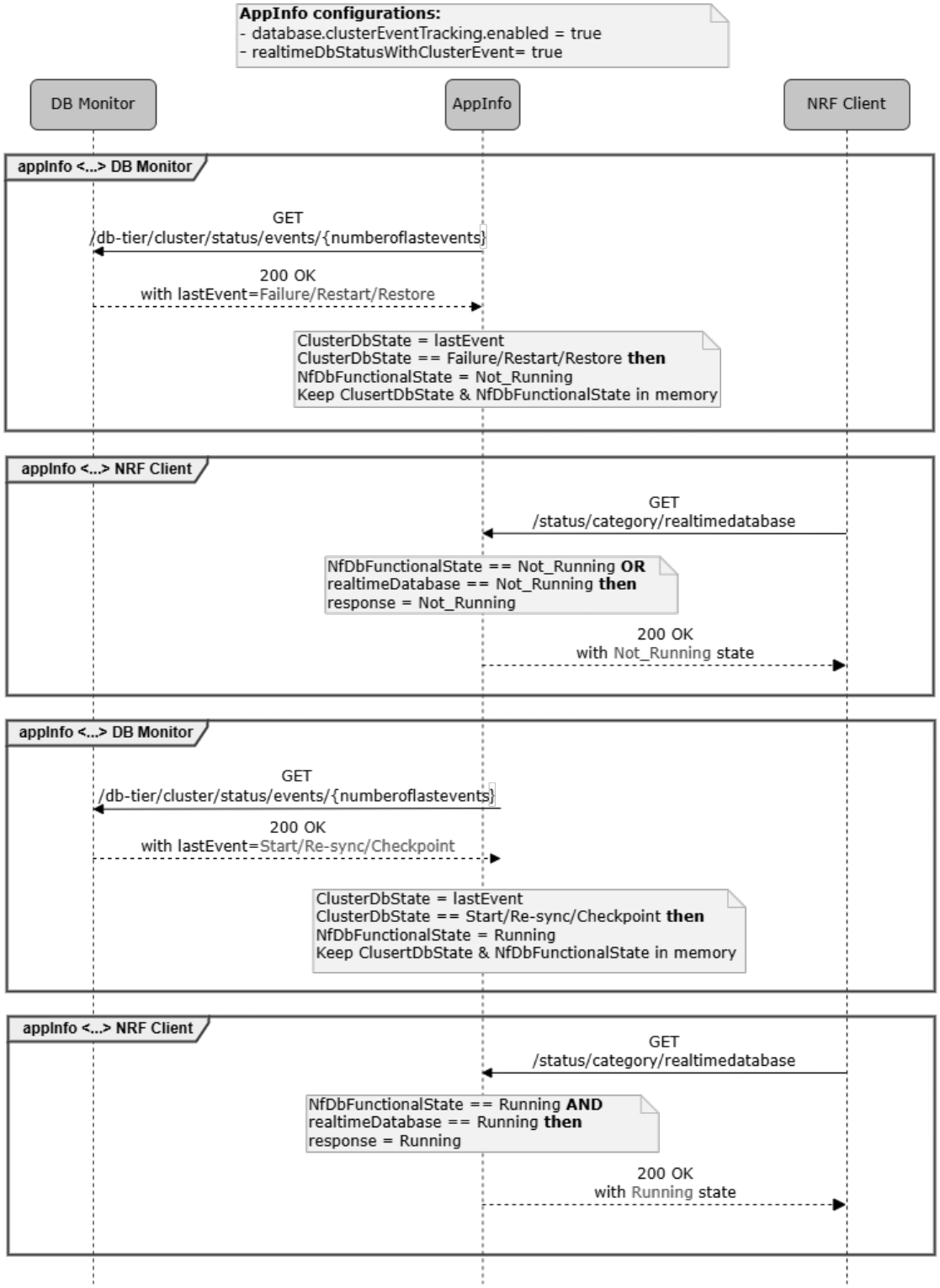
1. AppInfo polls DB Monitor for recent cluster events.
2. DB Monitor returns the last DB cluster event.
3. AppInfo maps the DB cluster event to `NfDbFunctionalState`.
4. AppInfo stores the current cluster state and NF DB functional state in memory, and may also persist cluster state in its states file.
5. Consumers such as NRF Client query AppInfo status APIs.
6. AppInfo includes the cluster-derived state when responding to realtime database or DB cluster state requests, depending on configuration.

When AppInfo receives a failure-like event such as `FAILURE`, `RESTART`, or `RESTORE`, it sets `NfDbFunctionalState` to `Not_Running`. When it receives a functional event such as `START`, `RE_SYNC`, or `CHECKPOINT`, it sets `NfDbFunctionalState` to `Running`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flows

Figure 4-2 clusterEventTracking enabled



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. DB Monitor detects a DB cluster disruption.

   When a DB cluster issue occurs, DB Monitor sends the latest cluster event to AppInfo. Disruption events include `Failure`, `Restart`, and `Restore`.

2. AppInfo reads the latest cluster event and stores it as the current cluster DB state:

   ```
   ClusterDbState = lastEvent
   ```

3. AppInfo marks the NF DB functional state as not running.

   If the latest cluster event is `Failure`, `Restart`, or `Restore`, AppInfo sets the NF DB functional state to `Not_Running`:

   ```
   ClusterDbState = Failure/Restart/Restore

   NfDbFunctionalState = Not_Running
   ```

   AppInfo keeps both `ClusterDbState` and `NfDbFunctionalState` in memory.

4. The NRF Client sends a status request to AppInfo to determine whether the database is available for NRF-related processing.

5. AppInfo evaluates the cluster-derived NF DB functional state and the real-time database state. If either value is `Not_Running`, AppInfo reports the database as not running:

   ```
   NfDbFunctionalState == Not_Running OR

   realtimeDatabase == Not_Running

   response = Not_Running
   ```

6. After the DB cluster begins recovery, DB Monitor sends a recovery event to AppInfo. Recovery events include `Start`, `Re-sync`, and `Checkpoint`.

7. AppInfo reads the latest cluster event and stores it as the current cluster DB state:

   ```
   ClusterDbState = lastEvent
   ```

8. If the latest cluster event is `Start`, `Re-sync`, or `Checkpoint`, AppInfo sets the NF DB functional state to `Running`:

   ```
   ClusterDbState = Start/Re-sync/Checkpoint

   NfDbFunctionalState = Running
   ```

   AppInfo keeps the updated `ClusterDbState` and `NfDbFunctionalState` in memory.

9. The NRF Client sends another status request after the recovery event has been processed.

10. AppInfo reports the database as running only when both the NF DB functional state and the real-time database state are running:

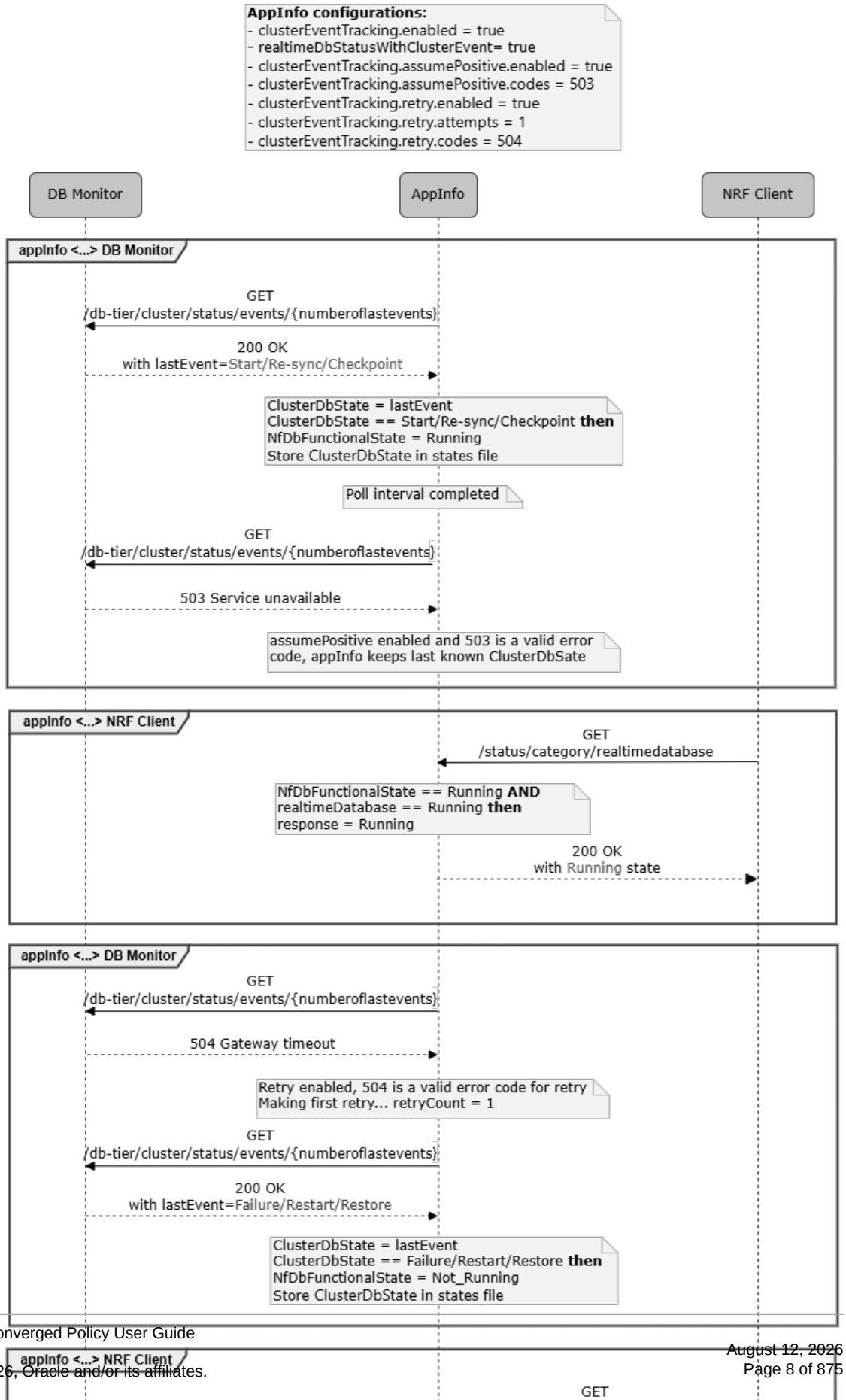
    ```
    NfDbFunctionalState == Running AND

    realtimeDatabase == Running

    response = Running
    ```


Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-3 clusterEventTracking, retry mechanism, and Assume Positive Configurations Enabled



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. DB Monitor sends the latest DB cluster event to AppInfo. In this flow, the event is a recovery event such as `Start`, `Re-sync`, or `Checkpoint`.
2. AppInfo stores the latest cluster event as the current DB cluster state. If the event is `Start`, `Re-sync`, or `Checkpoint`, AppInfo sets the NF DB functional state to `Running`:

   ```
   ClusterDbState = lastEvent

   ClusterDbState = Start/Re-sync/Checkpoint

   NfDbFunctionalState = Running
   ```
3. After deriving the NF DB functional state, AppInfo stores `ClusterDbState` in the states file.
4. AppInfo waits until the configured polling interval completes before polling DB Monitor again for the next cluster event.
5. If DB Monitor returns `503`, AppInfo treats it as a valid assume-positive error code because `clusterEventTracking.assumePositive.enabled` is enabled and `503` is configured in `clusterEventTracking.assumePositive.codes`.
6. Because the assume-positive condition is met, AppInfo does not mark the database as not running. AppInfo keeps the last known `ClusterDbState`, which continues to map the NF DB functional state to `Running`.
7. The NRF Client sends a status request to AppInfo after the assume-positive condition has been handled.
8. AppInfo reports the database as running when both the NF DB functional state and the real-time database state are running:

   ```
   NfDbFunctionalState == Running AND

   realtimeDatabase == Running

   response = Running
   ```
9. If DB Monitor returns `504`, AppInfo treats it as a valid retry error code because `clusterEventTracking.retry.enabled` is enabled and `504` is configured in `clusterEventTracking.retry.codes`.
10. AppInfo makes the first retry attempt and increments the retry count:

    ```
    retryCount = 1
    ```
11. After the retry, DB Monitor returns a disruption event such as `Failure`, `Restart`, or `Restore`.
12. AppInfo stores the latest event as the current DB cluster state. If the event is `Failure`, `Restart`, or `Restore`, AppInfo sets the NF DB functional state to `Not_Running`:

    ```
    ClusterDbState = lastEvent

    ClusterDbState = Failure/Restart/Restore

    NfDbFunctionalState = Not_Running
    ```
13. AppInfo stores the updated `ClusterDbState` in the states file.
14. The NRF Client sends another status request after AppInfo has processed the failure-type DB cluster event.
15. AppInfo reports the database as not running when either the NF DB functional state or the real-time database state is not running:

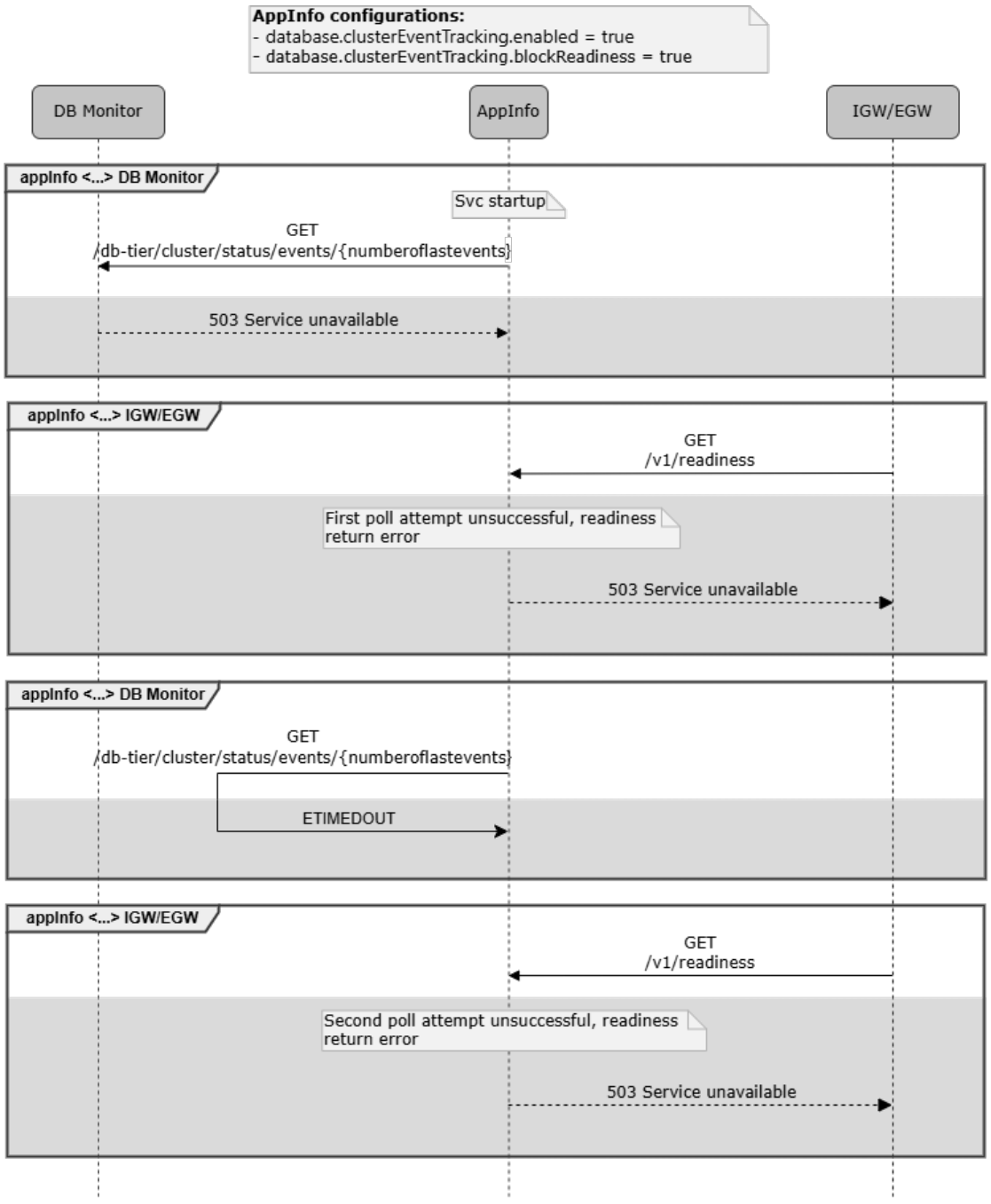
    ```
    NfDbFunctionalState == Not_Running OR

    realtimeDatabase == Not_Running
    ```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
response = Not_Running
```

Figure 4-4 clusterEventTracking and block readiness configuration enabled



1. During service startup, AppInfo initializes DB cluster event tracking because `database.clusterEventTracking.enabled` is set to `true`.
2. AppInfo polls DB Monitor for the current DB cluster state.

   AppInfo attempts to retrieve the latest DB cluster event from DB Monitor before reporting itself as ready.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. The first poll attempt is unsuccessful because DB Monitor responds with `503 Service unavailable`.
4. AppInfo blocks readiness after the unsuccessful first poll.

   Because `database.clusterEventTracking.blockReadiness` is enabled, AppInfo treats the unsuccessful DB Monitor poll as a readiness-blocking condition.
5. Ingress Gateway or Egress Gateway checks AppInfo readiness.

   Ingress Gateway or Egress Gateway sends a readiness-related request to AppInfo while AppInfo is still unable to confirm the DB cluster state.
6. AppInfo returns `503 Service unavailable` to Ingress Gateway or Egress Gateway.

   Because the first DB Monitor poll attempt was unsuccessful, AppInfo returns a readiness error to Ingress Gateway or Egress Gateway:

   ```
   response = 503 Service unavailable
   ```
7. AppInfo performs another poll attempt to retrieve the latest DB cluster state from DB Monitor.
8. The retry attempt is unsuccessful because the request to DB Monitor fails with a timeout:

   ```
   ETIMEDOUT
   ```
9. Because AppInfo still cannot confirm the DB cluster state, it keeps readiness blocked.
10. Ingress Gateway or Egress Gateway sends another readiness-related request after the second DB Monitor poll attempt fails.
11. Because the second DB Monitor poll attempt is also unsuccessful, AppInfo continues to return a readiness error to Ingress Gateway or Egress Gateway:

    ```
    response = 503 Service unavailable
    ```

Upgrade and Rollback Impact

Upgrade can fail if all of the following are true:

1. AppInfo readiness is blocked by `blockReadiness`.
2. `database.clusterEventTracking.enabled` is enabled.
3. The DB cluster has encountered a disconnect or failure event.

Managing Support for Handling DB Cluster Disconnect

Enable

To enable "Handling DB cluster disconnect" in PCF, configure the value of `database.clusterEventTracking.enabled` Helm parameter to `true` in the yaml file for AppInfo at the time of Policy installation or upgrade.

Configure

The configurations can be updated with the custom-values.yaml file along with the Helm install/upgrade process. The Helm process update the configMap with the configurations which are mounted in the app-info pods. Normally an upgrade between releases should restart pods and reflect the configuration changes. In a rare case that an in-release upgrade is needed, it is mandatory to restart the app-info pods manually to sync the configuration.

For more information, see *Cofiguring AppInfo to Handle cnDBTier DB Cluster Disconnect Functionality* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*

Copyright © 2019, 2026, Oracle and/or its affiliates.

Current DB cluster state and NF DB functional state can be viewed using the **PCF Cluster DB State** page under **DB Tier** on CNC Console.

For more information, see PCF Cluster DB State.

The current DB cluster state and NF DB functional state can be viewed using Policy DB Cluster State Query API using the URI `{apiRoot}/oc-cnpolicy-configuration/v1/dbClusterState`

For more information, see *Oracle Communications, Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics

The following metrics are used for this feature:

- appinfo_dbmonitor_request_total
- appinfo_dbmonitorclusterDbState_current
- appinfo_nfDbFunctionalState_change_total
- appinfo_nfDbFunctionalState_current
- appinfo_http_response_total

For more information, see AppInfo Metrics.

Alerts

The `PCF_STATE_NON_FUNCTIONAL_CRITICAL` alert is used for this feature.

For more information, see PCF_STATE_NON_FUNCTIONAL_CRITICAL.

4.3 Mutual Transport Layer Security

Mutual Transport Layer Security (mTLS) provides mutual authentication for both server and client. This method establishes TLS connection between client and server using the X.509 digital certificates to authenticate both server and client before sharing any data. In one-way TLS authentication, the client verifies the identity of the server. However, in mTLS, both client and server verify each other's identities before establishing a connection to share any data.

TLS certificates must be configured to enable HTTPS. These certificates are stored in Kubernetes secrets, and the secret details must be provided in the `custom_values.yaml` file. You must have the following files to create Kubernetes secret for mTLS:

- ECDSA private key and CA or self signed certificate if initialAlgorithm is ES256
- RSA private key and CA or self signed certificate if initialAlgorithm is RS256
- TrustStore password file
- KeyStore password file
- CA Root file

Copyright © 2019, 2026, Oracle and/or its affiliates.

Helm Configuration for Ingress and Egress Gateway HTTPS

The following configuration is a sample Helm parameter configuration required for Egress Gateway HTTPS:

```
#HTTPS Configuration#####################
#
initssl: true
enableIncomingHttps: false
#enable true only if "initssl" --> true
enableOutgoingHttps: true
http1:
  enableOutgoingHTTP1: false # Flag to enable or disable the feature
##########################################


service:
  # Specify type of service - Possible values are :- ClusterIP, NodePort,
LoadBalancer and ExternalName
  type: ClusterIP
  ssl:
    tlsVersion: TLSv1.2,TLSv1.3
    #supportedCipherSuiteList: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    privateKey:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      rsa:
        fileName: egwkey.pem
      ecdsa:
        fileName: ssl_ecdsa_private_key.pem

    certificate:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      rsa:
        fileName: egw.cer
      ecdsa:
        fileName: ssl_ecdsa_certificate.crt

    caBundle:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      fileName: caroot.cer

    keyStorePassword:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      fileName: key.txt

    trustStorePassword:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      fileName: trust.txt

    initialAlgorithm: RS256
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

The following configuration is a sample Helm parameter configuration required for Ingress Gateway HTTPS:

```
##############################################################################
# To Initialize SSL related infrastructure in init/update container
initssl: true
#Server Configuration for http and https support
enableIncomingHttp: false
enableIncomingHttp1: false
enableTLSIncomingHttp1: false
enableIncomingHttps: true
enableOutgoingHttps: false
#needClientAuth must be true if client certificate identity is required in
the header x-custom-ingress-client-identity
needClientAuth: true
##############################################################################

service:
  # Specify type of service - Possible values are :- ClusterIP, NodePort,
LoadBalancer and ExternalName
  type: ClusterIP
  ssl:
    tlsVersion: TLSv1.2,TLSv1.3
    #supportedCipherSuiteList: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    privateKey:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      rsa:
        fileName: igwkey.pem
      ecdsa:
        fileName: ssl_ecdsa_private_key.pem

    certificate:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      rsa:
        fileName: igw.cer
      ecdsa:
        fileName: ssl_ecdsa_certificate.crt

    caBundle:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      fileName: caroot.cer

    keyStorePassword:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      fileName: key.txt

    trustStorePassword:
      k8SecretName: ocegress-secret
      k8NameSpace: ocegress
      fileName: trust.txt
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
initialAlgorithm: RS256
```

Where,

- `initssl`: Generates KeyStore and TrustStore for HTTPS support. You must create TLS secret if this parameter is set to true.
- `enableIncomingHttps`: Opens https port on Ingress or Egress Gateway. You must enable this parameter if `initssl` is set to true.
- `enableOutgoingHttps`: Enables outgoing https connections at Ingress or Egress Gateway. You must enable this parameter if `initssl` is set to true.
- `enableOutgoingHTTP1`: Enables http1 outgoing connections.
- `enableStoreReloadEndpoint`: Controls the availability of the certificate reload endpoint. For more information about Helm parameters, see .

> **Note**
>
> – Based on initialAlgorithm, the init container considers an appropriate private key and certificate for KeyStore and TrustStore update. If initialAlgorithm is RS256, the RSA private key and certificate are used for handshake, and if initialAlgorithm is ES256, the ECDSA private key and certificate are used for handshake.
>
> – In earlier releases, Ingress or Egress Gateway used an endpoint for certificate reload capabilities. This endpoint was created when TLS was enabled in Ingress or Egress Gateway. After the deprecation of the update container, which was used to monitor certificates and trigger the certificate reload API, Ingress or Egress Gateway uses the certificate watcher for monitoring and reloading certificates.
> As there are no consumers for the certificate reload endpoint, its dependency is decoupled with TLS activation. If any NF wants this endpoint in Ingress or Egress Gateway, they must enable TLS in Ingress or Egress Gateway and set `enableStoreReloadEndpoint` to true.

Managing and Reloading Certificates in Gateway Services

Gateway Services access certificates available in Kubernetes secrets. When the certificates are expired or compromised, certificate renewal or new certificate update is required for which secret must be refreshed with new certificates. When there is an update in the certificate chain or a signed certificate is placed in the secrets, Kubernetes watcher, which is implemented in certificate management, checks for change in file state and replaces the KeyStore and TrustStore.

Dynamic reload of certificates is supported in Ingress and Egress Gateway. Certificate Management triggers the rest end point to dynamically reload KeyStore and TrustStore. Ingress and Egress Gateway considers new store files from shared volume and reloads trust and key managers. Ingress and Egress Gateway uses the replaced store to establish new connections and gracefully terminate existing connections by sending a GOAWAY frame.

1. To create and update the secrets and their content, do the following:

Copyright © 2019, 2026, Oracle and/or its affiliates.

a. To create the secrets for enabling HTTPS, run the following command:

```
kubectl create secret generic <secret-name> --from-file=<rsa private
key file name> --from-file=<ssl truststore password file name> --from-
file=<ssl keystore password file name> --from-file=<CA root bundle> --
from-file=<ssl rsa certificate file name> -n <Namespace of deployment>
```

b. To verify the secrets created, run the following command:

```
kubectl describe secret <secret-name> -n <Namespace of deployment>
```

c. To update an existing certificate, run the following command:

```
TLS_CRT=$(base64 < "<updated-certificate-name>" | tr -d '\n')
kubectl patch secret <secret-name> -p "{\"data\":{\"<certificate-
name>\":\"${TLS_CRT}\"}}" -n <namespace>
```

Creating CA Files

1. Create the following configuration file with identity information required for CA certificate generation:

```
[req]
distinguished_name = req_distinguished_name
x509_extensions = v3_ca
prompt = no

[req_distinguished_name]
C=IN
ST=KA
L=BLR
O=Oracle
OU=CGBU
CN=rootca.com

[ v3_ca ]
basicConstraints=critical,CA:TRUE
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
```

2. Run one of the following commands to generate RSA or ECDSA private key:
   - To generate RSA private key:

> **Note**
>
> Gateway Services support RSA and ECDSA cryptographic algorithm for data encryption and decryption.

```
#RSA key
openssl genpkey -algorithm RSA -out cakey.pem -pkeyopt
rsa_keygen_bits:2048 -outform PEM -quiet
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

- To generate ECDSA private key:

```
openssl genpkey -algorithm EC -out cakey.pem -pkeyopt
ec_paramgen_curve:secp384r1 -pkeyopt ec_param_enc:named_curve -outform
PEM
```

3. Run the following command to generate CA root certificate:

```
openssl req -new -x509 -days 3650 -config rootca.cnf -extensions v3_ca -
key cakey.pem -out caroot.cer
```

Creating Gateway (server or client) Files

1. Create the following configuration file with identity information required by certificate signing request to apply for a digital signed certificate:

```
[req]
distinguished_name=req_distinguished_name
req_extensions=req_ext
prompt=no
[req_distinguished_name]
C=IN
ST=KA
L=BLR
O=Oracle
OU=CGBU
CN=ingress-gateway.demo.svc.cluster.local
[req_ext]
keyUsage=digitalSignature, keyEncipherment
extendedKeyUsage=clientAuth, serverAuth
basicConstraints=CA:FALSE
subjectAltName=@alt_names
[alt_names]
IP.1=10.75.213.110
DNS.1=centos8-2.example.com
URI.1=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6
```

2. Run one of the following commands to generate RSA or ECDSA private key:
   - To generate RSA private key:

> **Note**
>
> Gateway Services support RSA and ECDSA cryptographic algorithm for data encryption and decryption.

```
openssl genpkey -algorithm RSA -out igwkey.pem -pkeyopt
rsa_keygen_bits:2048 -outform PEM -quiet
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

- To generate ECDSA private key:

```
openssl genpkey -algorithm EC -out igwkey.pem -pkeyopt
ec_paramgen_curve:secp384r1 -pkeyopt ec_param_enc:named_curve -outform
PEM
```

3. Run the following command to generate certificate signing request to get the certificate signed by CA:

```
openssl req -new -key igwkey.pem -out igw.csr -config igwcsr.cnf
```

4. Run the following command to sign the certificate with CA:

```
openssl x509 -req -in igw.csr -CA caroot.cer -CAkey cakey.pem -days 365 -
extfile igwcsr.cnf -extensions req_ext -out igw.cer -set_serial 1234
```

> **Note**
>
> extendedKeyUsage limits the purposes for which certificate can be used. clientAuth allows the certificate to be used for client identity and serverAuth allows the certificate to be used for server identity. Do not use the certificate with extendedKeyUsage as client in server and vice versa.

For digital signature algorithms, see Table 4-116.

4.4 Diameter Gateway Connection Repaving

In large Diameter deployments, connection distribution across Diameter Gateway (DGW) pods can become uneven over time due to node restarts, failovers, scaling operations, or network events. This imbalance can result in some DGW pods handling a disproportionately high number of Diameter connections while others remain underutilized.

With Diameter Gateway Connection Repaving feature provides a controlled mechanism to re-balance Diameter connections across the cluster without restarting services or causing a complete outage. It allows to force the disconnection of the existing external Diameter connections so that external peers reconnect through the Layer-4 load balancer and are re-distributed across available Diameter Gateway pods.

The feature supports:

- Controlled and staggered disconnection of Diameter connections
- Continuous acceptance of new incoming connections during repaving
- Historical auditing of repaving operations
- Configurable throttling and jitter controls
- Enable/disable control through configuration settings

The repaving process uses two levels of staggering:

- Pod-Level Jitter: Prevents all pods from disconnecting simultaneously.
- Connection-Level Throttle: Prevents flooding peers with mass disconnects

The repaving process can be triggered through either:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- CNC Console
- Diameter Repaving REST API

When the repaving process is triggered:

1. The operator, automation client, or CNC Console invokes the Diameter Repaving REST API on CM Service. CM Service validates the request, generates `invocationId` and `requestTimestamp`, updates the Config Server trigger topic, and records the trigger in historical_data. Diameter Gateway pods detect the Config Server topic update `common.public.connectionrepaving.diameter-gateway.trigger.disconnect` and executes the repaving operation when the feature is enabled.
2. Writes an audit entry into the `historical_data` table.
3. Diameter Gateway pods monitor this topic.
4. Upon detecting the update, if **Enable Diameter Gateway Repaving** field is enabled on **Diameter Connection Repaving** page under **Diameter Configuration** on CNC Console:
   - Each pod calculates a random stagger delay. This prevents simultaneous disconnections across pods.
   - After the jitter delay expires, existing external Diameter connections established before the trigger timestamp are disconnected.
     The connections are disconnected sequentially.

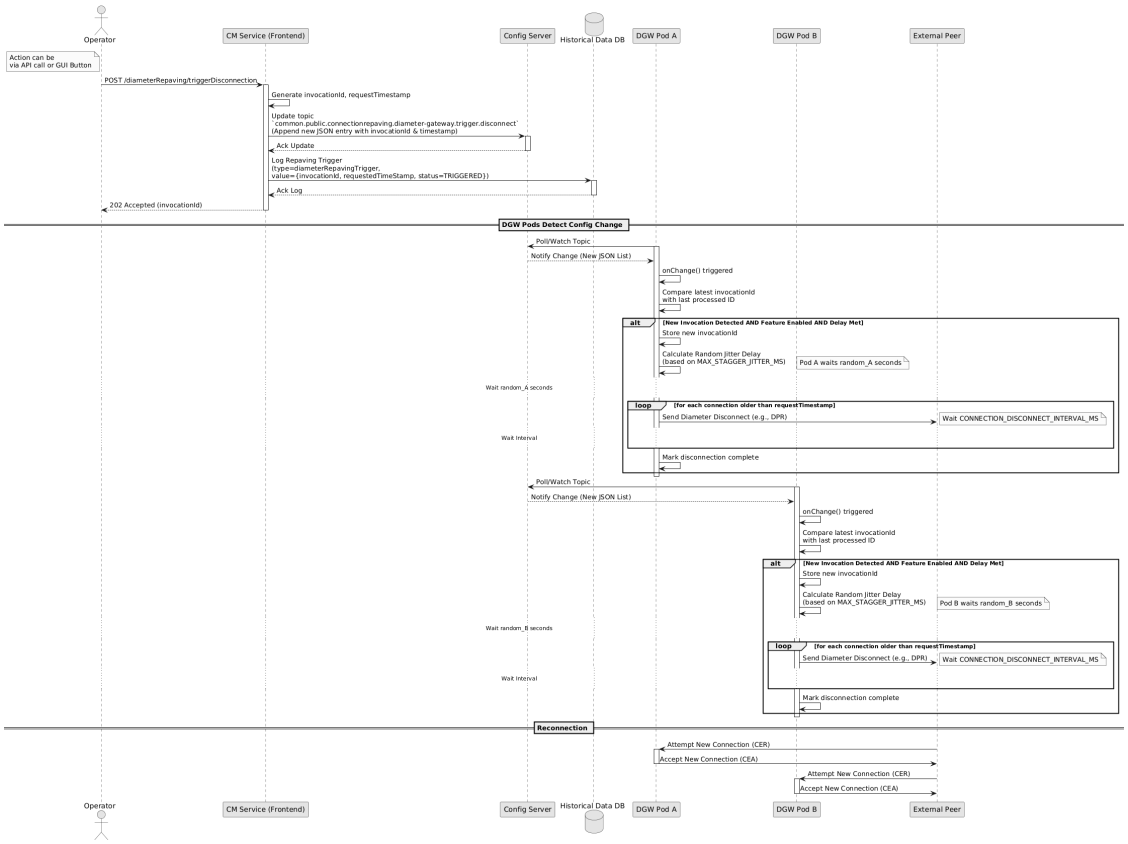
     A configurable delay is applied between disconnect operations.
   - New connection requests are continued to be accepted throughout the repaving process, ensuring service continuity.
5. The pod performs the throttled disconnection of connections established before the trigger timestamp. Once disconnections are complete, it marks processing for the trigger as finished and sets `isRepavingBusy` to `false`. The pod checks its internal queue and returns to idle monitoring when the queue is empty.
6. External Peers, having their old connections terminated, will automatically attempt to re-establish their connections (if they haven't already done so with new connections accepted during the process).
7. These new connection attempts are accepted by the Diameter Gateway pods.
8. Diameter Gateway processing completes after the pod has handled all eligible external Diameter connections established before the trigger timestamp and completed any applicable queued trigger processing. External peers subsequently reconnect, and the Layer-4 load balancer redistributes the new connections. The resulting connection distribution must be verified using external monitoring.

> **Note**
>
> The Diameter Gateway side repaving completes after eligible connections are disconnected. The final balancing depends on peer re-connection behavior and load balancer distribution.

Copyright © 2019, 2026, Oracle and/or its affiliates.

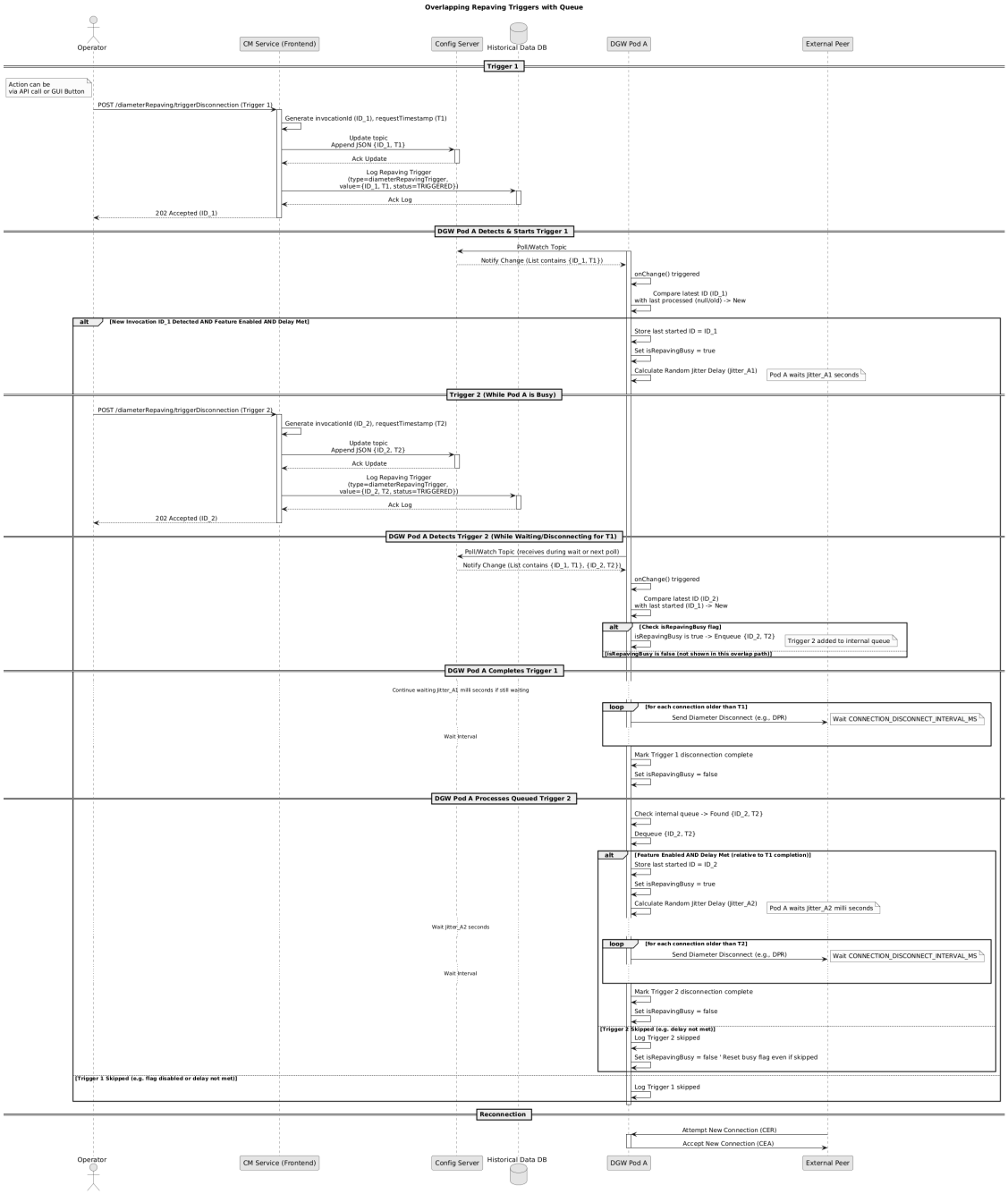
Call Flows

Figure 4-5 Diameter Gateway Connection Termination



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-6 Overlapping Repaving Triggers with Queue



Scenario 1: Successful Connection Repaving Execution

1. Initiation (Operator Action & CM Service Update)

A request is sent to the CM Service's dedicated repaving API endpoint such as `{apiRoot}/oc-cnpolicy-configuration/v1/diameterRepaving/triggerDisconnection`.

The CM Service validates the request, generates a unique `invocationId` and `requestTimestamp`.

The CM Service updates the configuration topic `common.public.connectionrepaving.diameter-gateway.trigger.disconnect` in the

Copyright © 2019, 2026, Oracle and/or its affiliates.

Config Server by replacing the trigger information with the latest one, holding the latest `invocationId` and `requestTimestamp`.

The CM Service logs a single entry to the `historical_data` table with `type="diameterRepavingTrigger"`, including the `invocationId` and `requestTimestamp` in the value field.

2. **Configuration Change Detection (Diameter Gateway Pods)**

   Each Diameter Gateway pod's configuration client, which is monitoring the `common.public.connectionrepaving.diameter-gateway.trigger.disconnect` topic, detects the update (the newly added entry).

   The config client invokes the onChange (or equivalent) callback method within the Diameter Gateway service, passing the updated list of invocation records.

3. **Two-Tiered Disconnection Execution (Diameter Gateway Pods)**

   a. Trigger Validation: Inside the onChange handler, each pod:

      Retrieves the latest invocation record from the received data.

      Compares its `invocationId` with the ID of the last trigger it processed (stored locally).

      If the ID is new: Checks if the feature is enabled, that is, `common.public.connectionrepaving.diameter-gateway.config enabled is true` and if the minimum re-invocation delay `DGW_CONNECTION_REPAVING.REINVOCATION_DELAY_MIN` has passed.

   b. Tier 1 (Pod-Level Jitter): If validation passes, the pod:

      Stores the new `invocationId` as the last processed ID.

      Independently calculates a random stagger delay based on `DGW_CONNECTION_REPAVING.MAX_STAGGER_JITTER_MS`.

      ```
      Wait Time = random(0, MAX_STAGGER_JITTER_MS)
      ```

      Pauses execution for this unique, random duration (for example, Pod-A might wait 17 ms, Pod-B might wait 142 ms). Logs that it is waiting.

   c. Service Continuity: During this entire process (both the initial wait and the disconnection phase), all Diameter Gateway pods remain active and accepts new incoming connections from peers.

   d. Tier 2 (Connection-Level Throttle): After its random pod-level delay expires, the pod begins its disconnection logic.

      It iterates through all its existing external Diameter connections that were established before the `requestTimestamp` associated with the current `invocationId`.

      The order of disconnection is not based on load or complex logic.

      To prevent flooding the peer, the pod pauses between terminating each connection for the interval specified in `DGW_CONNECTION_REPAVING.CONNECTION_DISCONNECT_INTERVAL_MS`.

4. Sequential Trigger Processing with Internal Queue: To enhance robustness in scenarios where repaving might be triggered very frequently (potentially faster than a pod's disconnection cycle + `DGW_CONNECTION_REPAVING.REINVOCATION_DELAY_MIN`), a queue and the `isRepavingBusy` flag are implemented In this model:

   The flag `isRepavingBusy` determines if a given repaving trigger is completed or it is still in progress, changing the status (true/false) when it starts and finishes.

   Each Diameter Gateway pod maintains an internal queue for incoming repaving triggers (represented by their `invocationId` and `requestTimestamp`).

Copyright © 2019, 2026, Oracle and/or its affiliates.

When a new trigger is detected using onChange, is added to the queue if the pod is currently busy processing a previous trigger.

Once a pod completes a repaving cycle the `isRepavingBusy` flag is set to `false`. It checks its internal queue. If the queue is not empty, it dequeues the next trigger and begins processing it. After validating the `DGW_CONNECTION_REPAVING.REINVOCATION_DELAY_MIN` against the dequeued trigger's timestamp relative to the previously completed one.

This ensures that the rapid triggers are not lost or rejected but are processed sequentially, preserving the order of operations while still preventing simultaneous execution within a single pod. This approach offers greater resilience against very high trigger rates.

5. Completion and Recovery:

   External Peers, having their old connections terminated, automatically attempts to re-establish their connections (if they are not already done so with new connections accepted during the process).

   These new connection attempts are accepted by the Diameter Gateway pods.

   The new connections are naturally re-balanced across the cluster by the Layer-4 load balancer, completing the repaving process.

Scenario 2: New Connection Attempt During Force Disconnection

This scenario describes what happens when an external system tries to connect while a pod is actively repaving.

1. Upon receiving the configuration change event, the Diameter Gateway pod starts the disconnection of all external connections established prior to the timestamp included in the event.
2. An external peer sends a new connection request (such as a Diameter CER message) to the Diameter Gateway pod.
3. Diameter Gateway pod continues accepting external connections during force disconnections.
4. The external peer likely retry the connection after a back off period, by which time the Diameter Gateway pod may have completed its process.

Scenario 3: Diameter Repaving is Triggered While this Feature is Disabled

This scenario covers the safety mechanism provided by the feature flag.

1. CM service receives a request for Diameter Gateway Repaving through REST API or CNC Console.
2. CM service reads the Diameter Gateway Repaving configuration.
3. If `enableRepaving` is `false`, CM Service blocks the trigger request.
4. CM service records the rejected trigger attempt in `historical_data` with `FAILURE` status and a disabled-feature reason.
5. CM Service does not update the Config Server trigger topic: `common.public.connectionrepaving.diameter-gateway.trigger.disconnect`.
6. Diameter Gateway pods are not notified, and no repaving operation is executed.

Scenario 4: Overlapping Repaving Triggers with Queuing

This scenario describes how a Diameter Gateway pod handles a new repaving trigger that arrives while it is already processing a previous one, utilizing an internal queue.

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Initial State: Diameter Gateway Pod-A is idle (not currently repaving) and is monitoring the `common.public.connectionrepaving.diameter-gateway.trigger.disconnect` topic. Its last processed `invocationId` is null or some older ID.
2. Trigger 1 Initiation: A repaving request is initiated through the API. The CM Service updates the config topic with `{ "invocationId": "trigger-UUID-1", "requestTimestamp": "T1" }`. CM Service logs the trigger in `historical_data`.
3. Diameter Gateway Pod-A Detects & Starts Trigger 1:

   Pod-A's config client detects the change. The onChange handler runs.

   It compares `"trigger-UUID-1"` (latest) with its last processed ID (old/null).

   Feature flag and re-invocation delay check is passed.

   Pod-A stores `"trigger-UUID-1"` as its last started ID.

   Pod-A calculates its random jitter delay (such as Jitter-1).

   Pod-A enters a `"busy"` state (for example, sets an internal `isRepavingBusy` flag to `true`) and begins the Jitter-1 wait period.
4. Trigger 2 Initiation (During Pod-A's Busy State): Before Pod-A completes its disconnection cycle for Trigger 1 (either during the Jitter-1 wait or the subsequent throttled disconnection phase), the operator triggers repaving again. The CM Service updates the config topic, appending `{ "invocationId": "trigger-UUID-2", "requestTimestamp": "T2" }`. CM Service logs this second trigger.
5. Diameter Gateway Pod-A detects trigger 2:

   Pod-A's config client detects the second change (the list now contains both triggers). The onChange handler runs again.

   It compares `"trigger-UUID-2"` (latest) with its last started ID (`"trigger-UUID-1"`).

   It checks its internal state and finds that `isRepavingBusy` flag is set to `true`.

   Instead of immediately processing it, Pod-A adds Trigger 2 (`"trigger-UUID-2", T2`) to its internal queue. It does not calculate jitter or start waiting for Trigger 2 yet.
6. Diameter Gateway Pod-A Completes Trigger 1:

   Pod-A finishes the Jitter-1 wait.

   It performs the throttled disconnection of connections established before T1.

   Once the disconnections for Trigger 1 are complete, it marks processing for `"trigger-UUID-1"` as finished and sets `isRepavingBusy` flag back to `false`.
7. Diameter Gateway Pod-A Dequeues & Starts Trigger 2:

   Pod-A checks its internal queue and finds Trigger 2. It dequeues it.

   It performs the validation checks for Trigger 2:

   - Feature flag check.
   - Re-invocation delay check: Compares T2 against the completion time of Trigger 1 using `REINVOCATION_DELAY_MIN`. The check is passed.

   Pod-A stores `"trigger-UUID-2"` as its last started ID.

   Pod-A calculates its random jitter delay (Jitter-2).

   Pod-A sets `isRepavingBusy` flag to `true` and begins the Jitter-2 wait period.
8. Diameter Gateway Pod-A Completes Trigger 2:

   Pod-A finishes the Jitter-2 wait.

Copyright © 2019, 2026, Oracle and/or its affiliates.

It performs the throttled disconnection of connections established before T2 (but after T1, if any were established and accepted in between).

Once disconnections for Trigger 2 are complete, it marks processing for `"trigger-UUID-2"` as finished, sets `isRepavingBusy` flag to `false`.

Pod-A checks its internal queue again; it's empty. The pod returns to idle monitoring.

Managing Diameter Gateway Connection Repaving

Enable

This feature can be enabled using CNC Console and REST API.

Enable Using CNC Console

To enable this feature using CNC Console, enable **Enable Diameter Gateway Repaving** field on **Diameter Connection Repaving** page under **Diameter Configuration** on CNC Console.

For more information, see Diameter Repaving.

Enable Using REST API

To enable this feature using REST API, use Diameter Repaving API.

The URI to access the Diameter Repaving API is `{apiRoot}/oc-cnpolicy-configuration/v1/diameterRepaving/config`.

Configure

This feature can be configured using CNC Console and REST API.

Configure Using CNC Console

Configure the following advanced settings keys under **Settings** page for **Diameter Configurations** on CNC Console:

- DGW_CONNECTION_REPAVING.MAX_STAGGER_JITTER_MS
- DGW_CONNECTION_REPAVING.REINVOCATION_DELAY_MIN
- DGW_CONNECTION_REPAVING.CONNECTION_DISCONNECT_INTERVAL_MS
- DGW_CONNECTION_REPAVING.DPR_DELAY_MS
- DGW_CONNECTION_REPAVING.DPR_DISCONNECT_CAUSE

For more information, see Settings.

Configure Using REST API

This feature can be enabled and configured using the Diameter Repaving API.

Use the `{apiRoot}/oc-cnpolicy-configuration/v1/diameterRepaving/config` to configure the feature.

Use the `{apiRoot}/oc-cnpolicy-configuration/v1/diameterRepaving/triggerDisconnection` to disconnect the existing external Diameter connections established before the trigger timestamp.

Also, configure the following advanced settings keys on Diameter Settings API using the following URI: `{apiRoot}/oc-cnpolicy-configuration/v1/diameter/settings`:

- DGW_CONNECTION_REPAVING.MAX_STAGGER_JITTER_MS
- DGW_CONNECTION_REPAVING.REINVOCATION_DELAY_MIN

Copyright © 2019, 2026, Oracle and/or its affiliates.

- DGW_CONNECTION_REPAVING.CONNECTION_DISCONNECT_INTERVAL_MS
- DGW_CONNECTION_REPAVING.DPR_DELAY_MS
- DGW_CONNECTION_REPAVING.DPR_DISCONNECT_CAUSE

> **Note**
>
> The default repaving values in these advanced settings keys are likely implicit unless they are overridden.

Observability

Metrics

The `diam_repaving_disconnections_total` metric is to count the total number of connections terminated by the "force disconnect" mechanism. For more information, see Diameter Gateway Metrics.

> **Note**
>
> - The success of the re-balancing relies on the Layer-4 Load Balancer distributing new connection attempts effectively across the available pods after the disconnections occur. Common load balancing methods like "round robin" or "least connections" are expected to facilitate this re-balancing, assuming external clients promptly attempt to reconnect.
> - It is assumed that the external Diameter clients automatically attempt to reconnect following the forced disconnection. The success of the connection repaving relies on this client behavior, even if not all connections are immediately re-established due to varying client load or specific retry logic.
> - External monitoring tools, such as KPIs must be used to detect connection imbalance.
> - This feature is not autonomous and requires explicit operator intervention to initiate.
> - The solution's effectiveness requires the Diameter Gateway pods to be up and running. While it works effectively with direct load balancer-to-pod routing and is expected to work with service meshes like Istio with ASM sidecars (acting as TCP proxies), certain Kubernetes network configurations using kube-proxy might limit the overall re-balancing effectiveness. This is because each kube-proxy instance on different nodes can independently load balance connections across the Diameter Gateway pods, potentially leading to less predictable or less globally optimized connection distribution after the repaving process completes.
> - The disconnection action triggers the termination of all existing external inbound connections on each pod, rather than calculating a minimal, targeted number of connections to drop.

4.5 Optimizing Lookup in Binding Service Database

The Binding Service stores and retrieves subscriber session bindings that are used by network functions and gateways to route requests to the correct session owner.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The Binding service database stores subscriber session and context information in the following tables:

- `contextbinding`
- `dependentcontextbinding`

Indexed-key based searches are performed on the `contextBinding` table to locate subscriber binding information using the following indexed columns:

- ipv6Prefix
- ipv4Addr
- supi
- gpsi

As system traffic increased, the database experienced:

- Higher query latency
- Increased database CPU usage
- Full table scans during index-based lookups
- Reduced scalability for high-session deployments

Also, index-based queries were mainly used during the following operations:

- Session registration
- Session deregistration
- Context owner discovery
- Dependent context lookup

As part of this feature, Policy improves Binding Service database performance by replacing index-based lookups with more efficient lookup patterns:

- Converts index-key searches to primary-key or partition-key lookups.
- Stores frequently used keys such as `supi`, `gpsi`, `ipv4Addr`, and `ipv6Prefix` in separate index tables.
- Migrates data automatically during live traffic when the indexing is enabled.

Primary key and Partition key lookups are significantly faster than index-based searches and reduces database response time.

Reduced database overhead improves system responsiveness during peak traffic conditions.

Decreases index scanning operations lower database CPU utilization.

With this optimization, Binding Service can support higher subscriber and session volumes efficiently.

Context owner discovery and subscriber lookup operations can complete more quickly.

This optimization reduces database load, improves response time, and enhances scalability for large deployments.

The feature primarily affects the Binding Service and related context lookup operations used during session registration, deregistration, and context owner discovery.

Dedicated lookup tables are used for:

- SUPI lookup table (`supiindex`)

Copyright © 2019, 2026, Oracle and/or its affiliates.

- GPSI lookup table (`gpsiindex`)
- IPv4 lookup table (`ipv4index`)
- IPv6 lookup table (`ipv6index`)

These tables map frequently searched keys to `contextBindingId`, that are partitioned by index key (that is, for `supiindex` table, composite key is `supi` and `contextBindingId`, partitioned by `supi`), and use a composite key of index key and `contextBindingId`.

The Binding Service first searches the lookup table and then performs a primary-key lookup in the main binding table.

> **Note**
>
> - This feature applies only to signaling APIs of Binding Service.
> - Existing records are indexed through audit notifications, and new records are indexed during the normal registration flow.
> - All sites must be upgraded before query optimization is enabled.
> - Lookup tables must be fully synchronized before query optimization is enabled.

> **Important**
>
> Binding custom queries are shown only when Binding Service is enabled.

Upgrade and Rollback Impact

Before rolling back Policy to any of the previous versions, disable the following configurations:

- Disable Indexing
- Disable Query Optimization

For more information on these configurations, see Binding Service.

> **Note**
>
> If the rollback policy version does not support index tables, the entries in index tables needs to be clean up manually.

In case of Geo redundant deployment:

- The **Enable Query Optimization** field should only be enabled once all the sites are upgraded and all records are migrated properly. The status of the migration can be viewed from the **Custom Query** page under **Status and Query** on CNC Console.
- Disable both **Enable Query Optimization** and **Preferred Subscriber ID for Session Limit** fields before rolling back on all sites.
- For more information, see Binding Service.
- Once roll back operation is complete:
  - Manually clean the index table.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- System automatically switch back to the index-key based lookup.

Managing the Support for Optimizing Lookup in Binding Service Database

Enable

Support for Optimizing Lookup in Binding Service Database can be enabled using CNC Console as well as REST API.

Enable Using CNC Console

Enable **Enable Indexing** field under **Optimization** section on **Binding Service** page for **Service Configurations** on CNC console. For more information, see Binding Service.

Enable Using REST API

Configure the `enableIndexMigration` and `enableQueryOptimization` parameters under the `optimization` section in the Binding Service API payload.

Configure

Support for Optimizing Lookup in Binding Service Database can be configured using CNC Console as well as REST API.

Configure Using CNC Console

Configure the following fields under **Optimization** section on **Binding Service** page for **Service Configurations** on CNC console:

- Enable Indexing
- Enable Query Optimization
- Preferred Subscriber ID for Session Limit

For more information, see Binding Service.

On the **Custom Query** page under **Status and Query**, select `Binding Service` from the drop down list for **Select the service** field.

Select `Count of context bindings with contextBindingId not equal to contextId` as the value of **Select the query** field.

For more information, see Custom Query.

Configure Using REST API

Configure the following parameters under the `optimization` section in the Binding Service API payload:

- `enableIndexMigration`
- `enableQueryOptimization`
- `preferredSubscriberId`

Binding Service API can be accessed using the following URI: `{apiRoot}/oc-cnpolicy-configuration/v1/services/binding`.

For more information, see *Binding Service* section on *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

The following Binding Service metrics are used for this feature:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- occnp_binding_index_restore_total
- occnp_binding_index_total

For more information, see Binding Service Metrics.

4.6 Support for QoS Monitoring

This feature enhances the Policy Authorization service with QoS Monitoring functionality. It enables PCF to support AF subscription to QoS Monitoring and, based on that subscription, notify or report to the AF about packet delay between the UPF and RAN. This report can be used to address use cases such as SLA compliance, monitoring real-time QoS, and adapting content delivery based on the network conditions.

> **Note**
>
> It is assumed that the notification conditions provided in relation to QoS monitoring (such as notification method, reporting frequency, wait time) are enforced by UPF/SMF appropriately and notifications are issued accordingly. PCF only relays the notification or report to AF/NEF without checking if the conditions such as notification method, reporting frequency, or wait time are the same as requested.

> **Note**
>
> Currently, Policy supports:
>
> - QoS Monitoring subscription only as part of Npcf_PolicyAuthorization_Create procedure and conveying the QoS Monitoring data decision to SMF.
> - Currently, Policy does not support subscription through Npcf_PolicyAuthorization_Update procedures, and receipt of notification or reports from SMF through Npcf_SMPolicyControl_Update service operation.
> - Currently, Policy supports only the request for QoS Monitoring from AF/NEF through Policy Authorization service and the corresponding updateNotify call to SMF with the mapped QoS Monitoring data tied to certain PCC rules.
> - Currently, Policy does not support SMF notifications with `repPolicyCtrlReqTriggers=[QOS_MONITORING]` containing QoS Monitoring report information sent to PCF and is forwarded to AF/NEF.
> - UpdateNotify operation only supports instructing SMF to directly notify AF/NEF through `notifyUri`.
> - Currently, Policy supports Npcf_PolicyAuthorization_Delete operation to remove the corresponding PCC Rules from SMF and QoS Monitoring Data Decision. Rest of the functionality associated with delete shall continue as supported by PCF.

PCF receives requests from AF/NEF to subscribe to reporting of packet delay measurements for Service Data Flows (SDFs) through the Policy Authorization service (PA Create). The measurements cover UL (Uplink), DL (Downlink), and RT (Round-trip) delays.

Through PCF Policy Authorization service, AF/NEF sends a subscription request to get notifications when a delay takes place on the mentioned measurements for that specific application session.

Copyright © 2019, 2026, Oracle and/or its affiliates.

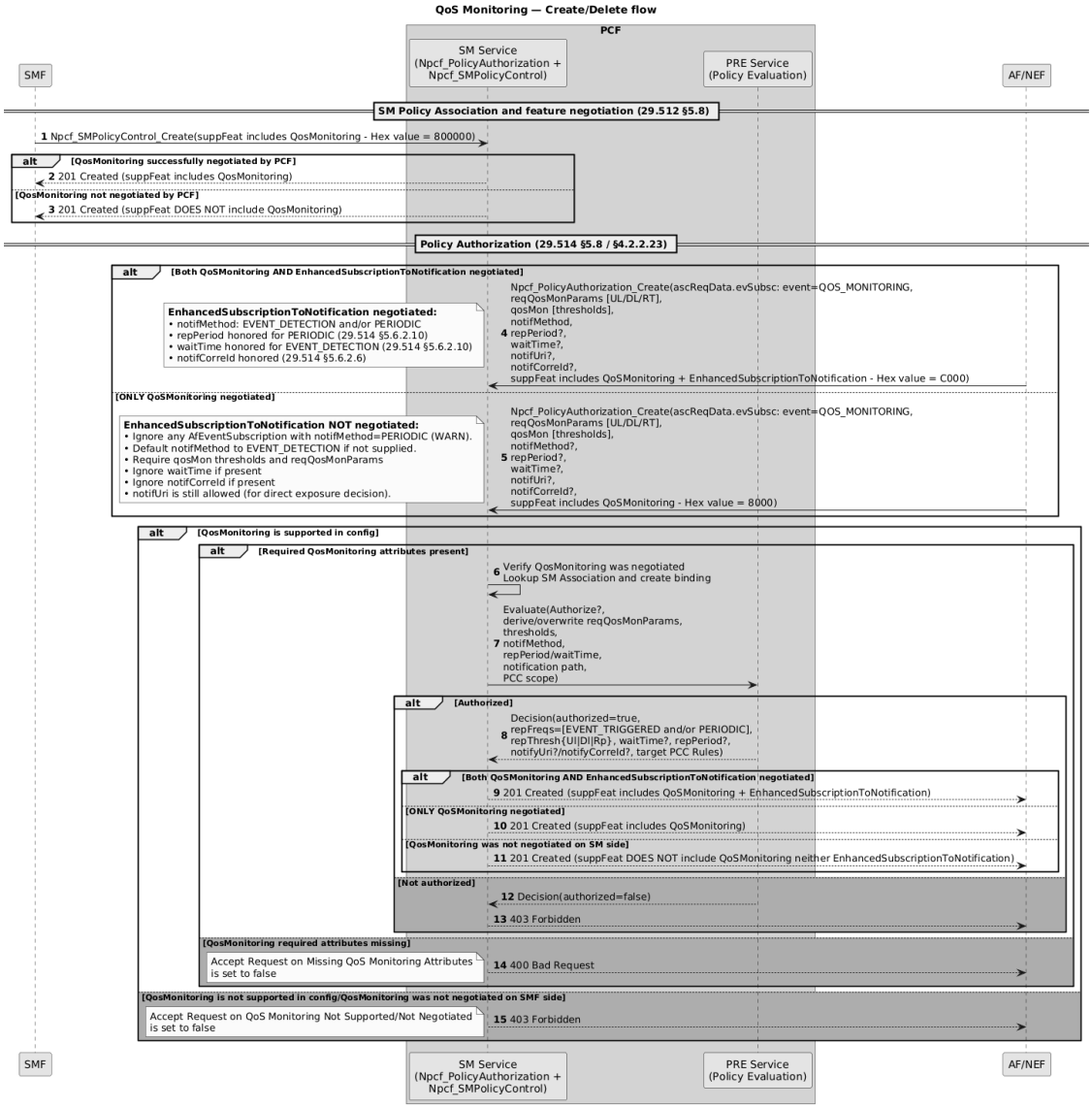
This feature is passed as event (`QOS_MONITORING`) in Policy Authorization operations (PA Create) alongside feature specific data.

Upon receiving a Policy Authorization operation with `QOS_MONITORING` request, PCF handles the QoS Monitoring data, maps it to the `SmPolicyDecision` data model, and ties it to certain PCC rules which are also part of the data model.

Call Flow

Feature Negotiation and Policy Authorization

Figure 4-7 Feature Negotiation and Policy Authorization



1. SM Policy association and feature negotiation:
   a. PCF receives `Npcf_SMPolicyControl_Create` request from SMF with `suppFeat` attribute indicating support for QoS Monitoring.

Copyright © 2019, 2026, Oracle and/or its affiliates.

b. PCF responds to SMF with 201 created message containing the list of negotiated features. If QoS Monitoring is negotiated by PCF, PCF response to SMF includes `suppFeat` attribute containing the `QoSMonitoring` in value.

2. Policy Authorization:
   a. PCF receives a `Npcf_PolicyAuthorization_Create` request from AF/NEF.
   b. When creating Policy Authorization for QoS Monitoring, PCF behavior differs depending on whether `EnhancedSubscriptionToNotification` is negotiated along with `QoSMonitoring`.
   c. If both `QoSMonitoring` and `EnhancedSubscriptionToNotification` are negotiated, PCF processes the Policy Authorization create request with:
      - `ascReqData.evSubsc.event = QOS_MONITORING`
      - `reqQosMonParams UL/DL/RT),qosMonThresholds`
      - Notification controls such as `notifMethod` (`EVENT_DETECTION` and/or `PERIODIC`), `repPeriod`, `waitTime`, `notifUri`, `notifCorreId`.
      - Response/feature indication: `suppFeat` includes `QoSMonitoring + EnhancedSubscriptionToNotification`.
   d. If only `QoSMonitoring` is negotiated (`EnhancedSubscriptionToNotification` not negotiated), PCF requests QoS Monitoring with reduced or adjusted notification handling, such as:
      - Default `notifMethod` to `EVENT_DETECTION` if not provided.
      - Require thresholds and `reqQosMonParams`.
      - Ignore or avoid `PERIODIC-only` subscription semantics (warn), ignore `waitTime/notifCorreId` if present.
      - `notifUri` may still be allowed.
      - Response or feature indication includes `suppFeat` attribute containing `QoSMonitoring` only.
3. PCF validation and Policy evaluation.
   a. PCF verifies that `QoSMonitoring` feature is negotiated, looks up for SM association, and creates session binding.
   b. The SM service in PCF interacts with PRE service to perform policy evaluation, and derives or overrides:
      - requested QoS Monitoring parameters and thresholds
      - notification method (event/periodic), reporting period, wait time
      - notification path and PCC scope/target PCC rules
   c. PRE returns a decision:
      - If `authorized=true`: returns reporting configuration (event-triggered and/or periodic) and optional `notifyUri/notifCorreId` plus target PCC rules.
      - If `authorized=false`: decision indicates not authorized.
4. PCF responds to AF/NEF with 201 Created containing `suppFeat` attribute depending on the feature negotiation:
   - If `QoSMonitoring` and `EnhancedSubscriptionToNotification` are negotiated, the response includes both the features.

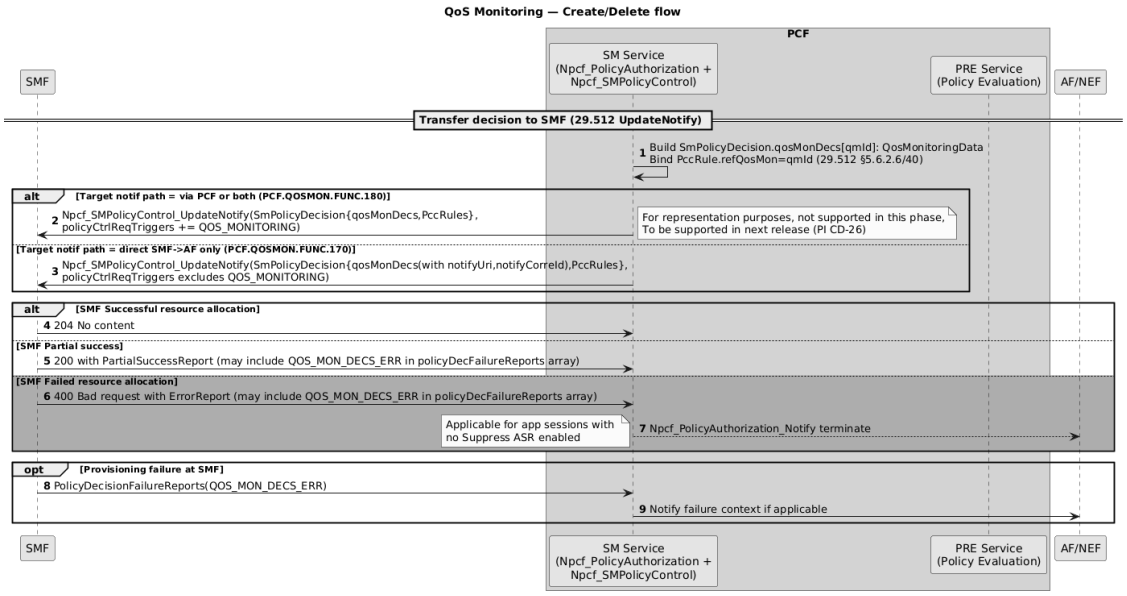
Copyright © 2019, 2026, Oracle and/or its affiliates.

- If only `QoSMonitoring` is negotiated, the response includes `QoSMonitoring`.
- If `QoSMonitoring` is not negotiated on SM service, the response does not include `QoSMonitoring` or `EnhancedSubscriptionToNotification`.

5. If PCF does not authorize the feature, it returns 403 Forbidden response to AF/NEF.
6. If required `QoSMonitoring` attributes are missing and `accept request on missing attributes` is `false`, PCF responds to AF/NEF with 400 Bad Request.
7. If `QoSMonitoring` is not supported in configuration or not negotiated on SMF and `accept request on not supported/not negotiated` is `false`, PCF responds to AF/NEF with `403 Forbidden` error.

QoS Monitoring - Transfer Decision to SMF

Figure 4-8 QoS Monitoring - Transfer Decision to SMF



1. PCF builds `SmPolicyDecision.qosMonDecs[...] (QoSMonitoringData)` and binds `PccRule.refQosMon = qmId`.
2. PCF sends a request to SMF with `Npcf_SMPolicyControl_UpdateNotify(...)` including PCC rules.
   a. If target notification path is through PCF: UpdateNotify includes `QOS_MONITORING` triggers.

   > **Note**
   >
   > Currently, notification path through PCF is not supported. Call flow and details added just for representation purpose.

   b. If target notification path is direct SMF to AF, the UpdateNotify is sent but policy control request triggers exclude `QOS_MONITORING`.
3. SMF responds to PCF with resource allocation:

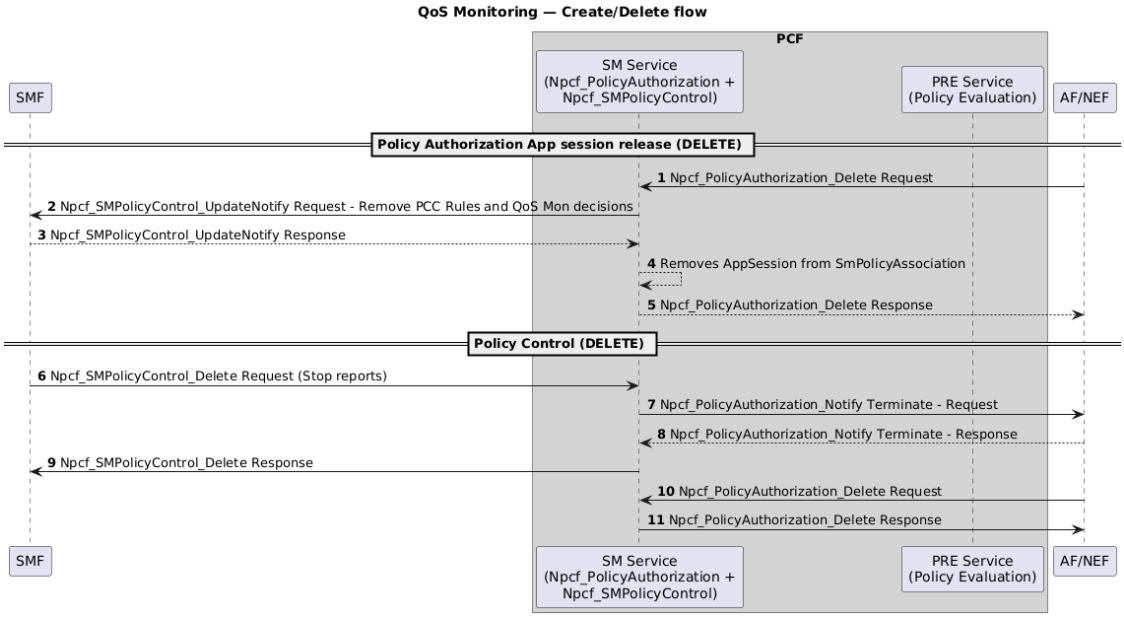
Copyright © 2019, 2026, Oracle and/or its affiliates.

- 204 No Content on successful allocation.
- 200 OK with `PartialSuccessReport` can include `QOS_MON_DECS_ERR` in `policyDecFailureReports`.
- 400 Bad Request with `ErrorReport` can include `QOS_MON_DECS_ERR` in `policyDecFailureReports`.

4. If applicable, PCF terminates the PolicyAuthorization notify interaction.
5. Optional failure reporting: In case of provisioning failure at SMF, failure reports are produced and failure context is notified (as applicable).

Policy Authorization Application Session Release and Policy Control Delete

Figure 4-9 Policy Authorization Application Session Release and Policy Control Delete



1. Policy Authorization Application Session Release (DELETE).
   a. PCF receives a `Npcf_PolicyAuthorization_Delete` request from AF/NEF to release the application session.
   b. PCF sends a `Npcf_SMPolicyControl_UpdateNotify` request to remove PCC rules and QoS Monitoring decisions.
   c. PCF receives a response from SMF to `Npcf_SMPolicyControl_UpdateNotify` request.
   d. PCF removes `AppSession` from the `SmPolicyAssociation`.
   e. PCF responds to AF/NEF.
2. Policy Control Delete (Stop QoS Monitoring Reports).
   a. PCF receives a `Npcf_SMPolicyControl_Delete` request from SMF to stop the reports.
   b. PCF sends a `Npcf_PolicyAuthorization_NotifyTerminate` request to AF/NEF and receives a response.
   c. PCF responds to SMF for `Npcf_SMPolicyControl_Delete` request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

d. PCF receives a `Npcf_PolicyAuthorization_Delete` request from AF/NEF and responds on the same.

Managing Support for QoS Monitoring

Enable and Configure
This feature can be enabled and configured using CNC Console as well as REST API.

Configure Using CNC Console

Add **QoSMonitoring** to **Override Supported Features** field under **System** section on **PCF Session Management** page in CNC Console.

Configure **QosMon Notification Target** field under **QoS Monitoring Configuration** section on **PCF Session Management** page on CNC Console.

For more information, see PCF Session Management.

Add **QoSMonitoring** and **EnhancedSubscriptionToNotification** to **Override Supported Features** field under **System** section on **PCF Policy Authorization** page on CNC Console.

Configure the following parameters under **QoS Monitoring** section on **PCF Policy Authorization** page on CNC Console:

- Accept Request on Missing QoS Monitoring Attributes
- Accept Request on QoS Monitoring Not Supported/Not Negotiated

For more information, see PCF Policy Authorization.

Enable and Configure Using REST API

Add `QoSMonitoring` as one of the values of `overrideSupportedFeatures` parameter under `System` section in `PCF Session Management Service` API.

Add `QoSMonitoring` and `EnhancedSubscriptionToNotification` as values of `overrideSupportedFeatures` parameter under `System` section in `PCF Policy Authorization Service` API.

For more information, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Blockly configuration
Use the following blockly under **Policy Projects** on CNC Console to configure QoS Monitoring functionality:

- Policy Trigger
- AF/NEF request contains supported feature
- attribute in AF request
- Install PCC Rules
- Apply PCC Rule Profile to flow
- Override QosMon Attributes
- QoSMon attribute override value
- QoSMon notification target
- Reject Session With Error Code And Error Cause

For more information, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide.*

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observability

Metrics

The following metrics are used for this feature:

- occnp_pa_qosmon_request_total
- occnp_pa_qosmon_response_total
- occnp_sm_qosmon_update_notify_sent_total
- occnp_sm_qosmon_decs_error_total

For more information, see PA Service Metrics and SM Service Metrics.

Alerts

The following alerts are used for this feature:

- QOS_MON_FAILED_AUTH_ABOVE_MINOR_PERCENT
- QOS_MON_FAILED_AUTH_ABOVE_MAJOR_PERCENT
- QOS_MON_FAILED_AUTH_ABOVE_CRITICAL_PERCENT
- QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MINOR_PERCENT
- QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MAJOR_PERCENT
- QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT
- QOS_MON_MISSING_ATTRIBUTES_ABOVE_MINOR_PERCENT
- QOS_MON_MISSING_ATTRIBUTES_ABOVE_MAJOR_PERCENT
- QOS_MON_MISSING_ATTRIBUTES_ABOVE_CRITICAL_PERCENT

For more information, see PCF Alerts.

Logging

ERROR/WARN logs are introduced for:

- The authorization fails
- When required QoS Monitoring attributes are not received from AF
- Indication of Policy decision errors due to QoS Monitoring decision policy such as QOS_MON_DECS_ERR

Format of the logs are in compliant with the feature `Error response log enhancement`.

4.7 Optimize Database Lookup in SM Service

The Optimize Database Lookup in SM Service feature improves PCF capacity per instance by reducing the storage footprint, database load, database replication, and latency in the SM Service. This feature optimizes how SM Service persists and retrieves session data as follows:

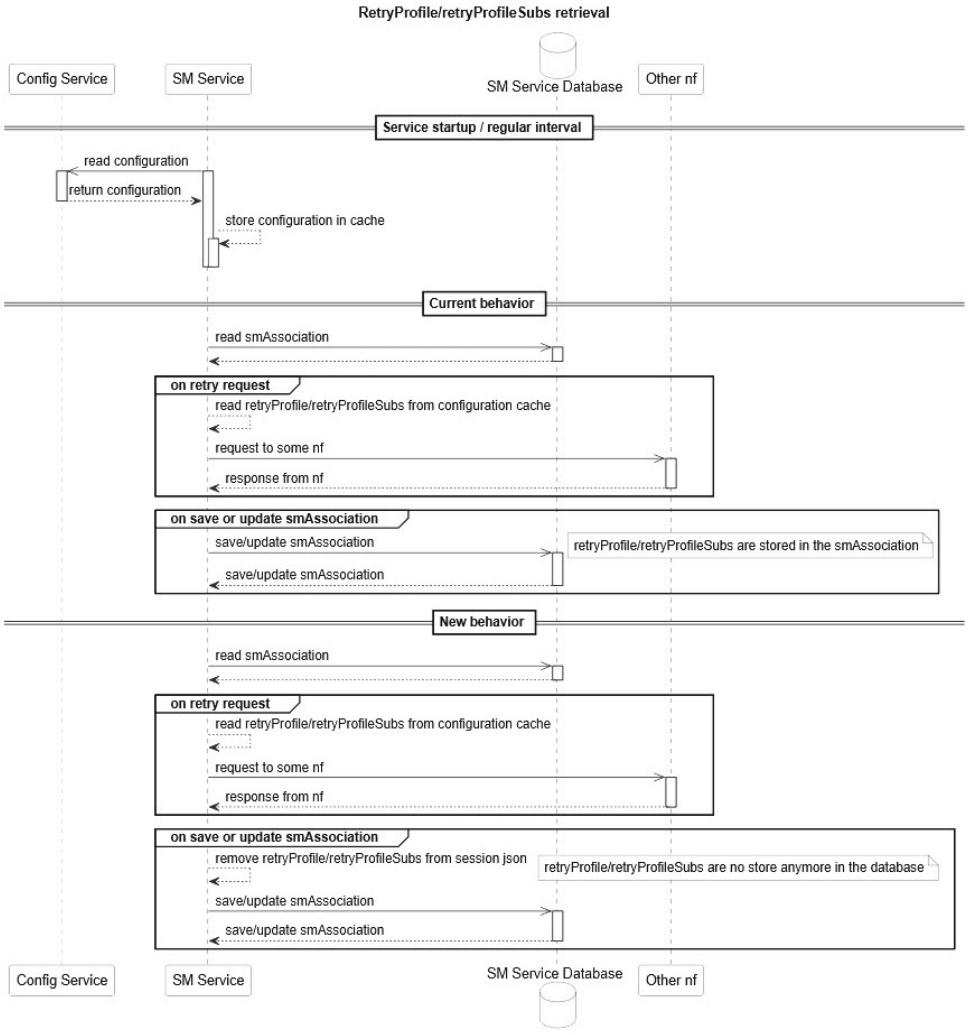
- Makes `dependentContextbinding` creation and deletion conditional for PCF deployments.
- The `dependentContextbinding` processing is controlled by deployment mode and the `BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` flag.
- The `BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` feature flag is used to controls whether Rx AAR-I/STR flows create or delete `dependentContextbinding` records in the Binding Service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Omits null attributes from persisted session JSON.
- Removes `retryProfile` and `retryProfileSubs` from persisted session JSON.
- Retrieves retryProfile and retryProfileSubs at runtime from an in-memory cache that is loaded from configuration.
- Existing non-null session data is preserved.
- Older records that contain `retryProfile` or `retryProfileSubs` are read successfully.

These changes help reduce database read and write payload size, reduce replication overhead, and improve runtime performance.

Figure 4-10 Retrieve retryProfile and retryProfileSubs Call Flow



This call flow shows how SM Service changes from storing retry profile data in session JSON to retrieving the data from configuration cache at runtime. At service startup, or at a regular interval, SM Service reads configuration from Config Service. After Config Service returns the configuration, SM Service stores the configuration in an in-memory cache. This cache becomes the runtime source for `retryProfile` and `retryProfileSubs`.

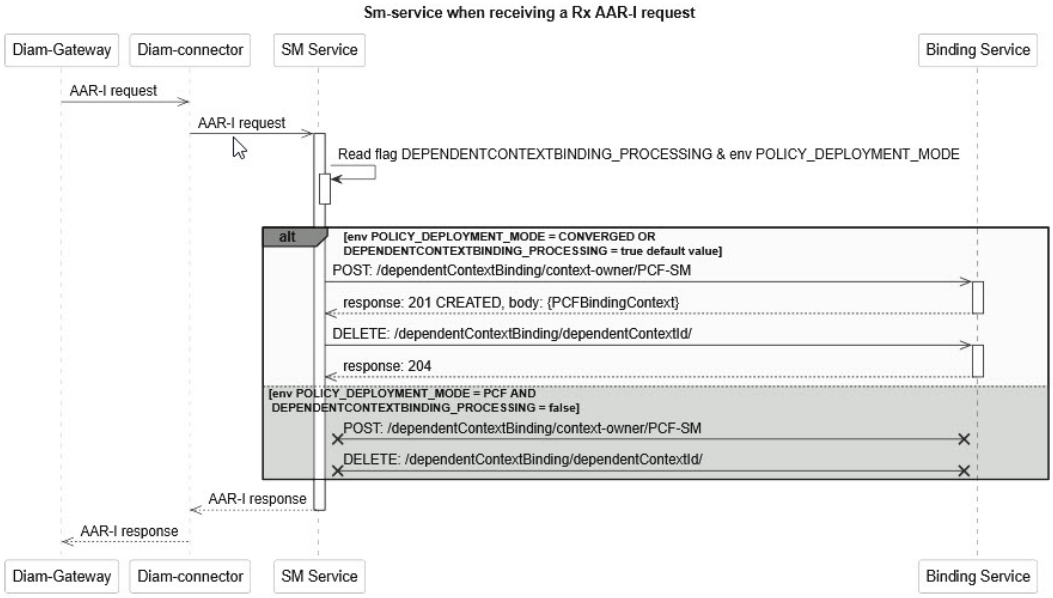
Copyright © 2019, 2026, Oracle and/or its affiliates.

In the current behavior section of the call flow, SM Service reads the `smAssociation` record from the SM Service database. When a retry request occurs, SM Service reads `retryProfile` and `retryProfileSubs` from the configuration cache and uses those values to send a request to another network function. However, when SM Service saves or updates the `smAssociation`, the retry profile data is still stored in the `smAssociation` session JSON in the database.

In the new behavior section, SM Service still reads the `smAssociation` record from the database and still retrieves `retryProfile` and `retryProfileSubs` from the configuration cache when a retry request occurs. The change happens during save or update of the `smAssociation`. SM Service removes `retryProfile` and `retryProfileSubs` from the session JSON before persisting the record. As a result, those values are no longer stored in the database.

Older records that still contain `retryProfile` or `retryProfileSubs` can be read, but SM Service ignores those values. On the next write, SM Service persists the session JSON without those fields. The main benefit is that the database stores smaller session JSON payloads. SM Service can continue to use retry profile data for business logic, but the data comes from the configuration cache instead of being repeatedly stored in every session record.

Figure 4-11 Config-driven dependentContextBinding Processing Call Flow



This call flow shows how SM Service decides whether to create or delete `dependentContextBinding` records when it receives an Rx AAR-I request. The request starts at Diameter Gateway, passes through Diameter connector, and reaches SM Service as an AAR-I request. After receiving the request, SM Service reads two values:

- `DEPENDENTCONTEXTBINDING_PROCESSING`
- `env POLICY_DEPLOYMENT_MODE`

These values determine whether SM Service calls Binding Service to create or delete `dependentContextBinding` records. This behavior is controlled by the `BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` flag and the policy deployment mode. The default value of the flag is true, which preserves legacy behavior.

When Binding Processing Is Performed

Copyright © 2019, 2026, Oracle and/or its affiliates.

SM Service performs the legacy create and delete operations when either of the following conditions is true:

- `POLICY_DEPLOYMENT_MODE=CONVERGED`
- `DEPENDENTCONTEXTBINDING_PROCESSING=true`

In this path, SM Service sends a POST request to Binding Service `POST: /dependentContextBinding/context-owner/PCF-SM` and the Binding Service returns `201 CREATED` with a `PCFBindingContext` response body.

SM Service can also send a delete request `DELETE: /dependentContextBinding/dependentContextId` and the Binding Service returns `204`. This path keeps the existing behavior for converged deployments and for PCF deployments where the flag remains enabled.

When Binding Processing Is Skipped

SM Service skips `dependentContextBinding` creation and deletion only when both of the following conditions are true:

- `POLICY_DEPLOYMENT_MODE=PCF`
- `DEPENDENTCONTEXTBINDING_PROCESSING=false`

In this path, the diagram marks the POST and DELETE calls with an X. This means SM Service does not call Binding Service for those operations. SM Service continues processing the Rx AAR-I request and returns the AAR-I response through Diam-connector to Diam-Gateway.

The following table describes `dependentContextBinding` processing behavior.

Table 4-1 Policy Deployment Mode

Policy Deployment Mode	`BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` Parameter	`dependentContextBinding` processing
Converged	`false`	Create and delete as legacy behavior
Converged	`true`	Create and delete as legacy behavior
PCF	`true`	Create and delete as legacy behavior
PCF	`false`	Skip creation and deletion

Managing Optimize Database Lookup in SM Service

Enable

This feature can be enabled using CNC Console:

This feature can be enabled by setting the `BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` parameter to **false** under Advanced Settings in **PCF Session Management** section in CNC Console. The default value is **true**. For more information, see PCF Session Management.

Observability

- **Metrics**

  The following metrics are added to support this feature:

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - `occnp_dependentContextBinding_processing_total`

  For more information, see Binding Service Metrics.

- There are no new KPIs or alerts available for this feature.

Logging

SM Service logs indicate whether `dependentContextBinding` records are created or skipped as follows.

- When `BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` parameter is set as false in PCF deployment mode, SM Service logs that `dependentContextBinding` creation or deletion is skipped.
  For example, `"level": "DEBUG", "message": "Skip create dependentContextBinding due to BINDING.DEPENDENTCONTEXTBINDING_PROCESSING flag is false for binding request {...}."`
- When `BINDING.DEPENDENTCONTEXTBINDING_PROCESSING` parameter is set as true in PCF deployment mode, SM Service logs that `dependentContextBinding` creation or deletion is processed.
  For example, `"level": "DEBUG", "message": "Create dependentContextBinding due to BINDING.DEPENDENTCONTEXTBINDING_PROCESSING flag is true for binding request {...}."`

4.8 Support for SBI Message Priority Header

PCF supports 3GPP-SBI-Message-Priority header in order to enable overload and congestion control through informed throttling decisions.

Using 3GPP-SBI-Message-Priority header, PCF and the associated producers and consumers such as UDR, CHF, SMF, AF, BSF, and NRF can distinguish between high-priority and low-priority Service-Based Interface (SBI) messages.

PCF includes 3GPP-SBI-Message-Priority header in requests and responses, which is used to specify the HTTP/2 message priority for 3GPP SBI interfaces.

The 3GPP-SBI-Message-Priority header specifies HTTP/2 message priority values ranging from 0 (highest) to 31 (lowest). Integrating this header enables priority-based processing of both Ingress and Egress HTTP/2 SBI messages.

> **Note**
>
> The mapping of Message Priofile with the default configuration by PRE happens before the congestion control mechanism.

Use Cases:

- Setting 3GPP-SBI-Message-Priority in the requests (inbound and outbound), success and error responses (inbound requests).
- Setting 3GPP-SBI-Message-Priority for outbound requests which can be used by intermediate NF's such as SCP to make use of their overload and congestion control mechanisms.

PCF supports sending and receiving 3GPP-SBI-Message-Priority header for the following SBI interfaces:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- PCF as a consumer can send 3GPP-SBI-Message-Priority header in the following requests:
  - PCF to UDR
  - PCF to CHF
  - PCF to BSF
  - PCF to AF/NEF
- PCF as a notification producer or client can send 3GPP-SBI-Message-Priority header in the following call flows:
  - PCF to SMF for SM services
  - PCF AF/NEF for PA service
- PCF as a producer supports receiving and sending the 3GPP-SBI-Message-Priority header with appropriate values in the response:
  - SMF to PCF for SM services
  - AF/NEF to PCF for PA service
- PCF as a notification consumer supports receiving the 3GPP-SBI-Message-Priority header in the notification request and sending the header with appropriate values in the Response:
  - UDR to PCF for SM services

> **Note**
>
> Currently, PCF supports only Session Management call flows.
>
> Currently, PCF does not support SCP Health Check HTTP options.

The following tables depict the supported Message Type and priorities for each interface:

Table 4-2 Npcf_SMPolicyControl

Message type/ operation type	Request direction	HTTP method	Set priority via configuration		Set priority via policy	
			Request	Response	Request	Response
Create	SMF → PCF	POST	Yes	Yes	No	Yes
Update	SMF → PCF	POST	Yes	Yes	No	Yes
Delete	SMF → PCF	POST	Yes	Yes	No	Yes
Update_Notify	PCF → SMF	POST	Yes	No	Yes[1]	No
Terminate_Notify	PCF → SMF	POST	Yes	No	Yes[1]	No

[1] For the messages marked with priority value **1**, priority cannot be set through policy when the message is triggered by Audit or Session Viewer APIs.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-3 Npcf_PolicyAuthorization

Message type/ operation type	Request direction	HTTP method	Set priority via configuration		Set priority via policy	
			Request	Response	Request	Response
Create	AF → PCF	POST	Yes	Yes	No	Yes
Update	AF → PCF	PATCH	Yes	Yes	No	Yes
Delete	AF → PCF	POST	Yes	Yes	No	No
Subscribe	AF → PCF	POST	Yes	Yes	No	No
Unsubscribe	AF → PCF	POST	Yes	Yes	No	No
Update_Notify	PCF → AF	POST	Yes	No	Yes[1]	No
Terminate_Notify	PCF → AF	POST	Yes	No	No	No

Table 4-4 Nudr_DataRepository

Message type/ operation type	Request direction	HTTP method	Set priority via configuration		Set priority via policy	
			Request	Response	Request	Response
Get_Policy_Data	PCF → UDR	GET	Yes	No	No	No
Subscribe	PCF → UDR	POST	Yes	No	No	No
Resubscribe	PCF → UDR	PUT	Yes	No	No	No
Unsubscribe	PCF → UDR	DELETE	Yes	No	Yes	No
Lookup_Subscription	PCF → UDR	GET	Yes	No	No	No
Patch_Policy_Data	PCF → UDR	PATCH	Yes	No	Yes	No
Policy_Data_Change_Notify	UDR → PCF	POST	Yes	Yes	No	No

Table 4-5 Nchf_SpendingLimitControl

Message type/ operation type	Request direction	HTTP method	Set priority via configuration		Set priority via policy	
			Request	Response	Request	Response
Subscribe	PCF → CHF	POST	Yes	No	Yes	No
Update_Subscription	PCF → CHF	PUT	Yes	No	Yes	No
Unsubscribe	PCF → CHF	DELETE	Yes	No	Yes	No
Update_Notify	CHF → PCF	POST	Yes	Yes	No	No
Terminate_Notify	CHF → PCF	POST	Yes	Yes	No	No

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-6 Nbsf_Management

Message type/ operation type	Request direction	HTTP method	Set priority via configuration		Set priority via policy	
			Request	Response	Request	Response
Register	PCF → BSF	POST	Yes	No	Yes[1]	No
Deregister	PCF → BSF	DELETE	Yes	No	Yes	No

Table 4-7 Npcf_Binding_Audit

Message type/ operation type	Request direction	HTTP method	Set priority via configuration		Set priority via policy	
			Request	Response	Request	Response
Audit_Notify	BSF → PCF	POST	Yes	Yes	No	No

In certain deployments, SM service disables the **Include S-NSSAI in User Query** and **Include DNN in User Query** settings in the service configuration. When these options are turned off, User Service does not receive the DNN and S-NSSAI values.

To address this, the custom SBI priority attributes uses oc-message-priority header. The oc-message-priority header carry the configured DNN and SNSSAI ids set by SM service, and is forwarded to the connectors (UDR/BSF) where these values are extracted and sent to the RuleEngine.

When a request or response contains a `oc-message-priority` header, the custom message priority defined in the header takes precedence over the default configuration.

For details on the different Message Types, for different attributes such as DNN, S-NSSAI, 3GPP-SBI-Message-prioirty, and oc-message-priority for each service type, see *Message Attributes Supported for Different Service Types and Interface Types* in Message Profiles.

The following table shows the default message priority assigned for different operation types for each service or interface type that Policy currently supports:

Table 4-8 Default Priorities

Interface Name	Message Type/ Operation Type	Default Request Priority	Default Response Priority
Npcf_SMPolicyControl	Create	24	23
	Update	18	17
	Delete	16	15
	Update_Notify	18	NA
	Terminate_Notify	18	NA
Npcf_PolicyAuthorization	Create	24	23
	Update	18	17
	Delete	16	15
	Subscribe	18	17
	Unsubscribe	18	17

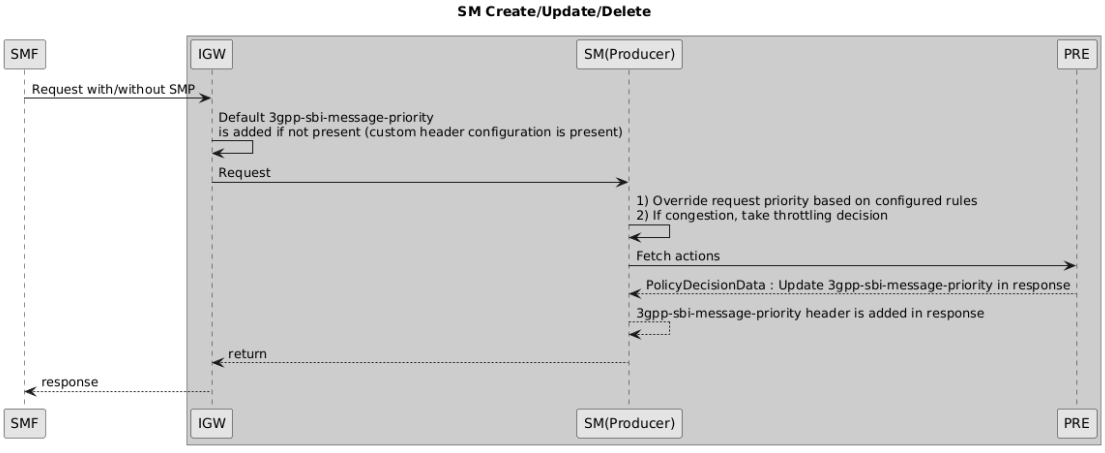
Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-8 (Cont.) Default Priorities

Interface Name	Message Type/ Operation Type	Default Request Priority	Default Response Priority
	Update_Notify	18	NA
	Terminate_Notify	18	NA
Nudr_DataRepository	Get_Policy_Data	22	NA
	Subscribe	24	NA
	Resubscribe	22	NA
	Unsubscribe	23	NA
	Patch_Policy_Data	23	NA
	Policy_Data_Change_Notify	18	17
	Lookup_subscription	22	NA
Nchf_SpendingLimitControl	Subscribe	24	NA
	Update_Subscription	23	NA
	Unsubscribe	22	NA
	Update_Notify	18	17
	Terminate_Notify	18	17
Nbsf_Management	Register	24	NA
	Deregister	23	NA
Npcf_Binding_Audit	Audit_Notify	18	17

Call Flow

Figure 4-12 SM as Producer (SM Create/Update/Delete)



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-13 SM as Producer- N5(AF), N30(NEF) Npcf_PolicyAuthorization Services

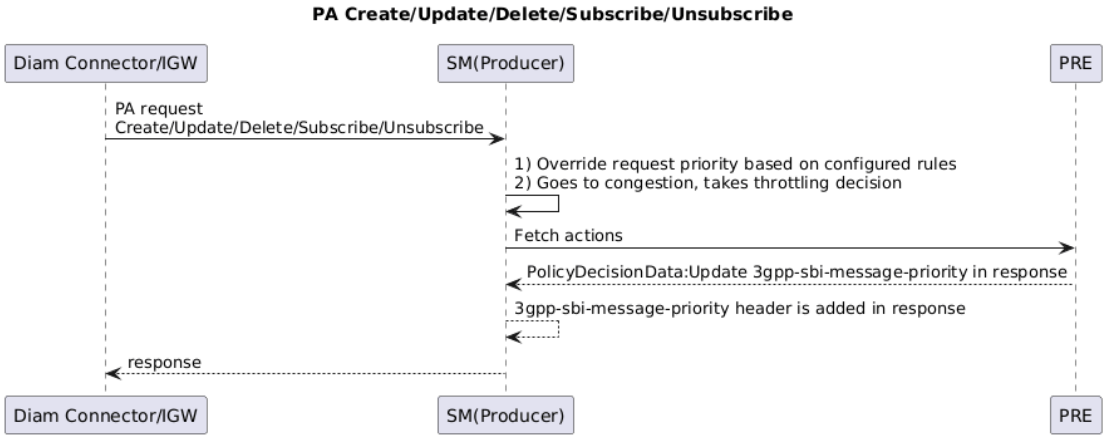
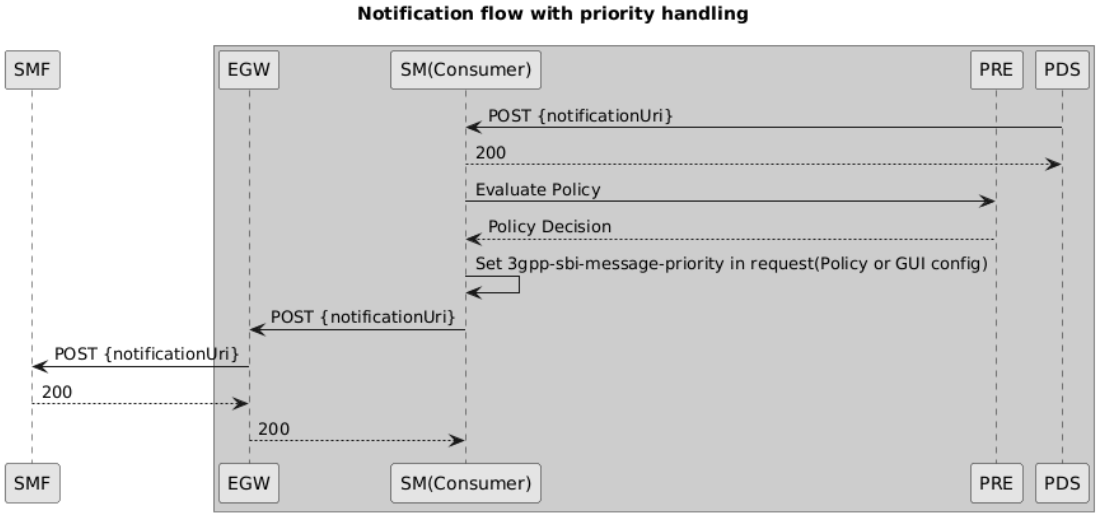


Figure 4-14 SM as Consumer Notification flow with priority handling



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-15 SM as Consumer Notification flow with PA Create/Update

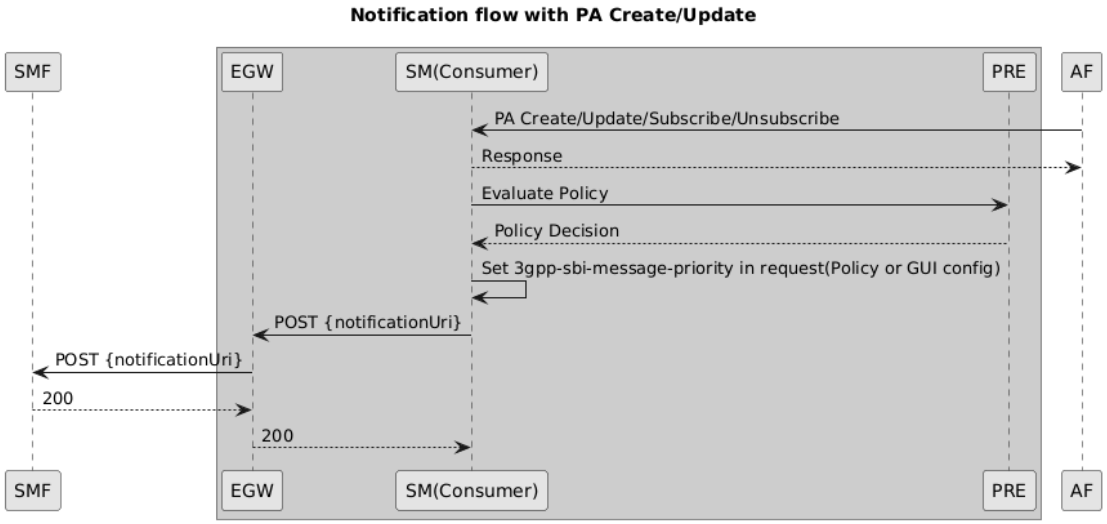
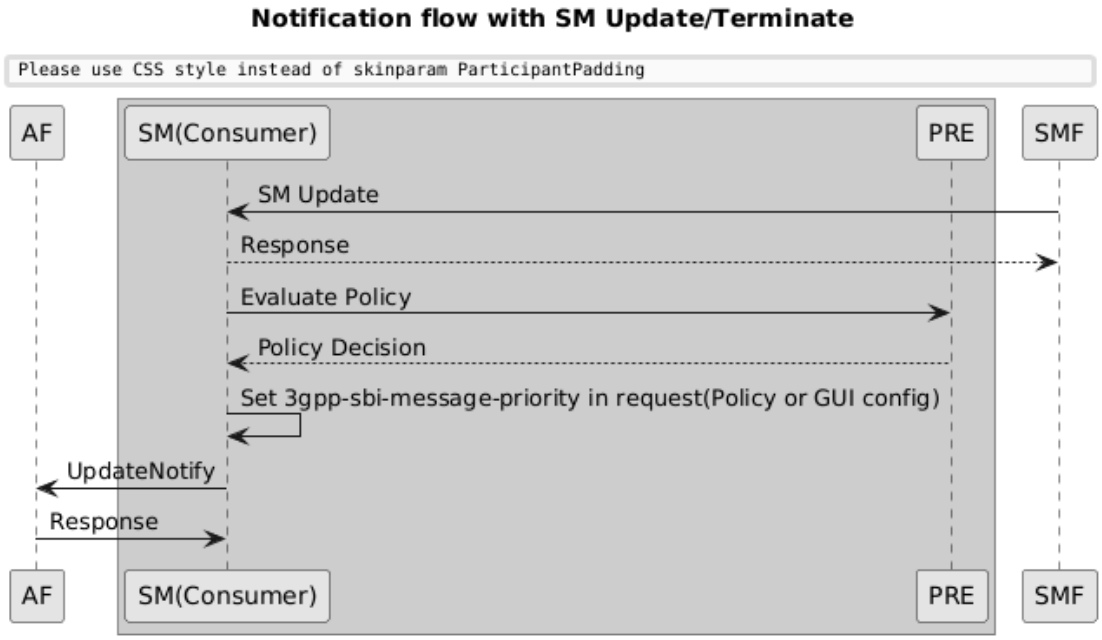


Figure 4-16 SM as Consumer Notification flow with SM Update/Terminate



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-17 SM to Binding Register Request

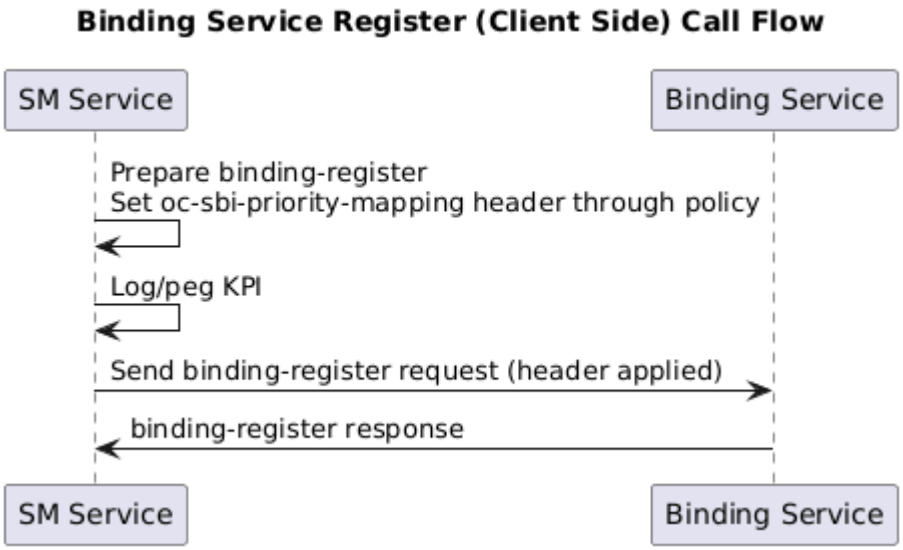
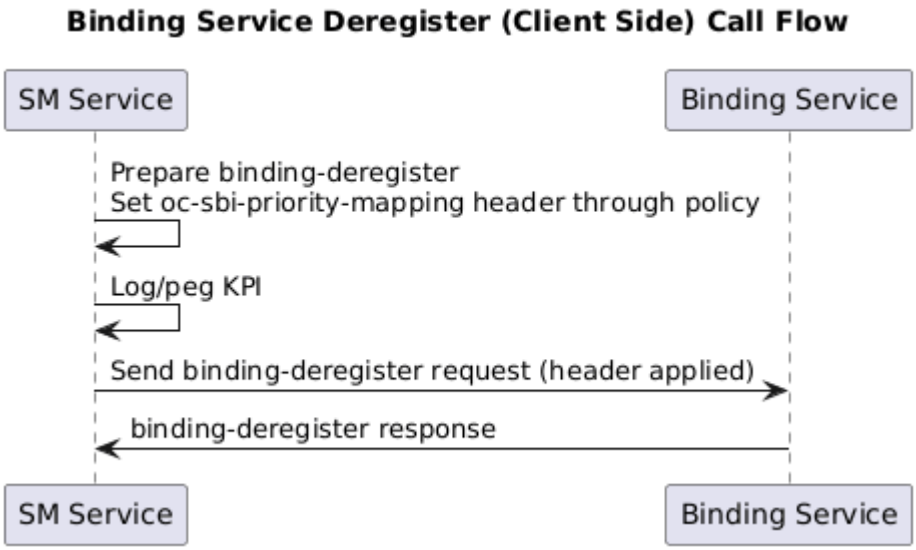


Figure 4-18 SM to Binding Deregister Request



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-19 SM to Binding Update Request

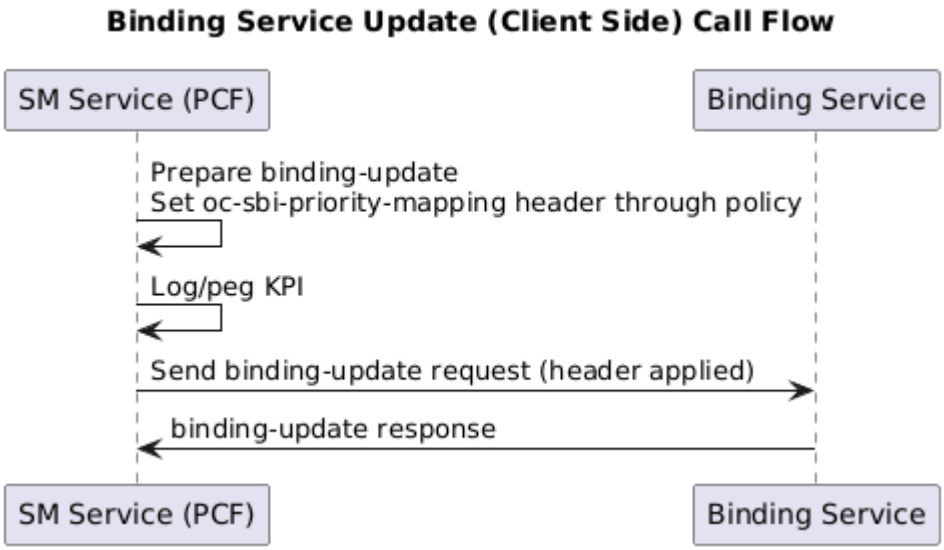
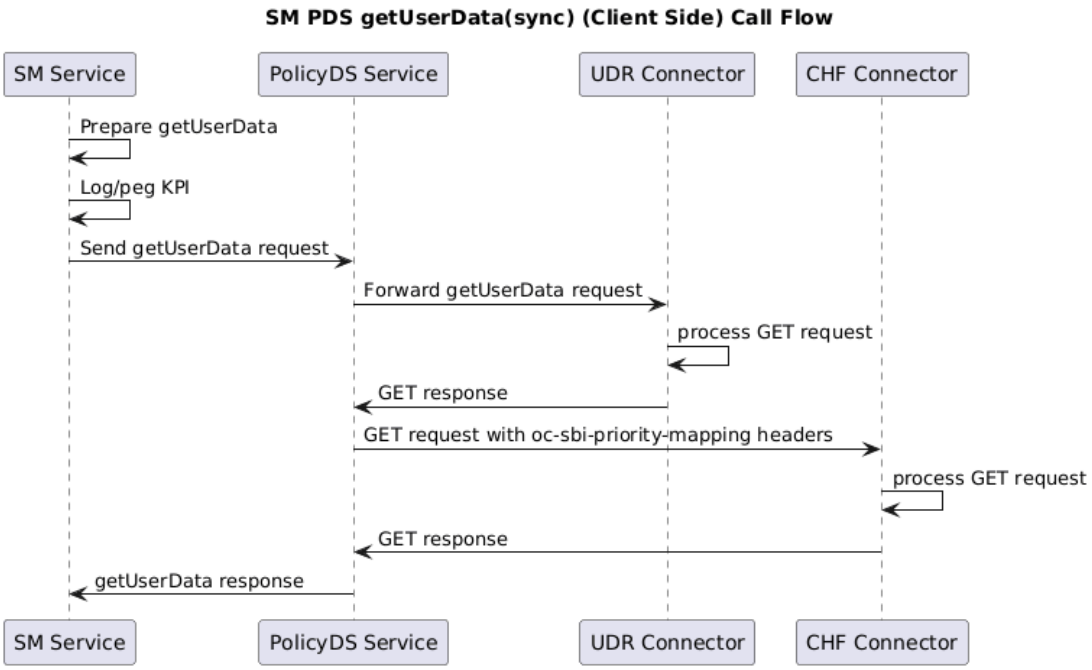


Figure 4-20 SM to PDS (getSpendingLimit sync): There will be no policy evaluation for assigning priority



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-21 SM to PDS (getSpendingLimit async): Policy Evaluation will happen in SM to decide whether to trigger getSpendingLimit request or not

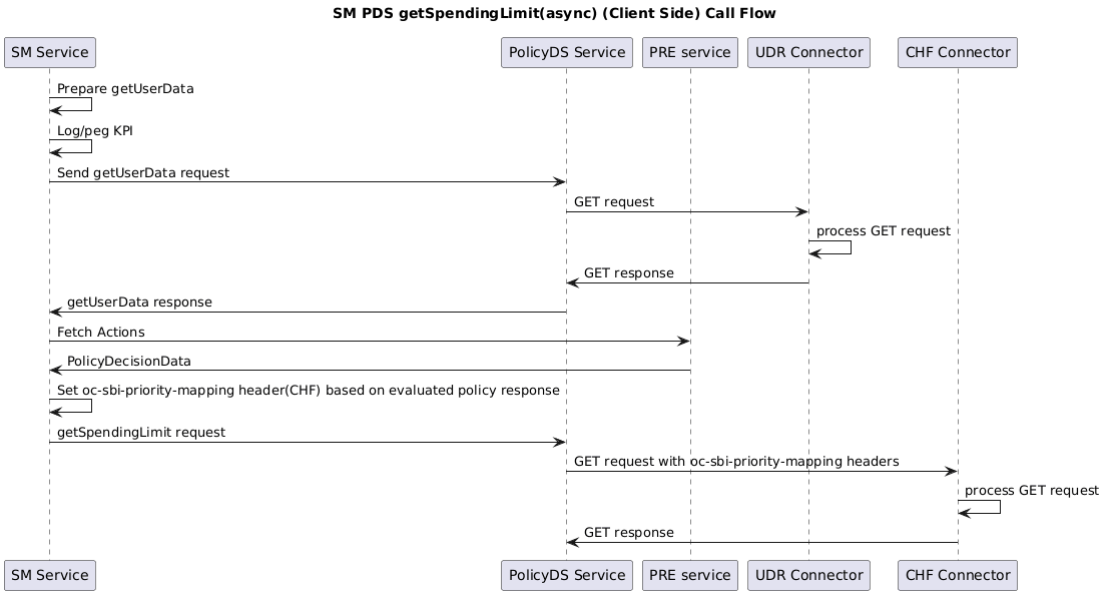
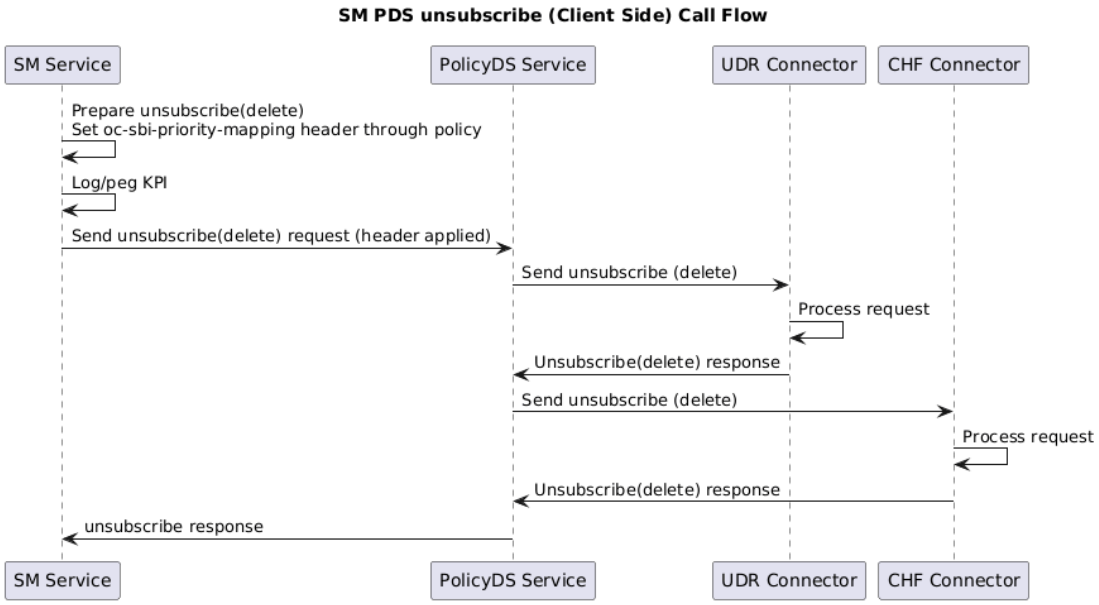


Figure 4-22 SM to PDS (Unsubscribe)



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-23 SM to PDS (updateSSV) : patch nudr

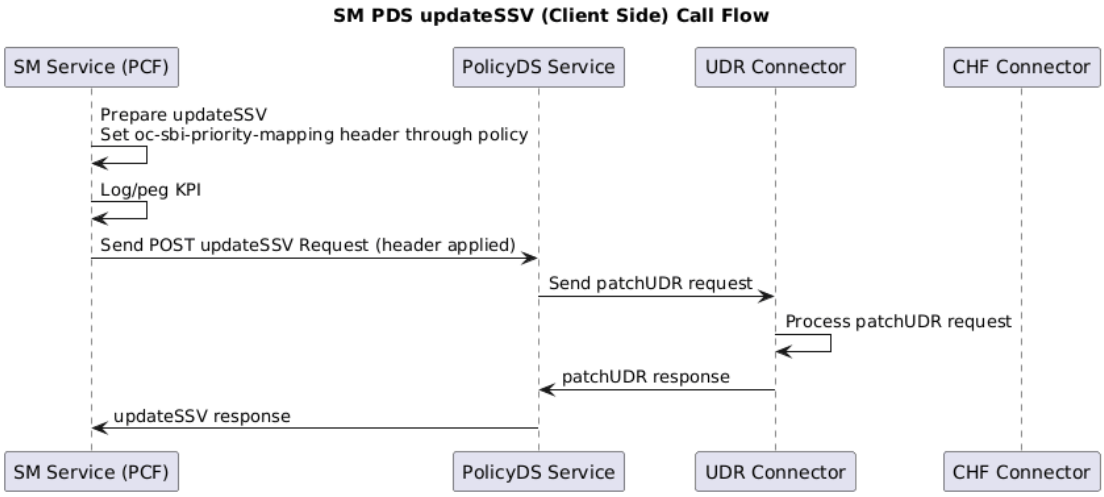
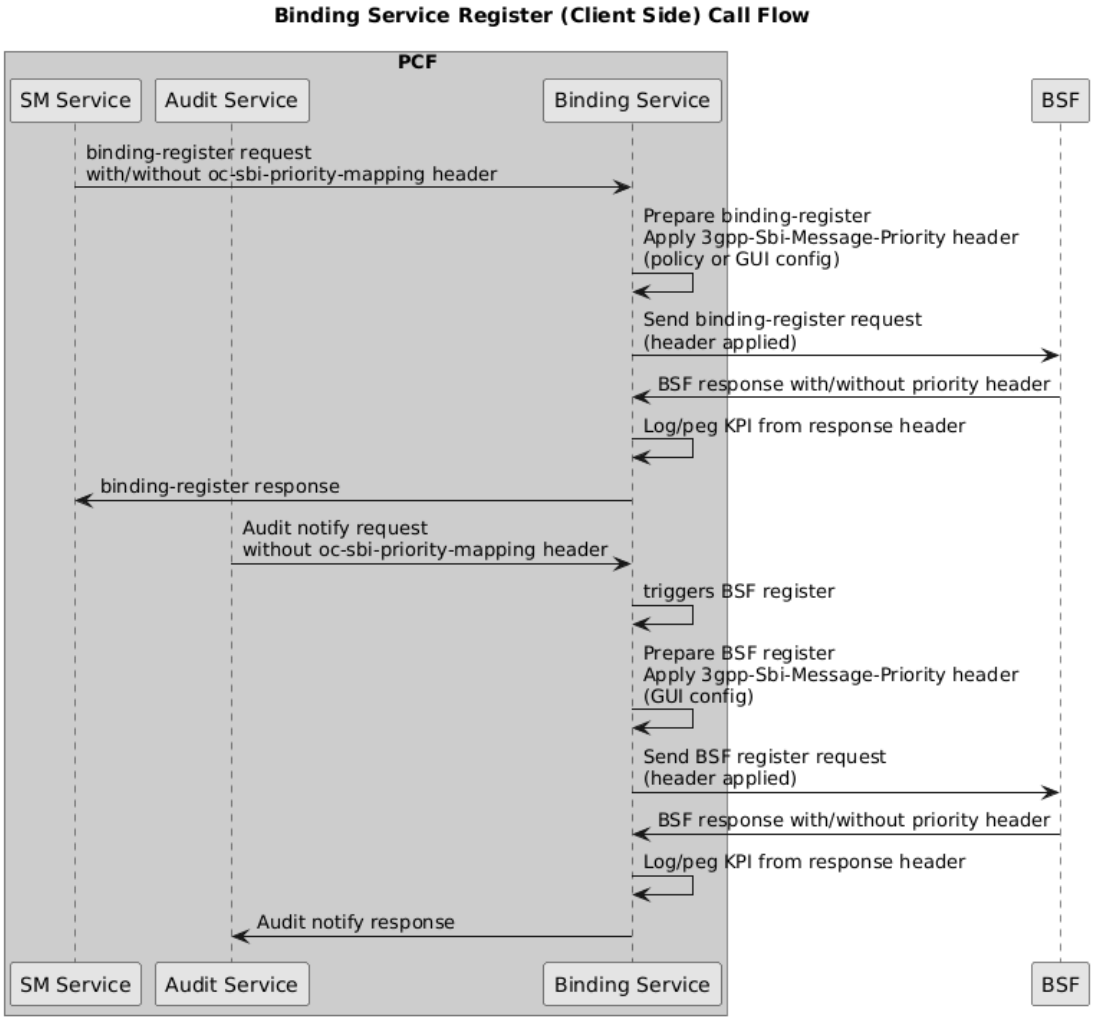


Figure 4-24 Binding Service Register



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-25 Binding Service Deregister

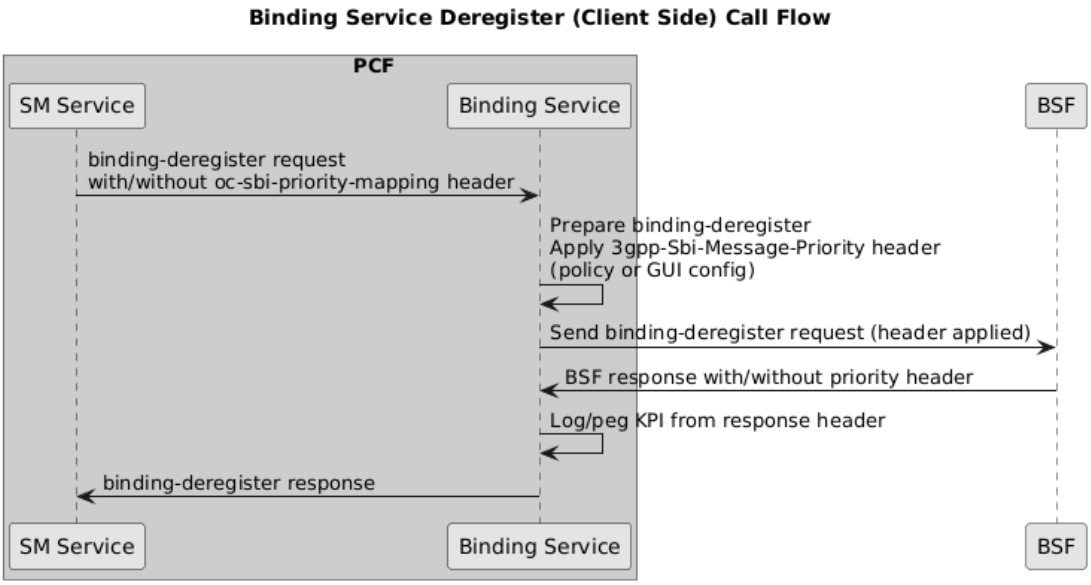
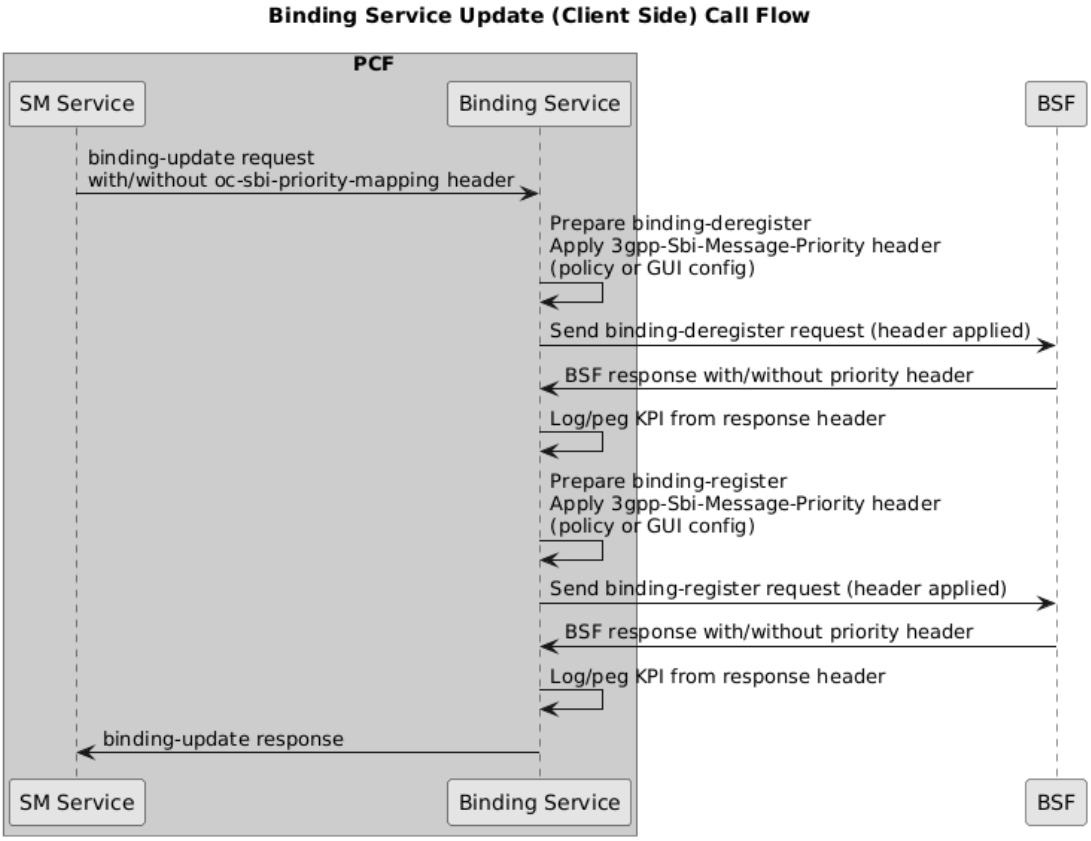


Figure 4-26 Binding Service Update



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-27 Binding as producer-Stale session validate

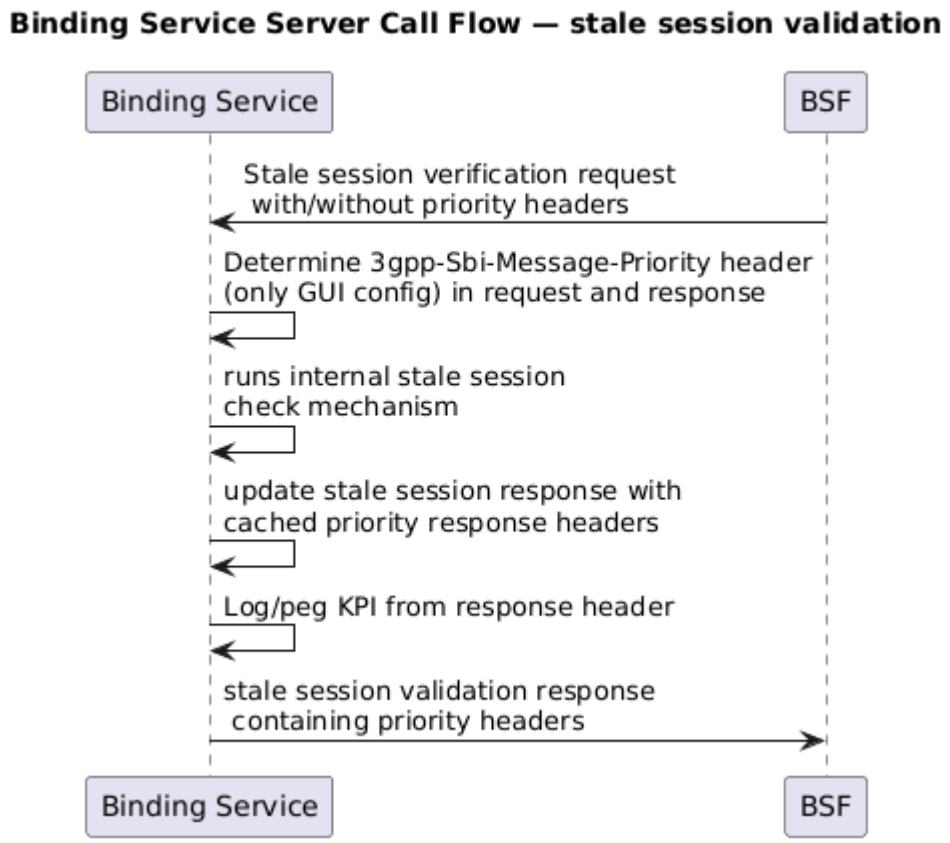
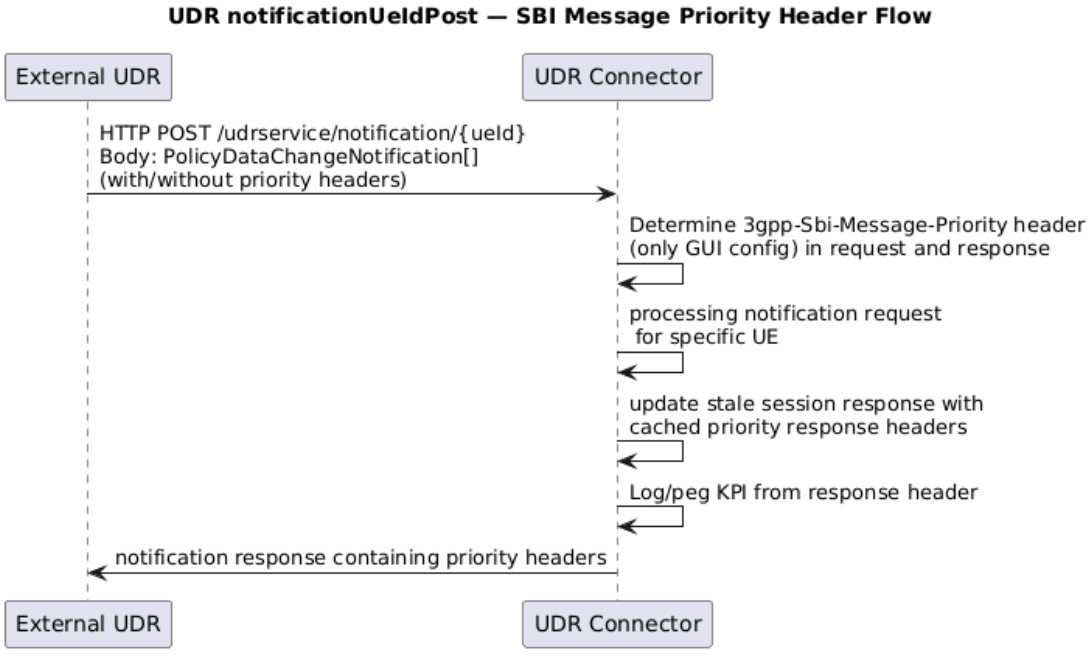


Figure 4-28 UDR-Connector as Producer-UDR notificationUeIdPost



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-29 UDR Connector as Consumer-UDR userDataUeIdListGet

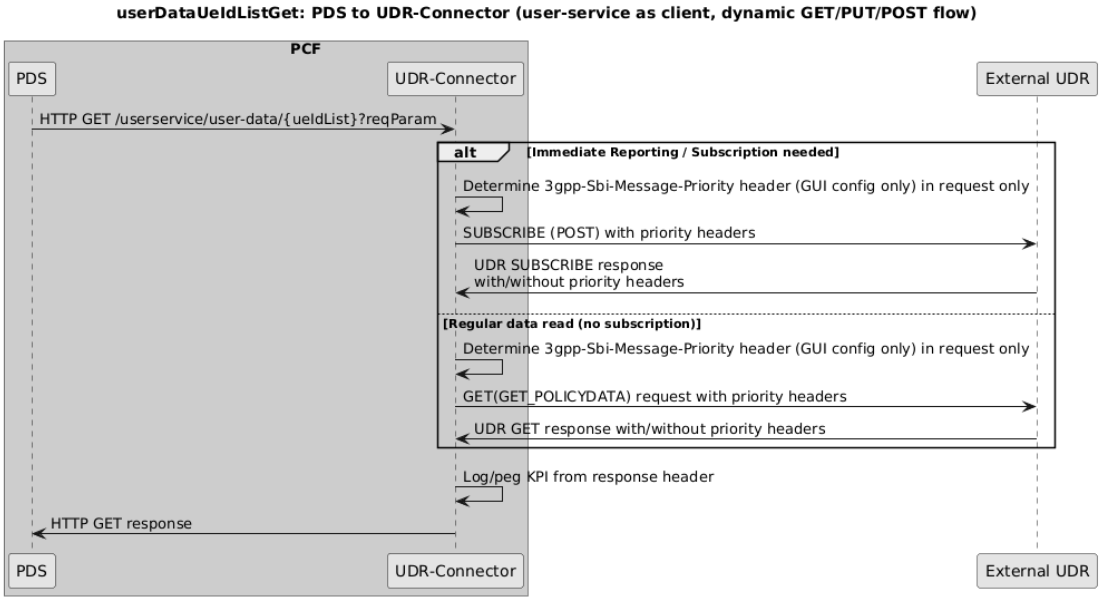


Figure 4-30 UDC Connector as Consumer-UDR userDataUeIdListPatch

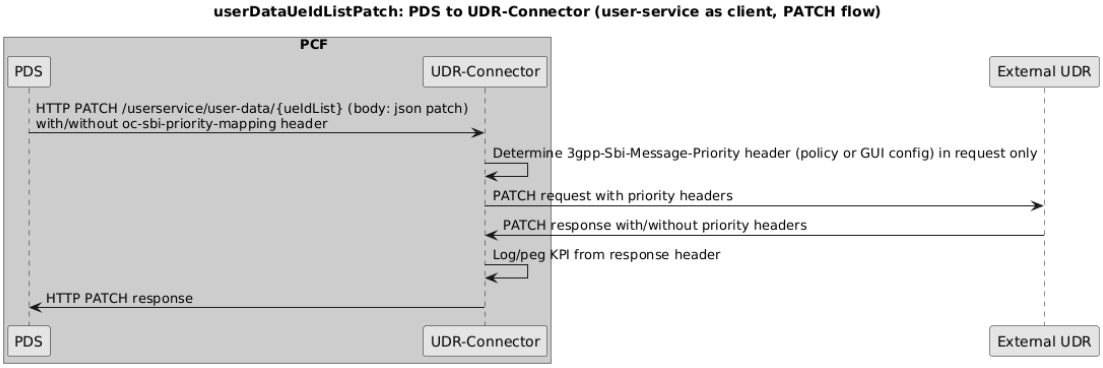
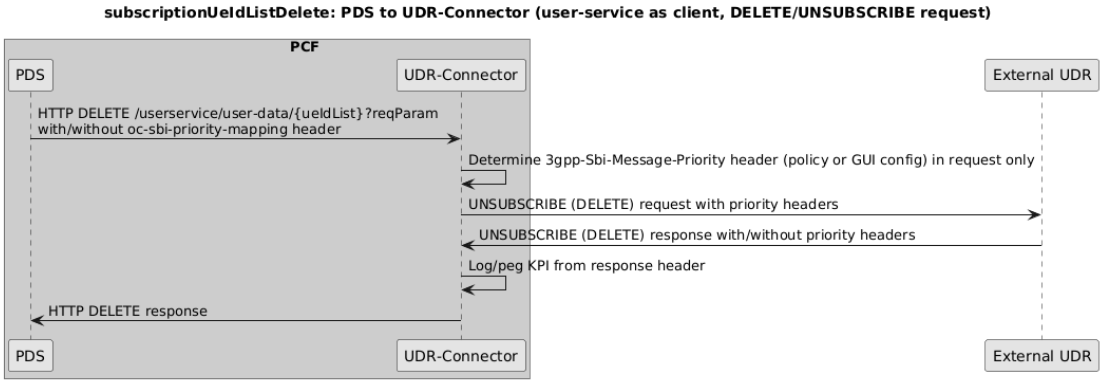


Figure 4-31 UDR Connector as Consumer-UDR subscriptionUeIdListDelete



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-32 UDR Connector as Consumer-UDR subsToNotifyUeIdListPost

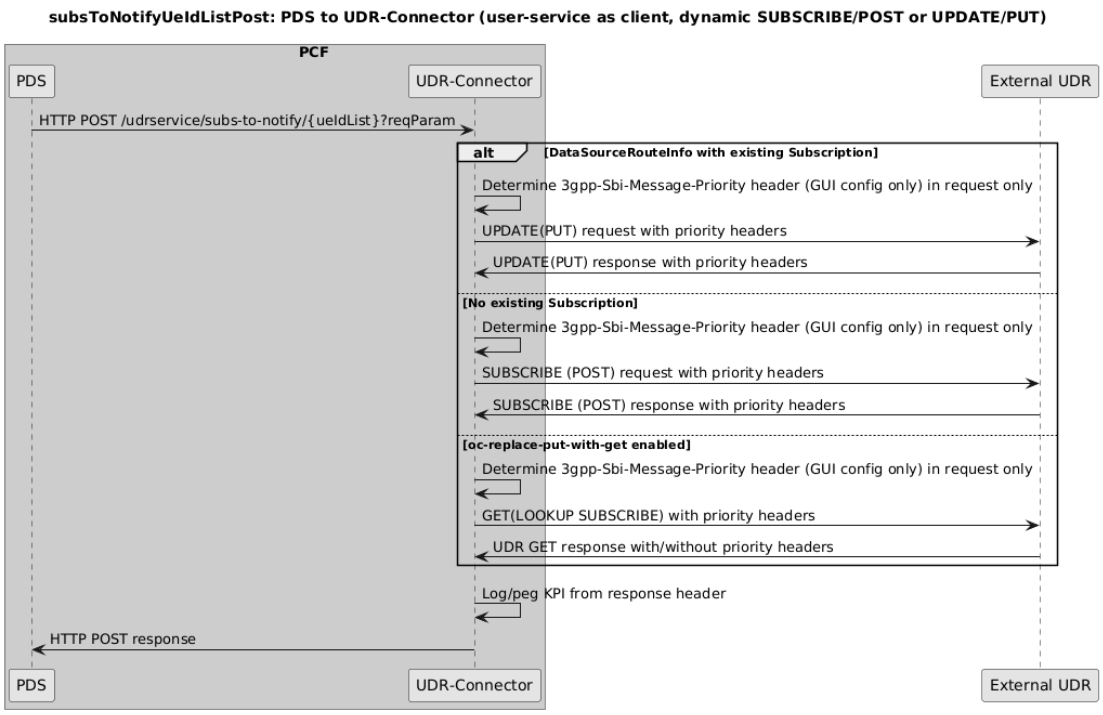
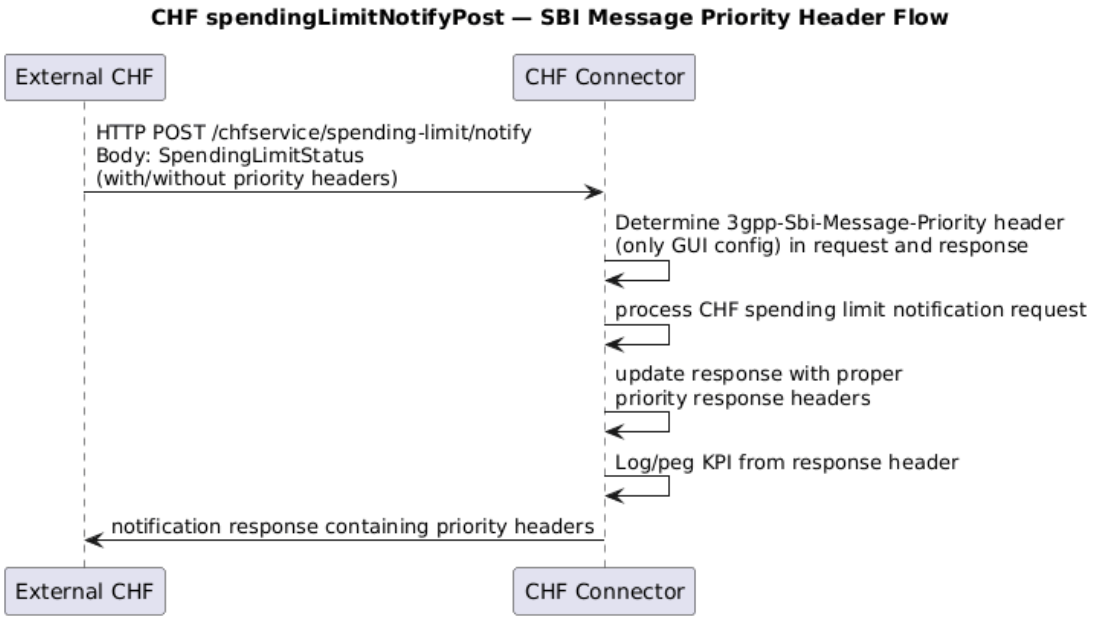


Figure 4-33 CHF Connector as Producer-CHF spendingLimitNotifyPost



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-34 CHF Connector as Producer - CHF spendingLimitTerminatePost

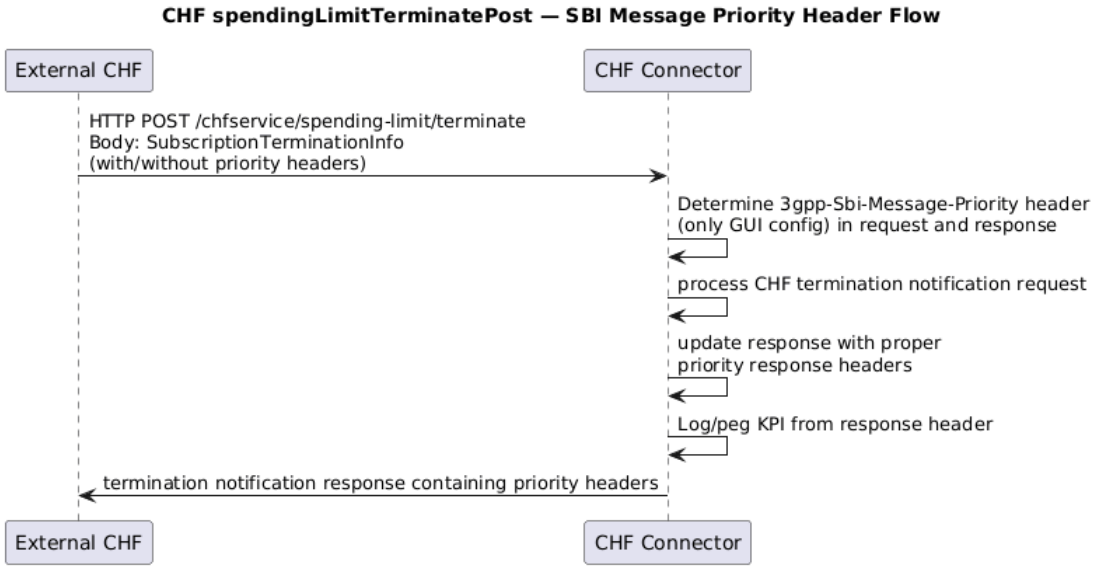
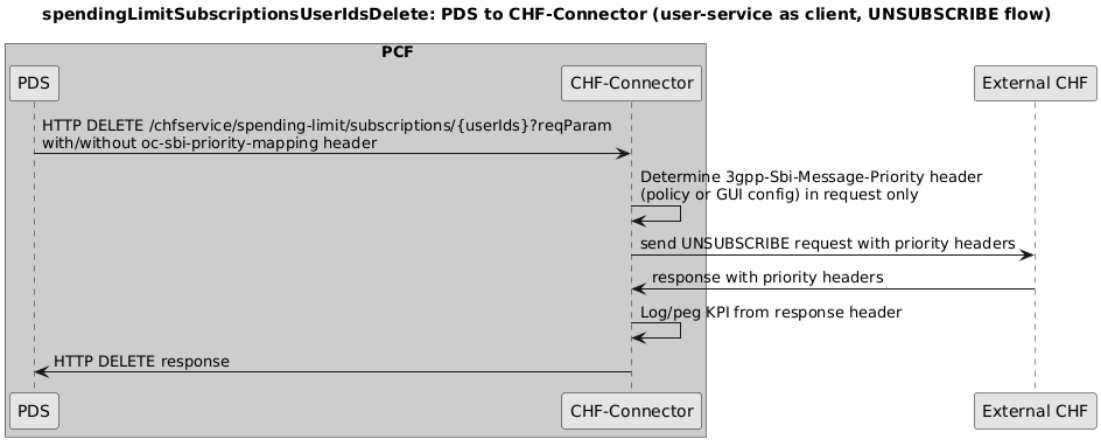
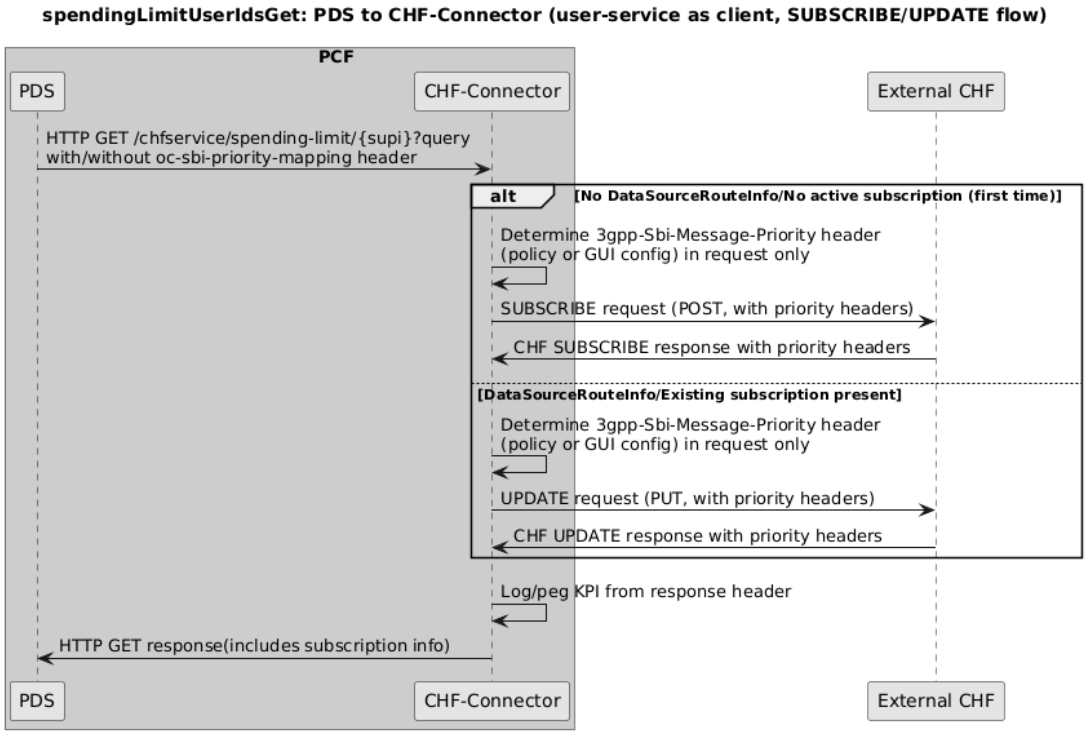


Figure 4-35 CHF Connector as Consumer - CHF spendingLimitSubscriptionsUserIdsDelete



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-36 CHF Connector as Consumer - CHF spendingLimitUserIdsGet



Possible Combination of Incoming Priorities

Below table lists possible combinations of the incoming (original) priorities in two headers:

- 3GPP-SBI-Message-Priority
- oc-message-priority

It depicts what happens to the original 3GPP-SBI-Message-Priority and the original oc-message-priority when the message profile is active or inactive for client and server requests.

It also shows two observable metrics:

- rcvd_priority: what was originally received in 3GPP-SBI-Message-Priority
- eval_priority: final priority to be considered for that request. That is, eval_priority is assigned to the oc-message-priority during server request and the same is applied to 3GPP-SBI-Message-Priority during client request.

Table 4-9 Possible Combination of Incoming Priorities with Sample Values of 3GPP-SBI-Message-Priority and oc-message-priority

Original 3GPP-SBI-Message-Priority Header/ Original oc-message-priority Header	msg-profile	client/ server	filter action	3GPP-SBI-Message-Priority/oc-message-priority	rcvd_priority/ eval_priority
12/NA	inactive	server	no change	12/NA	12/12

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-9 (Cont.) Possible Combination of Incoming Priorities with Sample Values of 3GPP-SBI-Message-Priority and oc-message-priority

Original 3GPP-SBI-Message-Priority Header/ Original oc-message-priority Header	msg-profile	client/ server	filter action	3GPP-SBI-Message-Priority/oc-message-priority	rcvd_priority/ eval_priority
NA/10	inactive	server	no change	NA/10	NA/10
12/10	inactive	server	no change	12/10	12/10
NA/NA	inactive	server	no change	NA/NA	NA/NA
12/NA	no matching rule	server	no change	12/NA	12/12
NA/10	no matching rule	server	no change	NA/10	NA/10
12/10	no matching rule	server	no change	12/10	12/10
NA/NA	no matching rule	server	no change	NA/NA	NA/NA
12/NA	rule action -> always(8)	server	insert OMP as 8	12/8	12/8
NA/10	rule action -> always(8)	server	update OMP from 10 to 8	NA/8	NA/8
12/10	rule action -> always(8)	server	update OMP from 10 to 8	12/8	12/8
NA/NA	rule action -> always(8)	server	insert OMP as 8	NA/8	NA/8
12/NA	rule action -> If not present(8)	server	insert OMP as 12	12/12	12/12
NA/10	rule action -> If not present(8)	server	no change	NA/10	NA/10
12/10	rule action -> If not present(8)	server	no change	12/10	12/10
NA/NA	rule action -> If not present(8)	server	insert OMP as 8	NA/8	NA/8
12/NA	rule action -> Never	server	insert OMP as 12	12/12	12/12
NA/10	rule action -> Never	server	no change	NA/10	NA/10
12/10	rule action -> Never	server	no change	12/10	12/10
NA/NA	rule action -> Never	server	no change	NA/NA	NA/NA
12/NA	inactive	client	don't send TGPP	NA/NA	12/NA
NA/10	inactive	client	don't send TGPP	NA/NA	NA/NA
12/10	inactive	client	don't send TGPP	NA/NA	12/NA
NA/NA	inactive	client	don't send TGPP	NA/NA	NA/NA
12/NA	no matching rule	client	don't send TGPP	NA/NA	12/NA
NA/10	no matching rule	client	don't send TGPP	NA/NA	NA/NA
12/10	no matching rule	client	don't send TGPP	NA/NA	12/NA
NA/NA	no matching rule	client	don't send TGPP	NA/NA	NA/NA
12/NA	rule action -> always(8)	client	update TGPP from 12 to 8	8/NA	12/8

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-9 (Cont.) Possible Combination of Incoming Priorities with Sample Values of 3GPP-SBI-Message-Priority and oc-message-priority

Original 3GPP-SBI-Message-Priority Header/ Original oc-message-priority Header	msg-profile	client/ server	filter action	3GPP-SBI-Message-Priority/oc-message-priority	rcvd_priority/ eval_priority
NA/10	rule action -> always(8)	client	insert TGPP as 8	8/NA	NA/8
12/10	rule action -> always(8)	client	update TGPP from 12 to 8	8/NA	12/8
NA/NA	rule action -> always(8)	client	insert TGPP as 8	8/NA	NA/8
12/NA	rule action -> If not present(8)	client	no change	12/NA	12/12
NA/10	rule action -> If not present(8)	client	insert TGPP as 10	10/NA	NA/10
12/10	rule action -> If not present(8)	client	update TGPP from 12 to 10	10/NA	12/10
NA/NA	rule action -> If not present(8)	client	insert TGPP as 8	8/NA	NA/8
12/NA	rule action -> Never	client	no change	12/NA	12/12
NA/10	rule action -> Never	client	insert TGPP as 10	10/NA	NA/10
12/10	rule action -> Never	client	update TGPP from 12 to 10	10/NA	12/10
NA/NA	rule action -> Never	client	no change	NA/NA	NA/NA

Managing the Support for SBI Message Priority Header

Enable

This feature is not enabled by default. The feature gets enabled when a message priority profile is selected for **Message Priority Profile** field on the configuration page for the service such as **PCF Session Management** page for SM service on CNC Console, and `3GPP-SBI-Message-Priority` header is added to the outgoing and incoming HTTP requests and responses to PCF depending on the configuration of the `Message Priority Profile` selected for SM service.

Configure

Support for SBI message priority header can be configured either using CNC console or using REST API.

Configure Using CNC Console

To configure the feature using CNC Console:

1. Configure the Message Profile as explained in Message Profiles.
2. Select the required message priority profile to be used under Message Priority Profile section on PCF Session Management page as explained in PCF Session Management.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Select the required message priority profile to be used under Message Priority Profile section for UDR Connector and CHF Connector on User Connector page as explained in PCF User Connector.
4. Select the required message priority profile to be used under Message Priority Profile section on Binding Service page as explained in Binding Service.

Use the following blocks available under **Public Category** in **Policy Projects** to configure the support for 3GPP SBI Message Priority:

- Set SBI Message Priority for Interface Type and Operation Type
- Priority
- Request Headers
- Attribute in SMF Request

For more information, see *Public Category* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Configure Using REST API

The following APIs for PCF are used to configure support for SBI message priority header:

- PCF Session Management Service API: can be accessed using the URI `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm`
- User Service API: can be accessed using the URI `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfuser`
- Binding Service API: can be accessed using the URI `{apiRoot}/oc-cnpolicy-configuration/v1/services/binding`
- Message Profiles API: can be accessed using the URI `{apiRoot}/oc-cnpolicy-configuration/v1/services/common/messageProfiles`

Observability

Metrics

The following metrics are used for this feature:

- occnp_http_message_priority_request_count_total
- occnp_http_message_priority_response_count_total
- nrfclient_nw_conn_out_request_total

Use Cases

Table 4-10 Message Profile Configuration Cases

Original 3GPP-SBI-Message-Priority	Original oc-message-priority	Message Profile	Client such as SMF, AMF, or UDR/PCF (server)	Filter Action	3GPP-SBI-Message-Priority / oc-message-priority	Received Priority / Evaluated Priority
12	NA	Inactive	PCF (server)	No Change	12 / NA	12 / 12
NA	10	Inactive	PCF (server)	No Change	NA / 10	NA / 10

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-10 (Cont.) Message Profile Configuration Cases

Original 3GPP-SBI-Message-Priority	Original oc-message-priority	Message Profile	Client such as SMF, AMF, or UDR/PCF (server)	Filter Action	3GPP-SBI-Message-Priority / oc-message-priority	Received Priority / Evaluated Priority
12	10	Inactive	PCF (server)	No Change	12 / 10	12 / 10
NA	NA	Inactive	PCF (server)	No Change	NA / NA	NA / NA
12	NA	No matching rule	PCF (server)	No Change	12 / NA	12 / 12
NA	10	No matching rule	PCF (server)	No Change	NA / 10	NA / 10
12	10	No matching rule	PCF (server)	No Change	12 / 10	12 / 10
NA	NA	No matching rule	PCF (server)	No Change	NA / NA	NA / NA
12	NA	Rule action → always(8)	PCF (server)	Insert oc-message-priority as 8	12 / 8	12 / 8
NA	10	Rule action → always(8)	PCF (server)	Update oc-message-priority from 10 to 8	NA / 8	NA / 8
12	10	Rule action → always(8)	PCF (server)	Update oc-message-priority from 10 to 8	12 / 8	12 / 8
NA	NA	Rule action → always(8)	PCF (server)	Insert oc-message-priority as 8	NA / 8	NA / 8
12	NA	Rule action → If not present(8)	PCF (server)	Insert oc-message-priority as 12	12 / 12	12 / 12
NA	10	Rule action → If not present(8)	PCF (server)	No Change	NA / 10	NA / 10
12	10	Rule action → If not present(8)	PCF (server)	No Change	12 / 10	12 / 10
NA	NA	Rule action → If not present(8)	PCF (server)	Insert oc-message-priority as 8	NA / 8	NA / 8
12	NA	Rule action → Never	PCF (server)	Insert oc-message-priority as 12	12 / 12	12 / 12
NA	10	Rule action → Never	PCF (server)	No Change	NA / 10	NA / 10
12	10	Rule action → Never	PCF (server)	No Change	12 / 10	12 / 10
NA	NA	Rule action → Never	PCF (server)	No Change	NA / NA	NA / NA

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-10 (Cont.) Message Profile Configuration Cases

Original 3GPP-SBI-Message-Priority	Original oc-message-priority	Message Profile	Client such as SMF, AMF, or UDR/PCF (server)	Filter Action	3GPP-SBI-Message-Priority / oc-message-priority	Received Priority / Evaluated Priority
12	NA	Inactive	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	12 / NA
NA	10	Inactive	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	NA / NA
12	10	Inactive	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	12 / NA
NA	NA	Inactive	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	NA / NA
12	NA	No matching rule	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	12 / NA
NA	10	No matching rule	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	NA / NA
12	10	No matching rule	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	12 / NA
NA	NA	No matching rule	Client such as SMF, AMF, or UDR	Do not send 3gpp -Sbi -Message-Priority	NA / NA	NA / NA
12	NA	Rule action → always(8)	Client such as SMF, AMF, or UDR	Update 3gpp -Sbi -Message-Priority from 12 to 8	8 / NA	12 / 8

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-10 (Cont.) Message Profile Configuration Cases

Original 3GPP-SBI-Message-Priority	Original oc-message-priority	Message Profile	Client such as SMF, AMF, or UDR/PCF (server)	Filter Action	3GPP-SBI-Message-Priority / oc-message-priority	Received Priority / Evaluated Priority
NA	10	Rule action → always(8)	Client such as SMF, AMF, or UDR	Insert 3gpp -Sbi -Message-Priority as 8	8 / NA	NA / 8
12	10	Rule action → always(8)	Client such as SMF, AMF, or UDR	Update 3gpp -Sbi -Message-Priority from 12 to 8	8 / NA	12 / 8
NA	NA	Rule action → always(8)	Client such as SMF, AMF, or UDR	Insert 3gpp -Sbi -Message-Priority as 8	8 / NA	NA / 8
12	NA	Rule action → If not present(8)	Client such as SMF, AMF, or UDR	No Change	12 / NA	12 / 12
NA	10	Rule action → If not present(8)	Client such as SMF, AMF, or UDR	Insert 3gpp -Sbi -Message-Priority as 10	10 / NA	NA / 10
12	10	Rule action → If not present(8)	Client such as SMF, AMF, or UDR	Update 3gpp -Sbi -Message-Priority from 12 to 10	10 / NA	12 / 10
NA	NA	Rule action → If not present(8)	Client such as SMF, AMF, or UDR	Insert 3gpp -Sbi -Message-Priority as 8	8 / NA	NA / 8
12	NA	Rule action → Never	Client such as SMF, AMF, or UDR	No Change	12 / NA	12 / 12
NA	10	Rule action → Never	Client such as SMF, AMF, or UDR	Insert 3gpp -Sbi -Message-Priority as 10	10 / NA	NA / 10

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-10 (Cont.) Message Profile Configuration Cases

Original 3GPP-SBI-Message-Priority	Original oc-message-priority	Message Profile	Client such as SMF, AMF, or UDR/PCF (server)	Filter Action	3GPP-SBI-Message-Priority / oc-message-priority	Received Priority / Evaluated Priority
12	10	Rule action → Never	Client such as SMF, AMF, or UDR	Update 3gpp -Sbi -Message-Priority from 12 to 10	10 / NA	12 / 10
NA	NA	Rule action → Never	Client such as SMF, AMF, or UDR	No Change	NA / NA	NA / NA

Table 4-11 Policy Evaluated Priority Cases

Original 3gpp-msg-priority	Original oc-msg-priority	PRE action	Client such as SMF, AMF, or UDR/PCF (PCF)	3gpp-msg-priority / oc-msg-priority	Received Priority / Evaluated Priority
12	NA	evaluate to 8	PCF response	8 / NA	NA / 8
12	NA	evaluate to 8	Client request	8 / NA	12 / 8
NA	10	evaluate to 8	Client request	8 / NA	NA / 8
12	10	evaluate to 8	Client request	8 / NA	12 / 8
NA	NA	evaluate to 8	Client request	8 / NA	NA / 8

4.9 Disabling mTLS to Establish Communication between Policy and cnDBtier

Communication between Policy and cnDBTier uses Mutual Transport Layer Security (mTLS), which provides mutual authentication for both server and client, on an ASM setup. The mTLS method establishes a TLS connection between client and server to authenticate both server and client before sharing any data.
ASM-managed TLS certificates are configured in Policy and cnDBTier. This method enables you to disable mTLS on the Policy-to-cnDBTier interface.

Note

- This migration requires cnDBTier 26.1.200 or later.
- In-service upgrade is not supported for this configuration. Traffic for the Policy site being upgraded to this release must be diverted to another site to isolate the current site.
- Disabling mTLS is an offline procedure performed after the upgrade is completed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information about the migration, see "Migrating Policy to Support an ASM Disabled cnDBTier" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

Managing mTLS to Establish Communication between Policy and cnDBTier

Enable

This feature is disabled by default.

Perform the deployment procedure with destination rule to disable mTLS towards cnDBTier. See "Installing Service Mesh Configuration Charts" section for the deployment procedure in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

> **Note**
>
> The procedure is applicable for fresh deployment of Policy and after the upgrade of Policy.

Configure

There is no specific configuration required for this feature.

4.10 Supports pcfIpEndPoints in pcfBinding- BSF Registration

In the previous releases, CnPolicy did not include its network endpoint information (pcfIpEndPoints) when registering with the BSF, it includes only its Diameter Host, Diameter Realm, and FQDN. Missing of pcfIpEndPoints prevents the Network Exposure Function (NEF) or Application Function (AF) from discovering the specific signaling port used by the CnPolicy for policy authorization requests. This can lead to signaling call failures, where the npcf-policyauthorization request from NEF to CnPolicy results in a 503 Service Unavailable response.

In 26.1.200 release, a new drop-down field, **Service FQDN and IP Endpoints Configuration**, in SM Service Configuration is added in CNC Console. The available options in the drop-down are:

- Service FQDN (no pcfIpEndPoints will be sent) - enabled by default
- Service FQDN and Endpoint(s) (IPv4, IPv6, Protocol, and Port)
- Service EndPoint(s) (IPv4, IPv6, Protocol, and Port)

Depending on the configuration, SM Service will now send the information present in the ipEndPoints of the NF Profile in its Binding Registration request; that is, IPv4, IPv6, Transport, and Port. Which is then going to be received by Binding Service, and forwarded towards BSF with the corresponding information. At that point, BSF Management Service registers the received pcfIpEndPoints inside the json_content column in the BSF's PCF Binding Table.

The feature works based on the NF Registration Profile defined at installation time, or whenever it is updated through CNC Console or REST API. When CnPolicy is installed, you can check its corresponding NF Registration Profile in the CNC Console under the following path: HOME > Status and Query > NF Data > NF Registration Profile. The feature works based

Copyright © 2019, 2026, Oracle and/or its affiliates.

only on the profile defined for Policy Authorization (PA) or SM Policy Control. Below is an example of Policy Authorization profile:

```
[
  {
    "nfServices": [
      {
        "fqdn": "occnp-ocpm-ingress-gateway.ocpcf.svc",
        "versions": [
          {
            "apiFullVersion": "1.0.0",
            "apiVersionInUri": "v1"
          }
        ],
        "ipEndPoints": [
          {
            "ipv4Address": "10.10.10.10",
            "transport": "TCP",
            "port": 5806
          },
          {
            "ipv6Address": "2001:dc9:3c4d::1",
            "transport": "TCP",
            "port": 80
          }
        ],
        "serviceName": "npcf-policyauthorization",
        "allowedNfTypes": [
          "AMF",
          "NEF"
        ],
        "nfServiceStatus": "REGISTERED",
        "serviceInstanceId": "03063893-cf9e-4f7a-9827-067f6fa9dd01"
      }
    }
  ]
}
```

It is assumed that the operator defines the ipEndPoints that will be used in the PCF Binding Registration requests.

Depending on the configuration selected in Session Management, the Binding Registration Request can contain the pcfIpEndPoints field with different values. Below are some examples on how the body is expected to look:

- FQDN only:

```
{
  "bindingId": "006f350a-6e40-488c-bc2f-c330a7fa69ca",
  "supi": "imsi-123456789012345",
  "gpsi": "msisdn-123456789012345",
  "dnn": "ims.mnc001.mcc001.3gppnetwork.org",
  "ipv4Addr": "192.168.120.111",
  "ipv6Prefix": "2001:db8:3c4d::/48",
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
  "pcfFqdn": "pcf-sim.oracle.com"
}
```

- FQDN and PCF IP Endpoints (IPv4 / IPv6, Transport, and Port):

```
{
  "bindingId": "006f350a-6e40-488c-bc2f-c330a7fa69ca",
  "supi": "imsi-123456789012345",
  "gpsi": "msisdn-123456789012345",
  "dnn": "ims.mnc001.mcc001.3gppnetwork.org",
  "ipv4Addr": "192.168.120.111",
  "ipv6Prefix": "2001:db8:3c4d::/48",
  "pcfFqdn": "pcf-sim.oracle.com",
  "pcfIpEndPoints": [
    {
      "ipv4Address": "10.10.10.255",
      "transport": "TCP",
      "port": 80
    },
    {
      "ipv6Address": "2810:acc:cab1:10:aca:88:1:0",
      "transport": "TCP",
      "port": 5806
    }
  ]
}
```

- PCF IP Endpoints (IPv4 / IPv6, Transport, and Port)

```
{
  "bindingId": "006f350a-6e40-488c-bc2f-c330a7fa69ca",
  "supi": "imsi-123456789012345",
  "gpsi": "msisdn-123456789012345",
  "dnn": "ims.mnc001.mcc001.3gppnetwork.org",
  "ipv4Addr": "192.168.120.111",
  "ipv6Prefix": "2001:db8:3c4d::/48",
  "pcfIpEndPoints": [
    {
      "ipv4Address": "10.10.10.255",
      "transport": "TCP",
      "port": 80
    },
    {
      "ipv6Address": "2810:acc:cab1:10:aca:88:1:0",
      "transport": "TCP",
      "port": 5806
    }
  ]
}
```

Managing Supports pcfIpEndPoints in pcfBinding- BSF Registration

Enable

This feature can be enabled using CNC Console as well as REST API.

Enable Using CNC Console

Copyright © 2019, 2026, Oracle and/or its affiliates.

To enable this feature using CNC Console, a new drop-down field, **Service FQDN and IP Endpoints Configuration**, is added in the **PCF Session Management** page.

Also, configure the value of **NF Profile for Service FQDN and IP Endpoints** in the **PCF Session Management** page.

For more information, see PCF Session Management.

Because of these new configurations, two advance settings, **BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS** and **BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS.SERVICE_NAME**, have been deprecated in 26.1.200.

Enable using REST API
This feature can also be enabled by configuring binding.fqdnIpEndpointsConfiguration and binding.fqdnIpEndpointsProfile parameters in Session Management Service API: `/oc-cnpolicy-configuration/v1/services/pcfsm`. For more information, see *Session Management Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Upgrade Impact
While Helm Upgrade, the following algorithm is run in SM Service Release Hook 26.1.200:

- 1. Obtain the Configuration Item of the topic: 'pcf.smservice.cfg'.
  2. If the **advancedSettings** field contains BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS
     a. If BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS has a false value, then add the fqdnIpEndpointsConfiguration field into the 'pcf.smservice.cfg' topic with the value:

        ```
        {"fqdnIpEndpointsConfiguration":"SERVICE_FQDN"}
        ```

     b. If BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS has a true value, then add the fqdnIpEndpointsConfiguration filed into the 'pcf.smservice.cfg' topic with the value:

        ```
        {"fqdnIpEndpointsConfiguration":"SERVICE_FQDN_AND_ENDPOINTS"}
        ```

  3. If the **advancedSettings** field contains BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS.SERVICE_NAME
     a. If BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS.SERVICE_NAME has a npcf-policyauthorization value, then insert the fqdnIpEndpointsProfile field into topic with the same value:

        ```
        {"fqdnIpEndpointsProfile":"npcf-policyauthorization"}
        ```

     b. If BINDING.REGISTRATION.INCLUDE.IP_ENDPOINTS.SERVICE_NAME has a npcf-smpolicycontrol value, then insert the fqdnIpEndpointsProfile field into topic with the same value:

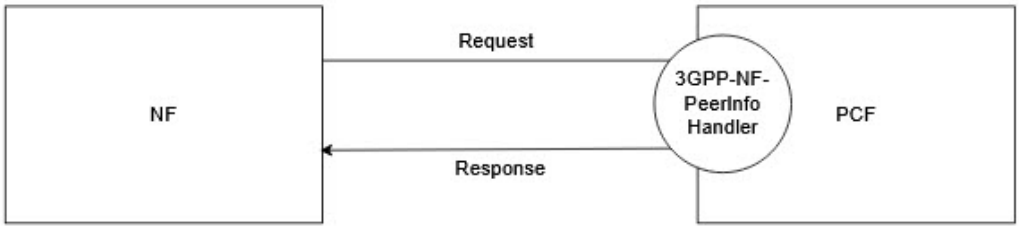
        ```
        {"fqdnIpEndpointsProfile":"npcf-smpolicycontrol"}
        ```

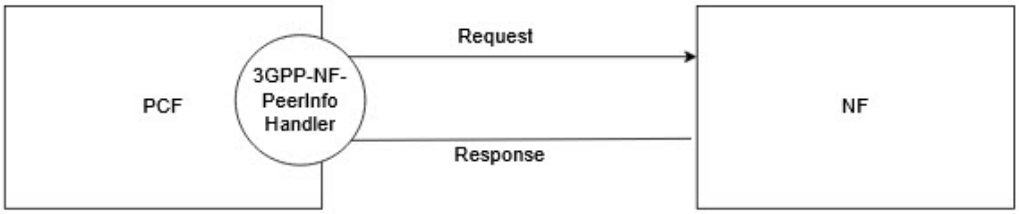
  4. If the **advancedSettings** field is not present, then do nothing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.11 Support for the 3gpp-Sbi-NF-Peer-Info Header

The 3gpp-Sbi-NF-Peer-Info header feature enables PCF to identify the source and destination Network Functions (NFs) or NF service instances in HTTP messages exchanged over Service Based Interfaces (SBIs). When the feature is enabled and the associated NF Communication Profile is configured to send NF Peer Info headers, PCF includes the 3gpp-Sbi-NF-Peer-Info header in supported request and response flows. The PCF must send the HTTP client and server peer identities in the 3gpp-Sbi-NF-Peer-Info custom HTTP header, as defined in 3GPP TS 29.500 Clause 5.2.3.2. PCF can receive, generate, forward, and return this header for supported PCF interfaces.





The feature provides the following functionalities:

- It identifies the source and destination NF or NF service instances in HTTP requests and responses.
- It forwards received or generated peer information to peer NFs.
- It provides interface-level control through NF Communication Profiles.

The header encoding follows Augmented Backus-Naur Form (ABNF) as defined in IETF RFC 7230:

```
3gpp-Sbi-NF-Peer-Info = "3gpp-Sbi-NF-Peer-Info" ":" OWS peerinfo *(";" OWS
peerinfo)

peerinfo = peertype "=" token
```

The header supports the following peer types.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-12 Header Peer Type

Peer Type	Description
`srcinst`	It is the source NF instance. Indicates the source NF instance ID.
`srcservinst`	It is the source NF service instance. Indicates the source NF service instance ID. If this parameter is present, `srcinst` must also be present.
`srcscp`	It is the source SCP. Indicates the FQDN of the source SCP in the format `SCP-<SCP FQDN>`. This parameter is included only by an SCP when the HTTP request or response is originated or relayed by an SCP.
`srcsepp`	It is the source SEPP. Indicates the FQDN of the source SEPP in the format `SEPP-<SEPP FQDN>`. This parameter is included only by a SEPP when the HTTP request or response is originated or relayed by a SEPP.
`dstinst`	It is the destination NF instance. Indicates the destination NF instance ID.
`dstservinst`	It is the destination NF service instance. Indicates the destination NF service instance ID. If this parameter is present, `dstinst` must also be present.
`dstscp`	It is the destination SCP. Indicates the FQDN of the destination SCP in the format `SCP-<SCP FQDN>`. This parameter contains the next-hop SCP of the HTTP request or response.
`dstsepp`	It is the destination SEPP. Indicates the FQDN of the destination SEPP in the format `SEPP-<SEPP FQDN>`. This parameter is included by an SCP, by clients or servers that send messages to a SEPP, or by a SEPP based on operator policy.

The header must contain destination peer information when destination peer information is available. When destination peer information is available, the PCF must include that information in the destination field of the peer information header when it initiates or responds to a request. For example:

```
3gpp-Sbi-NF-Peer-Info: srcinst=54804518-4191-46b3-955c-ac631f953ed8;
dstinst=54804518-4191-4453-569c-ac631f74765cd
```

The feature has the following limitations:

- NRF interaction messages and API gateway-generated messages do not include the 3gpp-Sbi-NF-Peer-Info header. The following scenarios are examples only:
  - Overload error responses returned by ingress gateway.
  - OAuth validation error responses returned by ingress gateway.
  - Error responses returned by ingress gateway because of a timeout while waiting for a response from the back-end service.
  - If the customer uses NRF access token requests sent from egress gateway.
  - HTTP OPTIONS requests sent from egress gateway to SCP.

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - Gateway-generated NF Peer Info, which is out of scope.
- If `srcscp` is received in a request, PCF internal services swap it to the corresponding `dstScp` value in response.
- PCF does not save SCP information in its database for subsequent requests.
- If the header information saved in the database differs from the header information received in the latest request, the header information in the latest request takes precedence.
- If unknown attributes, such as `srcNrf`, are present in the 3gpp-Sbi-NF-Peer-Info header, PCF ignores those fields and continues to process the known attributes. PCF does not save, forward, or include the unknown attributes in the response.
- Invalid or unsupported parameters in the 3gpp-Sbi-NF-Peer-Info header do not cause request rejection. PCF logs a message and continues processing because the header is used only for analytics, not for signaling.
- In some scenarios, such as SCP alternate routing or DNS SRV, the 3gpp-sbi-nf-peer-info header might not contain accurate information.
- If PCF cannot determine the NF instance or service instance that corresponds to the selected host and port, `dstinst` and `dstservinst` are not set in the outgoing 3gpp-sbi-nf-peer-info header sent to the external UDR or CHF.
- PCF uses the best available information to update NF peer information.
- If a locally configured BSF is used, the 3gpp-Sbi-NF-Peer-Info header is not sent.
- For the retry mechanism that uses `DestinationRoute` to retry a request:
  - The system searches for a configured `bsfProfile` by using the `nfInstanceId` received in `DestinationRoute`.
  - If a matching `bsfProfile` is found, the service instance ID is obtained.
  - If no match is found, the service instance is not set in `dstservinst`.
- When 3gpp-Sbi-Producer-Id is used to retrieve `nfInstanceId`:
  - This header contains only `nfInstanceId`. It does not contain a service instance ID.
  - The same approach applies. If no `bsfProfile` matches `nfInstanceId`, the service instance is not set in `dstservinst`.

Managing Support for 3gpp-Sbi-NF-Peer-Info header

Enable

You can enable the 3gpp-Sbi-NF-Peer-Info header feature using Helm Configuration:

You can enable or disable the feature by setting the `enableNfPeerInfo` parameter to true or false in the custom-values.yaml file. The default value is set as false. For more information on this parameter, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

Configure

This feature can be configured using CNC Console and REST API.

You must enable the 3gpp-Sbi-NF-Peer-Info header feature by using Helm Configuration. Then, configure interface-specific settings by using the CNC Console or REST API.

Configure using CNC Console

Copyright © 2019, 2026, Oracle and/or its affiliates.

Configure the interface-specific **NF Peer Info Settings** in the **NF Communication Profile**.

Configure the following fields under **NF Peer Info Settings**:

- **Send NF-Peer-Info Header**: Enables PCF to send the received or generated NF peer info headers to the peer NFs.
- **Include NF Service Instance ID**: Enables PCF to include the NF service instance ID when forwarding the received or generated headers.

> **Note**
>
> The **Include NF Service Instance ID** field depends on the **Send NF-Peer-Info Header** field as follows:
>
> - If **Send NF-Peer-Info Header** is disabled, then **Include NF Service Instance ID** is hidden and cannot be enabled.
> - If **Send NF-Peer-Info Header** is enabled, then **Include NF Service Instance ID** is displayed and configurable.

When the feature is enabled and the associated NF Communication Profile is configured to send NF Peer Info headers, PCF includes the 3gpp-Sbi-NF-Peer-Info header in supported request and response flows.

For more information, see NF Communication Profiles.

After you configure the NF Communication Profile to a back-end interface, the configuration applies only to that back-end interface. The supported back-end interfaces are PCF Session Management, PCF Binding, and PCF User Connector.

Configure using REST API

This feature can be configured using `sendNfPeerInfo` `includeSrcServInst` parameters in NF Communication Profiles APIs: `{apiRoot}/oc-cnpolicy-configuration/v1/services/common/nfcommprofiles/{nfCommunicationProfileName}`.

For more information, see *NF Communication Profiles* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

- **Metrics**

  The following metrics are used to support this feature:

  – occnp_nf_peer_info_header_received _total
  – occnp_nf_peer_info_header_sent_total

  For more information, see Sbi-NF-Peer-Info Header Metrics.
- There are no new KPIs or alerts available for this feature.

4.12 Support for DNN Replacement and Slice Support in AM Policy

DNN Replacement in AM Policy enables PCF to provide an alternate DNN when the UE-requested DNN is unsupported or configured for replacement by operator policy. PCF provides

Copyright © 2019, 2026, Oracle and/or its affiliates.

replacement candidates or a selected replacement DNN to AMF based on S-NSSAI, subscriber data, policy rules, and negotiated feature support.

PCF supports DNN replacement applicable to the following enterprise use cases:

- UE operates using local configuration.
- Operator policies enable the replacement of a UE requested DNN with another DNN intended solely for internal network use. During the UE registration procedure, the PCF can inform the AMF of the operator policies to apply for DNN replacement at PDU session establishment, substituting the UE requested DNN as necessary.

PCF provides the list of DNNs that AMF can replace when the UE establishes a PDU session.

- AMF performs DNN replacement.
- PCF in AM Policy association sends candidates.

> **Note**
>
> DNN Replacement requires successful feature negotiation between AMF and PCF. AMF must advertise support for `DNNReplacementControl`, and PCF must have the corresponding feature enabled through Override Supported Features. Slice-related candidate filtering also depends on SliceSupport negotiation and availability of `allowedSnssais`.

If the values of **Override Supported Features** field for PCF AM service includes `DNNReplacementControl` and `SliceSupport`, PCF indicates a policy for DNN replacement of UE requested DNNs not supported by the network. Policy supports the UE requested DNNs per S-NSSAI valid for the serving network, that are subject for replacement.

If the DNN requested by the UE is indicated for replacement, or if the DNN provided by the UE is not supported by the network and the network supports a policy for replacing UE requested DNNs, the AMF interacts with the PCF to perform a DNN replacement.

During PDU session establishment, as a result of the DNN replacement, PCF provides a replacement DNN selected for the requested S-NSSAI/DNN combination, as requested by the UE. The AMF uses the selected DNN in the query towards the NRF for the SMF selection.

In order to manage the SMF selection, PCF instructs the AMF to contact the PCF during the PDU session establishment to perform a DNN replacement.

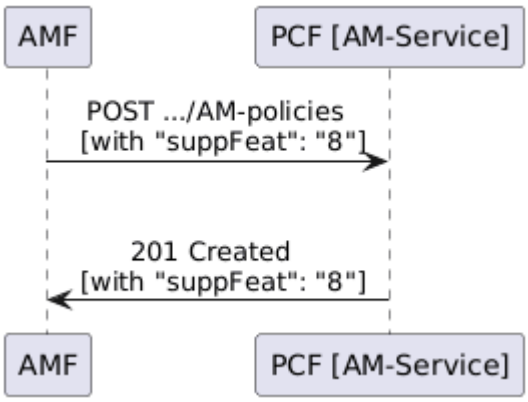
Call Flow

During Npcf_AMPolicyControl_Create service operation, `DNNReplacementControl` feature is negotiated and agreed upon between AMF and PCF.

AMF advertises the support for `DNNReplacementControl` feature in `suppFeat` attribute in the AM CREATE request. `"suppFeat":"8"` in the request/response represents the feature number "4" and feature name `DNNReplacementControl` as defined in Table 5.8-1: Supported Features, 3GPP TS 29.507.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-37 Feature Negotiation - DNN Replacement



1. If AMF advertises the support for `DNNReplacementControl` feature and:
   a. If the `DNNReplacementControl` is selected in **Override Supported Features** in PCF, then PCF advertises the same using `suppFeat` attribute with value 8 in the response message towards AMF.
   b. If the `DNNReplacementControl` is not selected in **Override Supported Features** in PCF, then PCF does not advertise the same using `suppFeat` attribute in the response message towards AMF.
2. If AMF does not advertise the support for `DNNReplacementControl` feature and:
   a. If the `DNNReplacementControl` is selected in **Override Supported Features** in PCF, then PCF does not advertise the same using `suppFeat` attribute in the response message towards AMF.
   b. If the `DNNReplacementControl` is not selected in **Override Supported Features** in PCF, then PCF does not advertise the same using `suppFeat` attribute in the response message towards AMF.

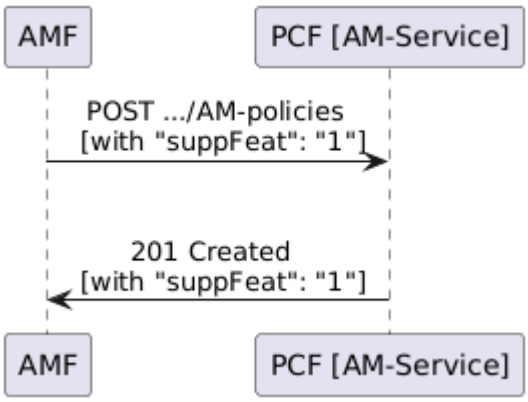
Feature Negotiation - Slice Support

During Npcf_AMPolicyControl_Create service operation, `SliceSupport` feature is negotiated and agreed upon between AMF and PCF.

AMF advertises the support for `SliceSupport` feature in `suppFeat` attribute in the AM CREATE request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-38 Feature Negotiation - SliceSupport

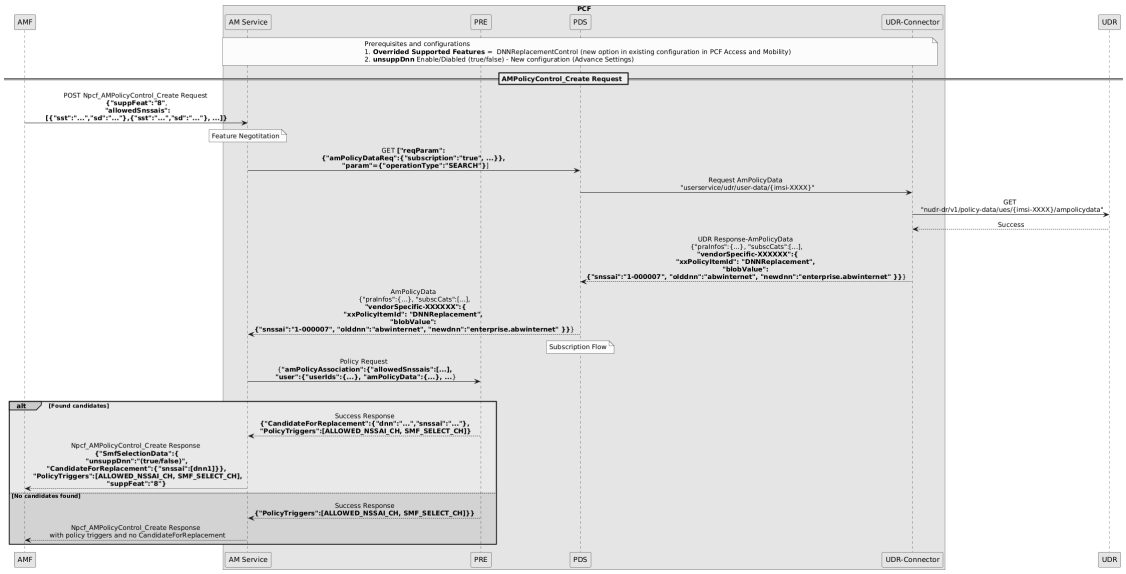


1. If AMF advertises the support for `SliceSupport` feature and:
   a. If the `SliceSupport` configuration is selected in **Override Supported Features** in PCF, then PCF advertises the same using `suppFeat` attribute with value "1" in the response message towards AMF.
   b. If the `SliceSupport` configuration is not selected in **Override Supported Features** in PCF, then PCF does not advertise the same using `suppFeat` attribute in the response message towards AMF.
2. If AMF does not advertise the support for `SliceSupport` feature and:
   a. If the `SliceSupport` configuration is selected in **Override Supported Features** in PCF, then PCF does not advertise the same using `suppFeat` attribute in the response message towards AMF.
   b. If the `SliceSupport` configuration is not selected in **Override Supported Features** in PCF, then PCF not advertise the same using `suppFeat` attribute in the response message towards AMF.

Combined `suppFeat` in responses reflects the set of negotiated features; for example “09” hex indicates features 1 and 4 active.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-39 AmPolicyControl_Create Procedure - DNN Replacement



Npcf_AMPolicyControl_Create Request

The AMF notifies the PCF that it supports the DNN replacement feature. It also provides the PCF with the Allowed NSSAI, enabling the PCF to select a subset as candidate DNNs (per S-NSSAI) for potential replacement. When `SYSTEM.CONSIDER_ALLOWED_SNSSAIS_FOR_CANDIDATES` Advanced settings key is enabled, PCF filters candidates based on `allowedSnssais`. When `SYSTEM.CONSIDER_ALLOWED_SNSSAIS_FOR_CANDIDATES` Advanced settings key is disabled, candidate behavior may include entries outside the current allowed NSSAI scope or null removal entries, depending on policy evaluation and update behavior. During the Npcf_AMPolicyControl_Create process, the AMF can include the `allowedSnssais` parameter in its request. This parameter represents the set of S-NSSAIs permitted in 3GPP access and includes the S-NSSAIs (maximum of 8 S-NSSAIs) that the UE is authorized to use in the serving PLMN. By providing this information, the PCF is able to generate a list of candidate DNNs (maximum of 10 DNNs per S-NSSAIs) for replacement, as this list must be a subset of the Allowed NSSAI. If the PRE cannot generate a candidate list to return, the AM service responds to the AMF with `PolicyTriggers` and sets the `unsuppDnn` as per the configuration of the advanced settings key..

Additionally, when PCF queries UDR for AM data, it receives AmPolicyData from the UDR containing VSA attributes. During policy evaluation, PCF uses these VSA attributes as conditions to determine whether DNN replacement is necessary for the UE. If DNN replacement is required, the policy writer updates the policy to set the `SmfSelectionData.candidates` attribute. This attribute can be assigned values either from the VSA attributes defined in the policy or provided as user input within the policy.

Policy supports multiple S-NSSAI and DNNs in `SmfSelectionData` to AMF for a UE and its respective AM Policy Association.

When an update is received from AMF with change in `ALLOWED_NSSAI_CH`, `SmfSelectionData` is updated to AMF. Also, `SmfSelectionData` is updated to AMF when a notification is received from UDR with change in VSA or any other attribute.

Policy overrides the DNN from VSA or adds DNN for S-NSSAI and the S-NSSAI, in `SmfSelectionData`, irrespective of whether it is present in VSA.

Copyright © 2019, 2026, Oracle and/or its affiliates.

S-NSSAI and DNNs are replaced through Policy Tables and Policy action by setting the S-NSSAI and the corresponding DNN in Policy Projects.

Also, Policy supports unsupported DNN for S-NSSAI in `SmfSelectionData`.

Error conditions are triggered when mandatory attributes are not received.

Npcf_AMPolicyControl_Create Response

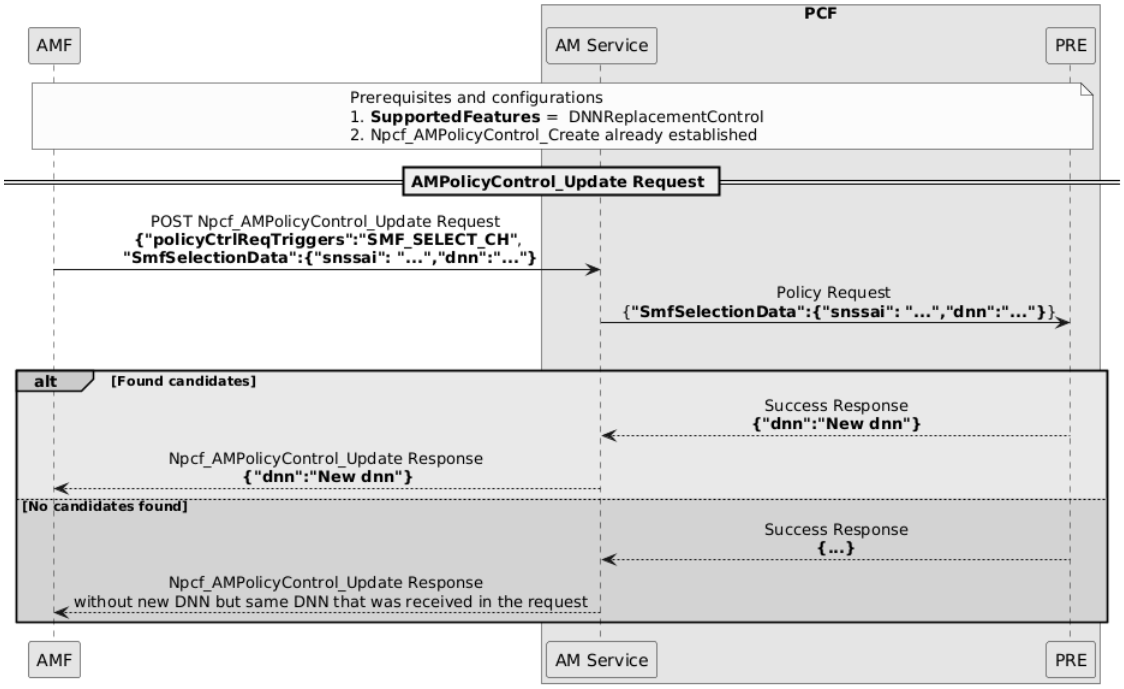
`PolicyTriggers` can include values such as `SMF_SELECT_CH` or `ALLOWED_NSSAI_CH`, which indicates that the AMF sends Npcf_AMPolicyControl_Update to the PCF with the following trigger notification: `SMF selection information change: UE request for an unsupported DNN or UE request for a DNN within the list of DNN candidates for replacement per S-NSSAI`.

The PCF informs the AMF of its capability to support the DNN replacement feature and supplies a list of candidate DNNs (for each S-NSSAI) available for replacement. If the UE requests to establish a PDU Session with any S-NSSAI/DNN combination from this list, the AMF sends an update request to the PCF specifying the selected S-NSSAI/DNN.

The S-NSSAI is in the serving PLMN and contains a S-NSSAI within the Allowed NSSAI, provided by the AMF in the Create Request.

The **unsuppDnn** attribute in **SmfSelectionData** is set based on `SYSTEM.SEND_UNSUPPDNN_ON_AM_RESPONSE` Advanced settings key. When the value of this key is set to `true`, the AMF requests DNN replacement if the UE requests an unsupported DNN during a PDU session establishment request.

Figure 4-40 AmPolicyControl_Update Procedure - DNN Replacement



Npcf_AMPolicyControl_Update Response

AMF sends the update request in either of the following two cases:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- The UE requested an `unsupported` DNN and the **unsuppDnn** attribute in the Npcf_AMPolicyControl_Create response is set to `true`,

  and/or

- The UE requested DNN and S-NSSAI matched one of the S-NSSAI and DNN provided in the `candidates` attribute in the Npcf_AMPolicyControl_Create response

The update request includes the following Policy Trigger: `SMF_SELECT_CH`. That is, SMF selection information change: UE request for an unsupported DNN or UE request for a DNN within the list of DNN candidates for replacement per S-NSSAI. The request also includes the combination S-NSSAI/DNN for which replacement is requested.

Npcf_AMPolicyControl_Update Response

PCF includes `DNN` in AM policy association update response. This DNN represents the PCF selected DNN.

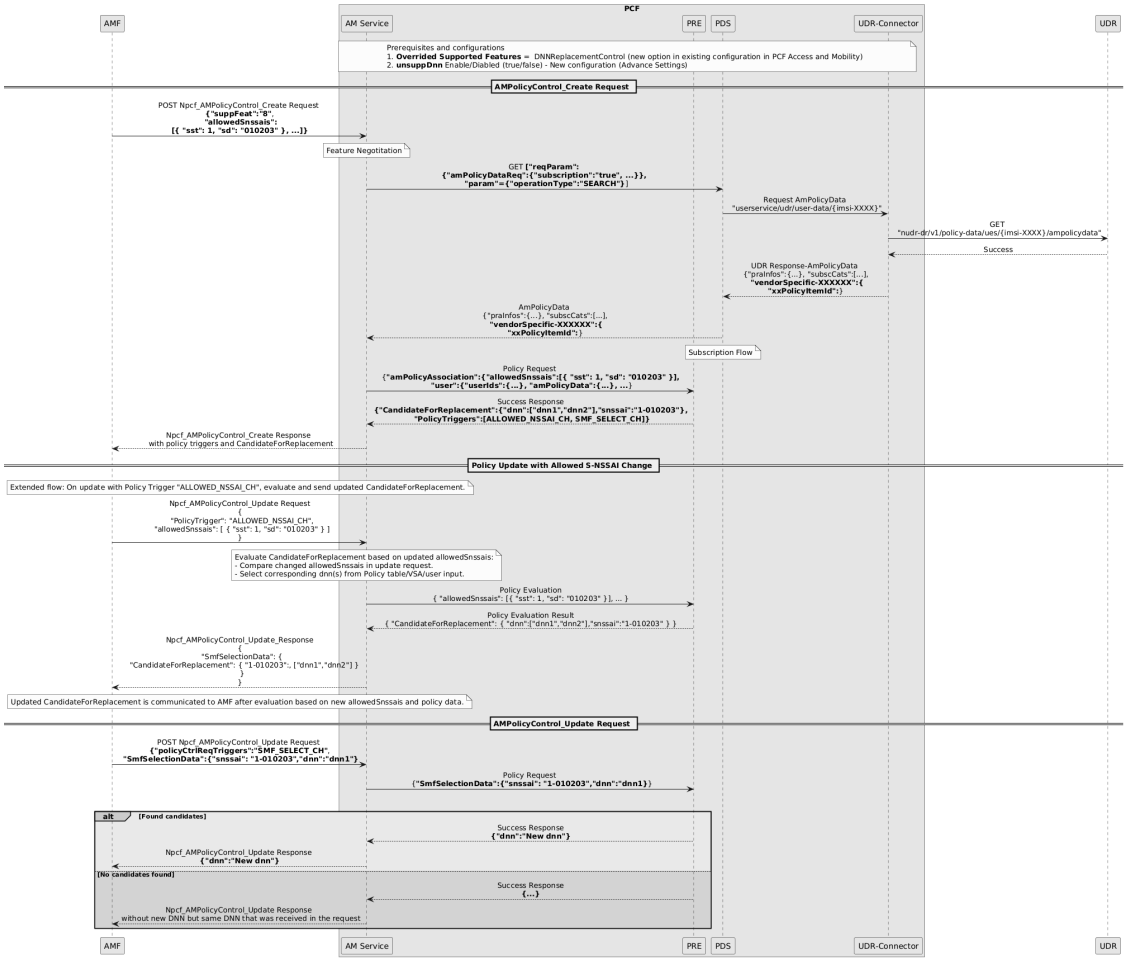
Policy allows policy evaluation to send updated candidates for replacement in the Update response to AMF. Policies to send the updated `CandidateForReplacement` are evaluated while responding to an Update request received or in the UpdateNotify request sent to AMF.

If the Policy Control Request Trigger for SMF selection information change (`SMF_SELECT_CH`) is provided or if that trigger is already set and the list of candidate DNNs for replacement must be changed, the `CandidateForReplacement` attribute within the `smfSelInfo` attribute is updated as follows:

- A new entry is added by supplying a new S-NSSAI as key and the corresponding `CandidateForReplacement` data type instance with complete contents as value in an entry within the map.
- An existing entry is modified by supplying the existing S-NSSAI as key and the `CandidateForReplacement` data type instance with complete contents as value in an entry within the map.
- An existing entry is deleted by supplying the existing S-NSSAI as key and "NULL" as value in an entry within the map.
- For an unmodified entry, no entry is provided within the map.
- The complete list of candidate DNNs for which reporting is required is removed by providing the `CandidateForReplacement` attribute with "NULL" value.
- If the Policy Control Request Trigger `SMF_SELECT_CH` is removed, the candidate DNNs for which reporting is required is also removed by providing the `smfSelInfo` attribute with "NULL" value.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-41 AmPolicyControl_Update Procedure - ALLOWED_NSSAI_CH Trigger Received and allowedSnssai on Request Body



Processing Npcf_AMPolicyControl_Create request from AMF:

1. PCF receives `Npcf_AMPolicyControl_Create` request from AMF with `suppFeat` and `allowedSnssais` attributes.
2. PCF performs feature negotiation based on `suppFeat` attribute.
3. PCF sends a request to UDR through UDR Connector to get the subscriber data.
4. UDR returns the AM Policy Data, including `praInfos`, `subscCats` and Vendor-specific policy data (such as `xxPolicyItemId`).
5. PCF performs Policy evaluation based on the data received from UDR and the request parameters (such as allowed S-NSSAIs).
6. PCF updates the `amPolicyAssociation` with `allowedSnssais`.
7. PCF prepares the `CandidateForReplacement` with the given DNN and S-NSSAI.
8. PCF runs Policy Trigger with `ALLOWED_NSSAI_CH` and `SMF_SELECT_CH`.
9. PCF responds to AMF with Policy triggers and `CandidateForReplacement` in the response.

Policy Update Triggered by Allowed NSSAI Change:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. PCF receives `Npcf_AMPolicyControl_Update` request from AMF. The Update request received from AMF includes `PolicyTrigger = ALLOWED_NSSAI_CH` and the updated `allowedSnssais`.
2. PCF evaluates `allowedSnssais` matching the DNNs from Policy data and Vendor Specific Attribute (VSA).
3. Accordingly, PCF selects the `CandidateForReplacement`.
4. PCF responds to the `Npcf_AMPolicyControl_Update` request from AMF with `SmfSelectionData` and the updated `CandidateForReplacement` in the response.

SMF Selection Update Flow (Npcf_AMPolicyControl_Update request):

1. PCF receives `Npcf_AMPolicyControl_Update` from AMF that includes `PolicyTrigger = SMF_SELECT_CH` and `SmfSelectionData` with the given DNN and S-NSSAI.
2. PCF evaluates request and determines the DNN candidate.
3. PCF responds with the updated DNN indicating DNN replacement.
4. If PCF cannot identify the candidate DNN, it responds to AMF with the original DNN received in the update request from AMF. This indicates that the DNN is not replaced.

Managing Support for DNN Replacement and Slice Support in AM Policy

Enable

This feature can be enabled using CNC Console as well as REST API.

Enable Using CNC Console

To enable this feature using CNC Console, add `DNNReplacementControl` and `SliceSupport` as values of **Override Supported Features** field under **System** section on **PCF Access and Mobility** for **Service Configurations**.

> **Note**
>
> Addition of `DNNReplacementControl` is mandatory to enable the feature. `SliceSupport` must be added for slice-related candidate filtering depending on the availability of `allowedSnssais`.

Also, configure the value of `SYSTEM.SEND_UNSUPPDNN_ON_AM_RESPONSE` advanced settings key on **PCF Access and Mobility** page to `true`.

For more information, see PCF Access and Mobility.

Enable Using REST API

This feature can also be enabled by adding `DNNReplacementControl` and `SliceSupport` as value of `overrideSupportedFeatures` parameter on Access and Mobility Service API: `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam`. For more information, see *PCF Access and Mobility* Service section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

Configure Using CNC Console

Select `ALLOWED_NSSAI_CH` or `SMF_SELECT_CH` as value of **Default Triggers** field under **Rules** section on **PCF Access and Mobility** page. For more information, PCF Access and Mobility.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Use the following blocks under **PCF-AM Blocks** category in **Policy Projects** to configure the support for DNN replacement:

- Convert SNSSAI In
- Create List With
- Set Replacement
- Attributes from Candidates
- Attributes from Candidates for S-NSSAI
- Request Trigger
- Attribute in AMF Request
- Attribute from smfSelInfo in Update Request
- Set Candidates
- attribute from smfSelInfo in Update Request
- Override unSuppDnn

For more information on these blocks, see *PCF-AM Blocks* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Configure Using REST API

This feature can be configured using `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam`. For more information, see *PCF Access and Mobility* Service section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

> **Note**
>
> Currently, Policy does not support regex or comma separated values as mentioned below:

Table 4-13 Support for Comma Separated String, Regex, and Wildcard for CandidateForReplacement and ReplacementDnn

Type of expression	CandidateForReplacement	ReplacementDnn
Comma separated string	dnn1,dnn2,dnn3	dnn4
Regex or wildcard	dnn.*	newCord.dnn

Policy Tables can be used for setting inputs in the Policy Design, such as S-NSSAIs, DNNs, and allowedSnssais.

Table 4-14 Sample Format to Define Candidate for Replacement

S-NSSAI (String)	DNN (List)
1-010203	dnn1, dnn2, dnn3
1-030405	abiw.internet, newDnn.enterprise
2	newDnn

Also, Policy tables can be used to set a new DNN replacement to be mapped for the candidate for replacement DNNs.

Copyright © 2019, 2026, Oracle and/or its affiliates.

When there are multiple `CandidatesForReplacement` with the same DNN, a Priority column must be added to define which replacement is the one to consider.

Table 4-15 Example for Adding Priority to Define Multiple CandidatesForReplacement with the Same DNN

Priority	CandidatesForReplacement	Replaced DNN
1	dnn2	EntInternet3
1	dnn1	EntInternet2
1	test1	EntInternet1
1	test2	EntInternet1
1	*	EntCommon
1	dnn3	newDnn3
1	test3	newDnn3
2	dnn3	EntInternet4
2	test3	EntInternet3

> **Note**
>
> Currently, the max number of DNNs that can be configured for Policy Table, "Replacement Dnn", is 3000.

Observability

Metrics

`dnn_replacement_total` metric is used for this feature. For more information, see AM Service Metrics.

Alerts

The following alerts are used for this feature:

- DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MINOR_PERCENT
- DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MAJOR_PERCENT
- DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_CRITICAL_PERCENT

4.13 Support for USER_LOCATION_CH Event Trigger

Policy provides the capability to handle User Location Change (USER_LOCATION_CH) network event by enabling `AggregatedUELocChanges` feature as defined in 3GPP TS 29.512.

The User Location Change event indicates a change in the UE's serving cell and/or serving area (tracking area).

This feature enables the PCF to request and process aggregated user location change notifications from SMF, supporting location-aware policy control and dynamic PCC rule enforcement.

Policy supports handling of the network event triggers as per *3GPP TS 29.512*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Currently, Policy supports the user location change in the following scenarios:
>
> - Interaction between PCF and SMF during SM Policy Association establishment.
> - Enabling per-subscriber feature through PRE policies and operator-defined conditions.
> - Notifications initiated by PCF involving `USER_LOCATION_CH`.

Feature negotiation

When PCF receives SMPolicyAssociation Create request with `AggregatedUELocChanges` set in `suppFeat` attribute and this feature is enabled in PCF, PCF negotiates the feature support with SMF by including `AggregatedUELocChanges` in `suppFeat` attribute in its response to the Create request.

To enable the support for `AggregatedUELocChanges` when SMF sends SM Create requests, `AggregatedUELocChanges` must be added as one of the values of **Override Supported Features** field under **System** section on **PCF Session Management** page in CNC Console.

The support for `AggregatedUELocChanges` feature is indicated with the feature number 42 and the hexadecimal value is 0x020000000000 for **Override Supported Features** in the SM Create request.

Functional capability

When **AggregatedUELocChanges** is enabled, PCF includes `USER_LOCATION_CH` in `policyCtrlReqTriggers` during SMPolicyAssociation Create, enabling the SMF to send updates when relevant location changes occur.

The `USER_LOCATION_CH` event can either be applied to all the subscribers or can be limited based on specific criteria such as DNN, subscriber category, entitlements and operator data. It is possible to control this functionality using Policies.

Following are some examples of how inclusion of `USER_LOCATION_CH` event in Policy Control Request Triggers is influenced by the global configuration and policies:

- Configuration enabled, no policies.
- Configuration enabled, Policy is created to include `USER_LOCATION_CH` event for DNN1, DNN1 is received in the Create request.
- Configuration enabled, Policy is created to include `USER_LOCATION_CH` event for DNN1, DNN2 is received in the Create request.
- Configuration enabled, Policy is created to exclude `USER_LOCATION_CH` event for DNN1, DNN1 is received in the Create request.
- Configuration is disabled, but Policy condition is satisfied.

The Policy evaluation to check whether `USER_LOCATION_CH` event must be included in Policy Control Request Trigger (`policyCtrlReqTriggers`) is carried out when a Create, Update, or UpdateNotify request is received from UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Location-based Policies

The PCF (through PRE) supports the installation, modification, or removal of Policy and Charging Control (PCC) Rules based on location-specific conditions contained in the `userLocationInfo` attribute received from the SMF.

The location conditions to be evaluated include:

- Tracking Area Identifier (TAI)
  - **PLMN ID** (Public Land Mobile Network Identifier)
  - **Tracking Area Code (TAC)**

  TAI enables location-aware policies at the tracking area level.
- Cell Identifier
  - **PLMN ID**
  - **Cell Identity**

  Cell Identifier enables location-aware policies at the specific cell level.

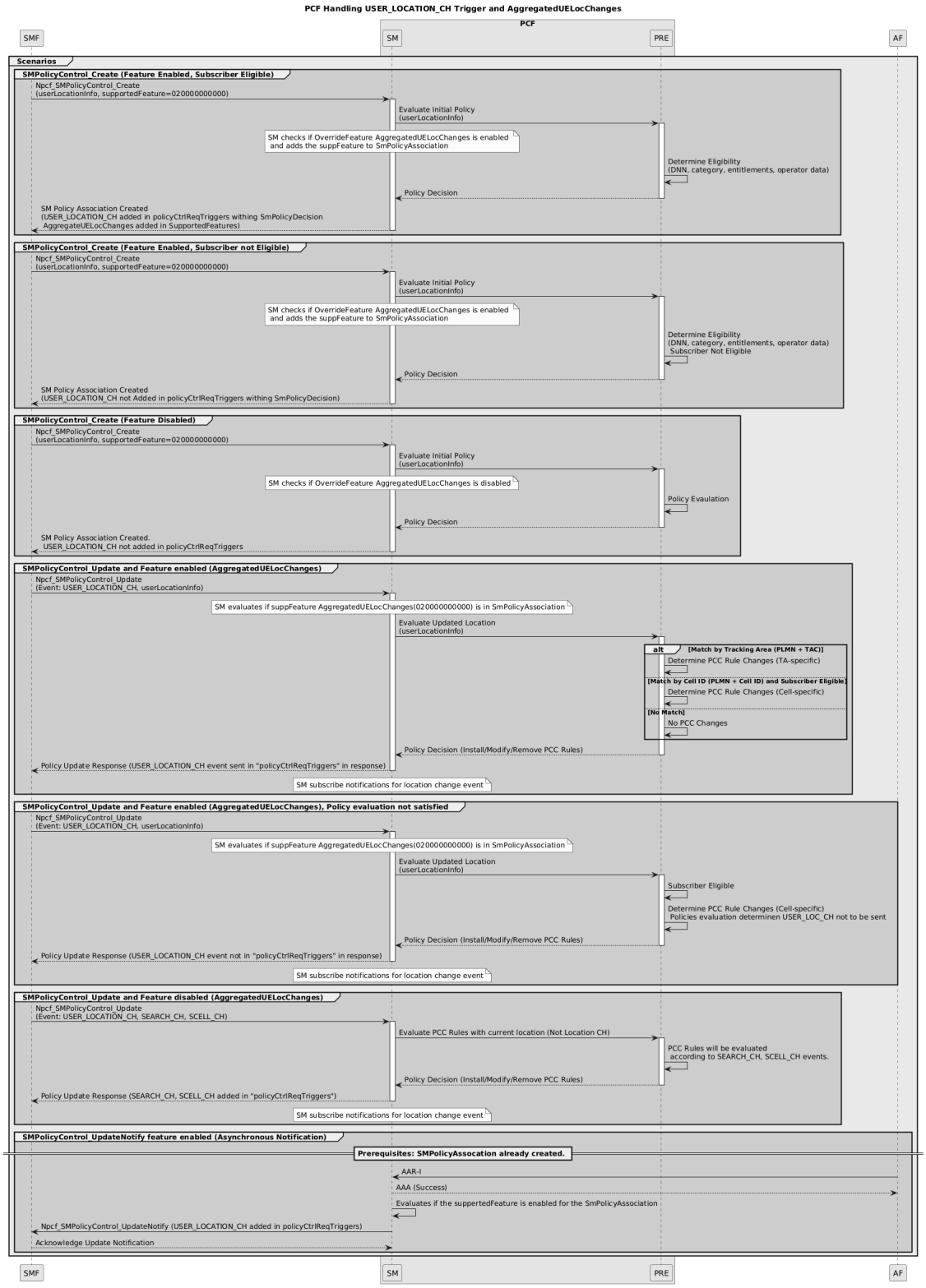
Upon receiving a `USER_LOCATION_CH` trigger with updated `userLocationInfo` in SMPolicyAssociation Update request from SMF:

1. PCF parses the `userLocationInfo` structure to extract TAI and Cell Identity parameters.
2. Per-subscriber eligibility is determined by PRE policies (DNN, category, entitlements, operator data).
3. PRE evaluates the configured policy conditions to determine whether:
   - Existing PCC rules to be modified (for example, change QoS parameters).
   - New PCC rules to be installed (for example, enable location-specific services).
   - Current PCC rules to be removed (for example, disable services outside the allowed area).
4. If no location-specific policies are matched, PCF maintains the current PCC rules and acknowledges the event without further action.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

Figure 4-42 Support for Handling USER_LOCATION_CH Trigger and AggregatedUELocChanges



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. **SMPolicyControl Create (AggregatedUELocChanges Enabled, Subscriber Eligible)**:
   a. SMF sends `SMPolicyControl_Create` with `userLocationInfo`, `supportedFeature=0x020000000000` to PCF.
   b. PCF evaluates the initial policy for `userLocationInfo`.
   c. PCF checks if the **Override Supported Features** field includes `AggregatedUELocChanges` value and adds the supported feature to `SmPolicyAssociation`.
   d. SM service interacts with PRE to evaluate whether `USER_LOCATION_CH` event needs to be sent or not and then includes it based on the outcome.
   e. PRE evaluates eligibility (DNN, category, entitlements, operator data). Verifies that the subscriber is `Eligible`.
   f. PCF returns `AggregatedUELocChanges` in `SupportedFeatures` and saves in `SmPolicyAssociation`.

      The response to SMF includes `USER_LOCATION_CH` in `policyCtrlReqTriggers` within `SmPolicyDecision` and `AggregatedUELocChanges` in `suppFeat` of Create Response.
2. **SMPolicyControl Create (AggregatedUELocChanges Enabled, Subscriber Not Eligible)**
   a. SMF sends `SMPolicyControl_Create` with `userLocationInfo`, and `supportedFeature=0x020000000000` to PCF.
   b. PCF evaluates the initial policy for `userLocationInfo`.
   c. PCF checks if the **Override Supported Features** field includes `AggregatedUELocChanges` as one of the values and adds the supported feature to `SmPolicyAssociation`.
   d. SM service interacts with PRE for Policy evaluation.
   e. PRE determines if the conditions to track the user location change event are met. If not eligible, the subscriber is `Not Eligible`.
   f. PCF sends a Policy Decision back to SMF. However, `USER_LOCATION_CH` is not added in `policyCtrlReqTriggers`.
      PCC Rules are assessed based on `userLocationInfo`, if there are any policies existing.
3. **SMPolicyControl Create (AggregatedUELocChanges Disabled)**
   a. SMF sends `SMPolicyControl_Create` with `userLocationInfo`, `supportedFeature=0x020000000000` (feature disabled) to PCF.
   b. PCF evaluates the initial policy.
   c. PCF checks if the **Override Supported Features** field includes `AggregatedUELocChanges` as one of the values.
   d. If `AggregatedUELocChanges` is not present, PCF sends a Policy decision back to SMF. without adding `USER_LOCATION_CH` to `policyCtrlReqTriggers`.
4. **SMPolicyControl Update and AggregatedUELocChanges Enabled**
   a. To notify PCF that a user location change occurred, SMF sends a `SMPolicyControl_Update` request with the following information:
      - `USER_LOCATION_CH` in `reqPolicyReqTriggers` attribute.
      - Current serving area and or cell id with the `userLocationInfo` attribute.

Copyright © 2019, 2026, Oracle and/or its affiliates.

b. PCF checks if negotiated `AggregatedUELocChanges` in `suppFeat` is enabled in `SmPolicyAssociation`. That is, if previously negotiated successfully.

c. If `USER_LOCATION_CH` is received and the feature is enabled, PCF evaluates the updated location (`userLocationInfo`).

d. SM service interacts with PRE to determine whether to install, modify, remove the PCC Rules.
PCF supports assessment and provisioning of the PCC Rules based on the policies designed against the tracking area and Cell identifier received in `userLocationInfo` attribute.

Policy evaluation can either lead to removal of `USER_LOCATION_CH` event or addition of `USER_LOCATION_CH` event in `policyCtrlReqTriggers` along with other events.

e. PRE determines PCC Rule changes by tracking area:

- `TA-based`: By PLMN + TAC
- `Cell-based`: By Cell ID

f. PCF responds to SMF with policy update response (`USER_LOCATION_CH` event in `policyCtrlReqTriggers`).
If there is no change, then `PolicyCtrlReqTrigger` is not sent.

g. If PCF receives the request from SMF with the feature disabled and `USER_LOCATION_CH` received:

i. PCF accepts the request but the handling corresponding to User Location Change shall not be applied.

ii. The PCC Rules are assessed based on `userLocationInfo` for any other network event such as `SAREA_CH` and `SCELL_CH` as applicable.
Other network events, such as `SUCC_RES_ALLO` and `SEARCH_CH` are supported as usual.

5. **SMPolicyControl Update and AggregatedUELocChanges Enabled, Policy Evaluation Not Satisfied**

a. SMF sends `SMPolicyControl_Update` (`USER_LOCATION_CH`, `userLocationInfo`).

b. PCF checks for `AggregatedUELocChanges` in `SmPolicyAssociation`.

c. PCF evaluates updated location (`userLocationInfo`).

d. PRE determines if the conditions to track the User location change event are met.

e. PCF sends Policy decision (install, modify, remove PCC Rules).

f. PCF responds with policy update response (no `USER_LOCATION_CH` event in `policyCtrlReqTriggers`).

g. SMF subscribes for location change event notifications.

6. **SMPolicyControl Update and AggregatedUELocChanges Disabled**

a. SMF sends `SMPolicyControl_Update` (`SEARCH_CH`, `SCELL_CH`, `userLocationInfo`).

b. PCF evaluates the current PCC Rules (not Location CH).

c. PCF sends a Policy decision (install, modify, remove PCC Rules).

d. PCF responds with policy update response.

e. SMF subscribes for location change event notifications.

7. **SMPolicyControl Update Notify AggregatedUELocChanges Enabled (Asynchronous Notification)**

Copyright © 2019, 2026, Oracle and/or its affiliates.

a. SmPolicyAssociation already created.
b. AF sends AAR-I or AAR-U message.
c. PCF responds with a AAA Success message.
d. PCF evaluates if the supported feature is enabled for the SmPolicyAssociation.
e. Policy evaluation satisfies the conditions to subscriber for USER_LOCATION_CH event.
f. SMF sends SMPolicyControl_UpdateNotify(USER_LOCATION_CH added in policyCtrlReqTriggers).
g. PCF sends an Acknowledge Update notification.

Upgrade and Rollback Impact

During Rollback scenario, USER_LOCATION_CH is not defined in previous versions, SM service does not negotiate AggregatedUELocChanges supported feature and event USER_LOCATION_CH is not considered during policy evaluation. Event is not sent to SMF to be reported.

Managing Support for USER_LOCATION_CH Event Trigger

Enable

Support for USER_LOCATION_CH event trigger can be enabled based on the following two conditions during the SM Create request:

- Enable the feature: AggregatedUELocChanges must be added as one of the value of **Override Supported Features** field under **System** section on **PCF Session Management** page in CNC Console.
- SMF support is indicated during feature negotiation with **AggregatedUELocChanges** as one of the values of **supportedFeature** attribute. The feature number is 42 and the hexadecimal value is 020000000000. This is the value that PCF received from SMF in SMPolicyControl_Create request.

Enable Using REST API

This feature can also be enabled by adding AggregatedUELocChanges value to overrideSupportedFeatures parameter on **Session Management Service** API: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm. For more information, see *Session Management Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

To configure policyCtrlReqTriggers, under the **Policy Control Request Trigger** group on **PCF Session Management** page on CNC Console, select **USER_LOCATION_CH** value for **Default Policy Control Request Triggers** drop-down list. For more information, see PCF Session Management.

Configure Using REST API

The policyCtrlReqTriggers can also be configured by adding USER_LOCATION_CH value to policyControlRequestTrigger parameter on **Session Management Service** API: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm. For more information, see *Session Management Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configuring Policy Projects

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following blocks are used to configure Policy projects to support processing of `UE Location changes` received in the requests from SMF, evaluating and deciding whether to install or modify or remove PCC Rules, and also to configure `policyCtrlReqTriggers`.

- Request Attributes in SMF
- PLMN Id
- Policy Trigger

For more information, see *PCF SM Category* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Observability

The following metrics are used to support this feature:

- usr_loc_ch_supp_feat_in_sm_create_req
- usr_loc_ch_sent_in_response
- usr_loc_ch_in_update_notify
- usr_loc_ch_in_sm_update

For more information, see SM Service Metrics.

4.14 UE Policy Enhancements - Handling of AMF Updates with Change in AMF ID- Interaction with N1N2Communication Session Retry and backoff

Policy enables to dynamically handle AMF changes upon receiving a different GUAMI during an update for a UE Policy Association.

When PCF receives a new GUAMI during an Update from AMF for UEPolicyAssociation, PCF unsubscribes with the old AMF and subscribes with the new one.

PCF discovers the new AMF and performs `N1N2Subscription` with the newly discovered AMF, if the new AMF is in a different set than the old AMF, when changed GUAMI is received by PCF during an Update from AMF for UEPolicyAssociation.

> **Note**
>
> PCF does not subscribe again to the new AMF if it is in the same set, but it performs the AMF and the new AMF is updated for the UEPolicyAssociation session in PCF to which the new or pending `N1N2Transfer` is performed.

After PCF successfully subscribes to the new AMF, PCF sends `N1N2Transfer` messages to the new AMF until there is change in the AMF.

The `N1N2Transfer` can be new or pending which are backed-off.

When a changed GUAMI is received, Policy:

1. Discovers the corresponding AMF using GUAMI (or AMFSetId+RegionID derived from GUAMI) from NRF discovery.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Compares the AMF, AMF set, or AMFSet and Region of the new GUAMI with that of the previous one.

If the new AMF belongs to a different AMF, AMF set, or AMFSet&Region:

1. Policy unsubscribes from the old AMF as part of the transition.
2. Policy performs a `N1N2Subscription` with the newly discovered AMF.
3. Once successfully subscribed, Policy sends `N1N2Transfer` messages (new or pending transfers) to the new AMF.

If the new AMF is in the same AMF, AMF set, or AMFSet and region as the previous one:

1. Policy does not perform a new subscription.

   However, it still performs the AMF discovery.
2. Policy updates the UEPolicyAssociation session context (UE context) with the newly discovered AMF.
3. All the new or pending **N1N2Transfer** messages are sent to this updated AMF.

Important

- As a pre-requisite for this feature, Bulwark service must be enabled.
- Currently, Policy does not support multi-PLMN for routing (route selection, session retry) and resubscription.
- The standard HTTP `Retry-After` header is not considered for handling retries. Only the `retryAfter` Information Element (IE) is supported within the signaling procedures.
- The `RETRY.AFTER.IE.MAX.SECONDS` advanced settings key can be used to configure the maximum `retryAfter` duration in seconds for which the UE Policy service must wait before attempting a reAttempt for a failed N1N2Transfer. The supported duration can be between 1 to 600 seconds.
- Currently, Policy does not support multi-site concurrency scenarios.
- The identification of whether a newly discovered AMF belongs to the same or different AMF set must be reliable to avoid unnecessary re-subscriptions.
- Policy must maintain accurate session context for each UE to handle AMF transitions properly.

The unsubscription with the old AMF and resubscription with the new AMF is performed based on the configuration of **AMF Re-subscription Condition** field under **AMF** section on **PCF UE Policy** page on CNC Console.

Resubscription Trigger Logic Considering Configuration and Inputs for Single PLMN

Following is a sample AMF configuration:

AMF1 (guami1) belongs to NFSet1 "set001.region02.amfset.5gc.mnc480.mcc311"

AMF2 (guami2) belongs to NFSet2 "set002.region02.amfset.5gc.mnc480.mcc311"

AMF3 (guami3) belongs to NFSet3 "set001.region03.amfset.5gc.mnc480.mcc311"

AMF4 (guami4) belongs to NFSet4 "set002.region03.amfset.5gc.mnc480.mcc311"

Copyright © 2019, 2026, Oracle and/or its affiliates.

AMF5 (guami5) belongs to NFSet1 "set001.region02.amfset.5gc.mnc480.mcc311"

It is assumed that each AMF has a unique GUAMI (because AMF1 and AMF5 sharing the same `amfSetId` and `amfRegionId` have different AMF pointers).

> **Note**
>
> When the value of **AMF Re-subscription Condition** field is `DISABLED`, there is no resubscription regardless of the AMF change.

Resubscription Condition : AMF Set ID and AMF Region Id

There is no resubscription when switching between AMFs with the same `amfSetId` and `amfRegionId`.

Resubscription happens when there is any change in `amfSetId` or `amfRegionId` (means different nfSetId in single PLMN).

Table 4-16 Resubscription scenarios with AMF Set ID and AMF Region Id

From \ To	AMF1	AMF2	AMF3	AMF4	AMF5
AMF1	X				X
AMF2		X			
AMF3			X		
AMF4				X	
AMF5	X				X

Resubscription Condition : AMF Set ID

There is no resubscription if `amfSetId` remains the same (for example, both AMF1 and AMF3 have set001).

Resubscription happens if `amfSetId` changes (for example from set001 to set002 or from set002 to set001).

Table 4-17 Resubscription scenarios with AMF Set ID

From \ To	AMF1	AMF2	AMF3	AMF4	AMF5
AMF1	X		X		X
AMF2		X		X	
AMF3	X		X		X
AMF4		X		X	
AMF5	X		X		X

Resubscription Condition : GUAMI

There is no resubscription when moving within the same AMF (same GUAMI).

Resubscription happens when there is any change in GUAMI triggers resubscription, even if `amfSetId` and `amfRegionId` are same but AMF Pointer differs.

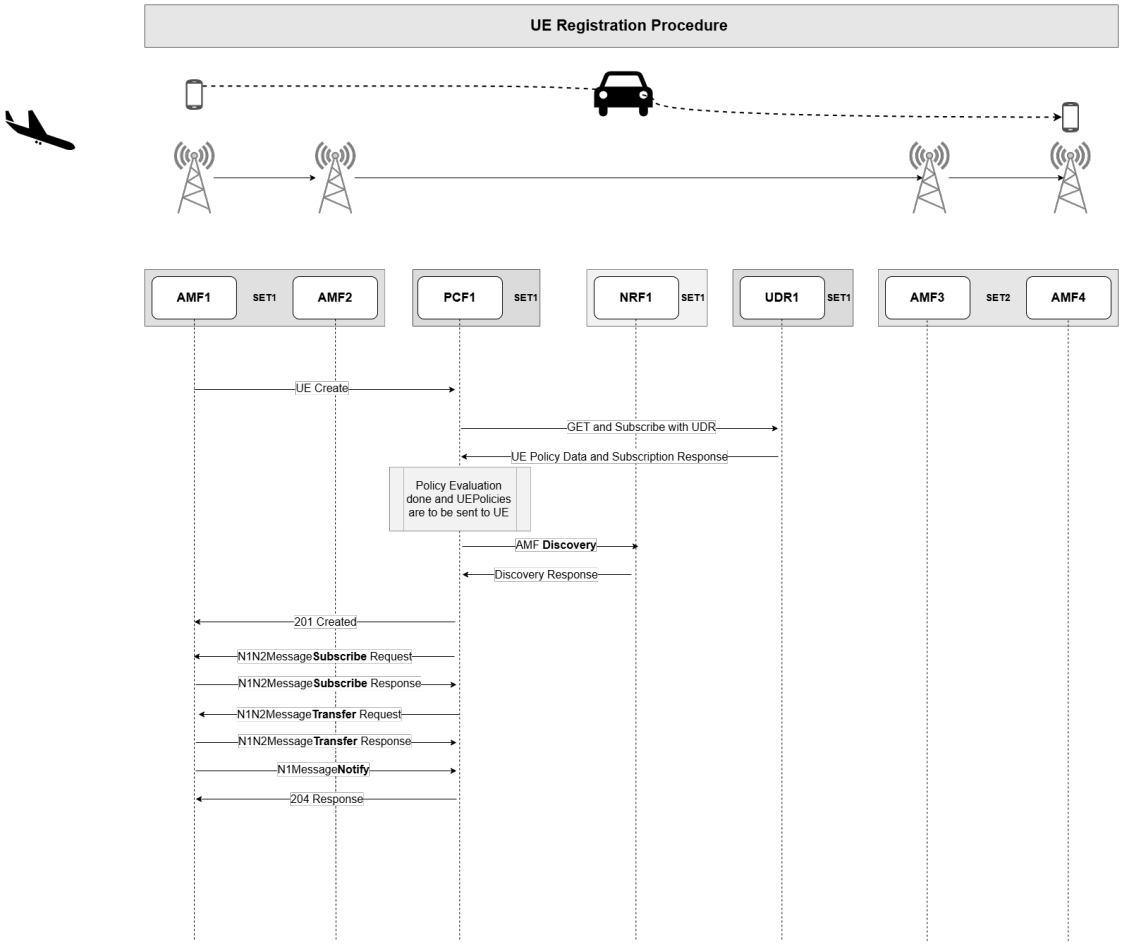
Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-18 Resubscription scenarios with GUAMI

From \ To	AMF1	AMF2	AMF3	AMF4	AMF5
AMF1	X				
AMF2		X			
AMF3			X		
AMF4				X	
AMF5					X

Call Flow

Figure 4-43 UE Registration

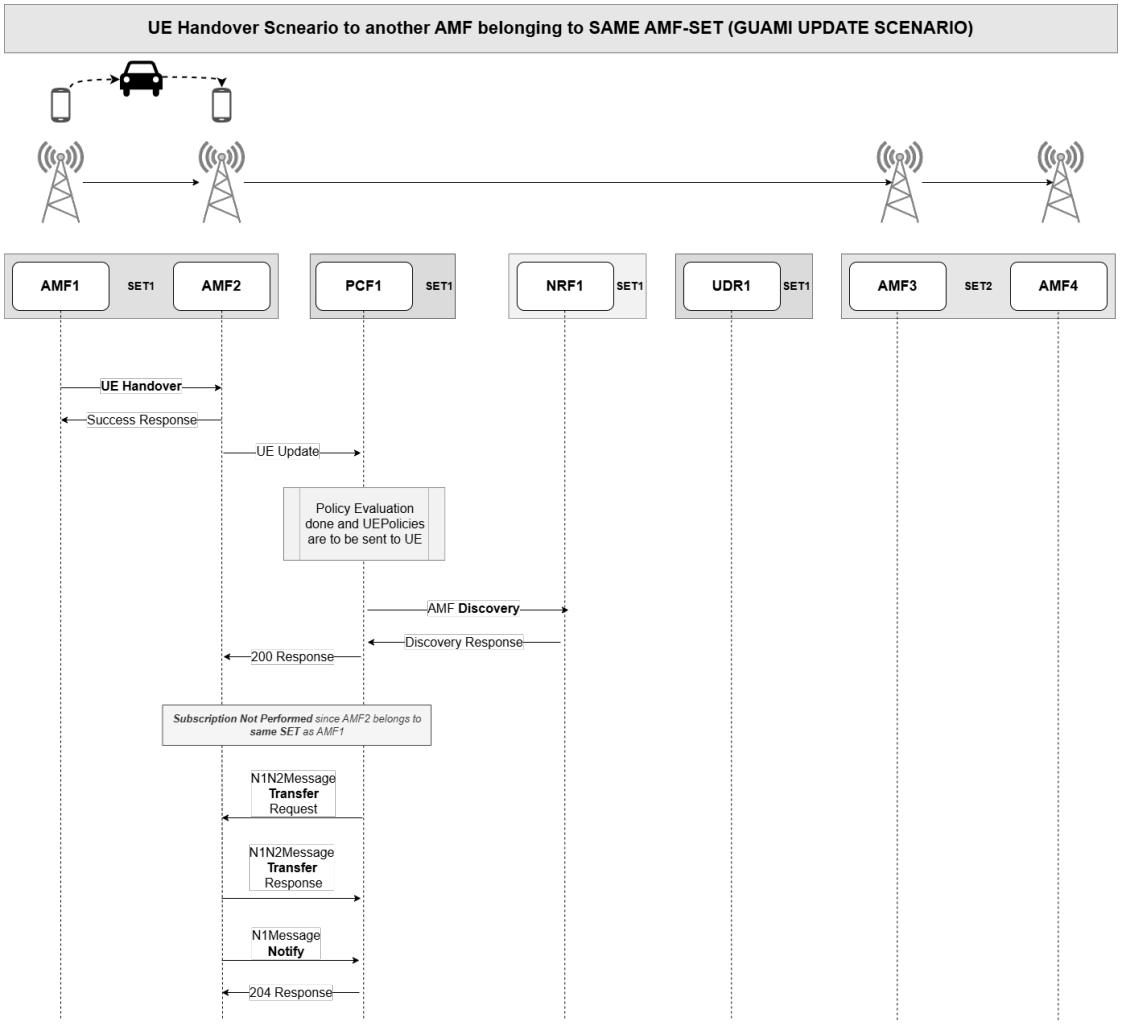


1. AMF1 sends a UE Create request to PCF1 for initiating a new UE registration session.
2. The PCF1 interacts with the UDR1 to get the user's data and subscribes for updates to any user data changes.
3. UDR1 responds back to PCF1 with the requested UE policy data and confirms the subscription for data changes.
4. PCF1 evaluates the received data and determines the UE policies that need to be sent to the AMF and, eventually, to the UE.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. PCF1 queries the NRF1 in order to discover the appropriate AMF that should handle the UE session.
6. NRF1 responds back to PCF1 with the details of the AMFs available for handling the UE registration.
7. PCF1 sends a confirmation back to the originating AMF (AMF1), indicating the successful completion of policy setup with a standard HTTP 201 Created response.
8. AMF1 subscribes for N1N2 messages from PCF1 to receive UE-specific policy notifications and instructions.
9. PCF1 responds to AMF1, confirming the subscription to N1N2 messages.
10. PCF1 sends an N1N2 Message Transfer Request to AMF1, to provide UE-specific policies or trigger further actions.
11. AMF1 acknowledges the message transfer to PCF1.
12. AMF1 notifies PCF1 that the N1 message (message between AMF and UE) was delivered to the UE.
13. PCF1 sends a `204 No Content` response back to AMF1, indicating the notification is received and no further content is needed.

Figure 4-44 UE Handover Scenario to another AMF belonging to same AMF SET (GUAMI UPDATE)

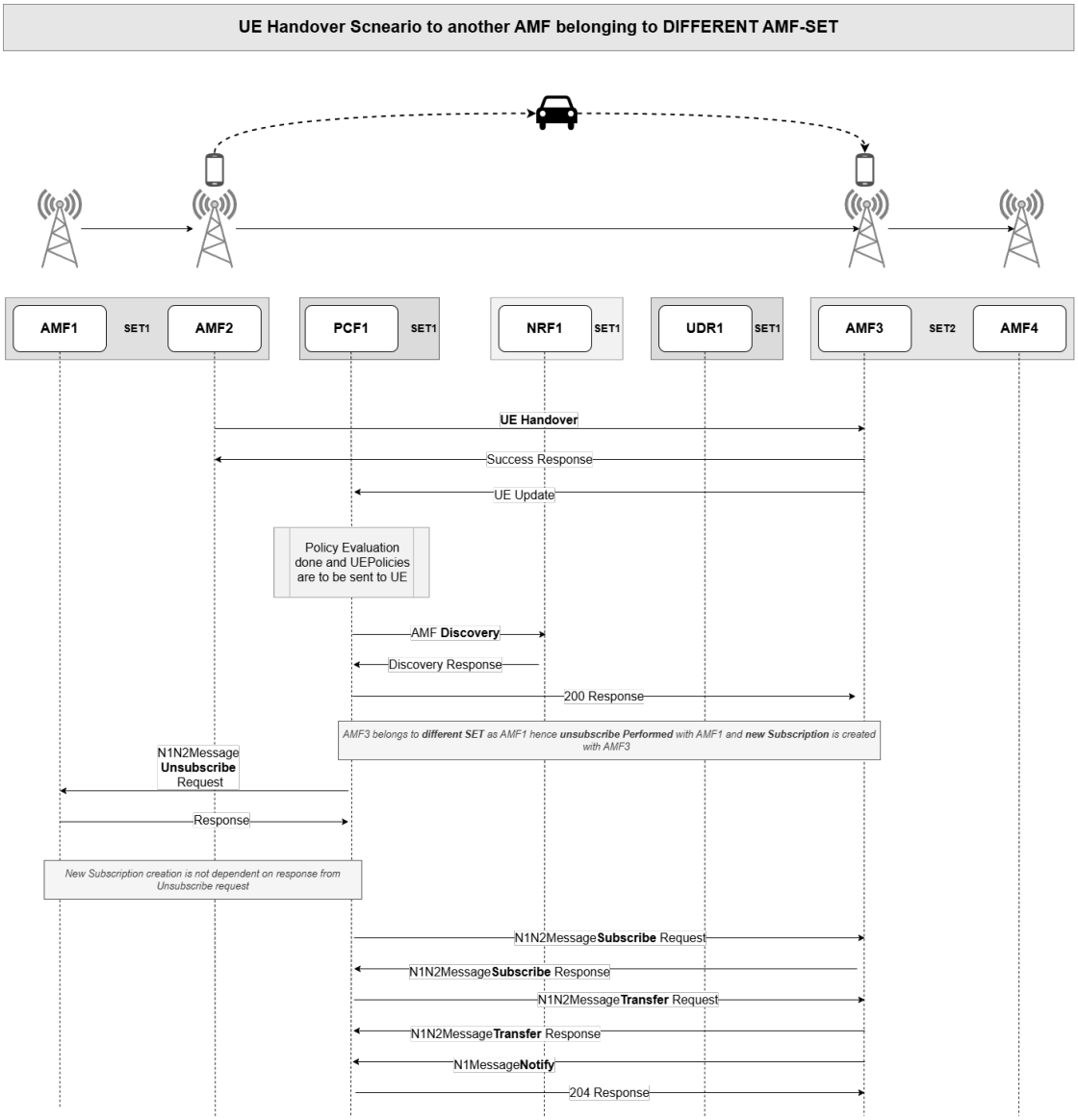


Copyright © 2019, 2026, Oracle and/or its affiliates.

1. The UE initiates a handover request from the current base station (connected to AMF1) to a neighboring base station (to be served by AMF2, both belonging to the same AMF-SET).
2. The handover succeeds and a success response is sent from AMF2, confirming that the UE has connected successfully to the new cell.
3. AMF2 sends a `UE Update` towards PCF1 to inform it about the change in serving AMF for the UE.
4. PCF1 evaluates required policy updates and completes the UE policy evaluation. PCF1 decides which policies and parameters must be communicated back to the UE.
5. PCF1 discovers the network functions and initiates an `AMF Discovery` request towards the NRF1.
6. NRF1 replies with a `Discovery Response`, providing information about the required network functions.
7. Since AMF2 and AMF1 belong to the same AMF-SET, no new N1N2 message subscription is required.
8. PCF1 sends an `N1N2 Message Transfer` request to AMF2, instructing it to transfer Policy-related information to the UE.
9. AMF2 responds with an `N1N2 Message Transfer` response to PCF1, confirming receipt and processing of the request.
10. AMF2 notifies the UE by sending the appropriate `N1 Message Notify`, which usually contains updated policy or configuration information.
11. UE (through AMF2) responds with a `204 Response`, confirming that the new policies or configurations have been received and applied successfully.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-45 UE Handover Scenario to another AMF belonging to different AMF SET



1. The UE initiates a handover from one gNodeB (served by AMF2 in SET1) to a new gNodeB (to be served by AMF3 in SET2).
2. AMF2 sends a `UE Handover` message indicating the handover event to the relevant network entities.
3. A `Success Response` is generated by AMF3 in SET2, confirming the handover procedure has been initiated and processed optimally.
4. A `UE Update` message is sent by AMF3 in SET2 to PCF1 in SET1, updating the state of the UE in the network after the handover.
5. PCF1 in SET1 performs policy evaluation. UEPolicies are determined and are prepared to be sent to the UE after the update.
6. PCF1 in SET1 initiates an AMF Discovery procedure towards NRF1 to determine the appropriate AMF in the target set.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7. NRF1 replies to PCF1 with a `Discovery Response`, providing information about the available AMFs in the target set.
8. PCF1 in SET1 sends a `200 Response` to AMF3 in SET2 to indicate successful update of UE registration with the new AMF (AMF3).
9. Since AMF3 in SET2 belongs to a different AMF-SET than AMF1 in SET1, an unsubscribe request (`N1N2MessageUnsubscribeRequest`) is sent to AMF1 in SET1 to remove the UE's old subscription.

   AMF1 in SET1 processes the unsubscribe request and sends a response.
10. Independent of the unsubscribe response, a new subscription is created with AMF3 in SET2.
    PCF1 in SET1 sends a `N1N2MessageSubscribeRequest` message to AMF3 in SET2.

    AMF3 in SET2 replies with `N1N2MessageSubscribeResponse` confirming the subscription.
11. PCF1 in SET1 sends a `N1N2MessageTransferRequest` message to AMF3 in SET2 to transfer UE context or policy information.
    AMF3 in SET2 responds with `N1N2MessageTransferResponse`, confirming the receipt and processing of the transferred information.
12. AMF3 in SET2 sends a `N1MessageNotify` message to PCF1 in SET1 to notify the UE about the successful subscription and the new policy updates.
13. PCF1 in SET1 sends a `204 Response` message to AMF3 in SET2 to confirm the notification process is complete.

Managing the Policy Support for Dynamic AMF Subscription and N1N2 Message Routing on GUAMI Update

Enable and Configure
The Policy Support for Dynamic AMF Subscription and N1N2 Message Routing on GUAMI Update feature can be enabled and configured using CNC Console as well as REST API.

Configure Using CNC Console

The **AMF Re-subscription Condition** field under **AMF** section on **PCF UE Policy** page for **Service Configurations** in CNC Console is used to enable and configure this feature.

Possible values of **AMF Re-subscription Condition** field are:

- DISABLED
- AMF Set ID and AMF Region ID
- AMF Set ID
- GUAMI

If the value of this field is configured to any of the below mentioned values other than `DISABLED`, when the set ID is different in the UE Update received from AMF, PCF sends unsubscribe to old AMF and subscribes to the new AMF.

For more information, see PCF UE Policy Service.

For more details, see PCF UE Policy Service.

Configure Using REST API

The `amfResubscriptionCondition` parameter under `AMF` section in UE Policy API can be used to configure this feature.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see *UE Policy* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.14.1 UE Policy Enhancements - Handling of AMF Updates with Change in AMF ID- Interaction with N1N2Communication Session Retry and backoff, with retry-after Timer

During mobility of the UEs, the UEs may move to different AMFs, which may be in the same set or different set. When PCF performs N1N2Transfer to send the UE Policy to UE, due to mobility of the UE, the AMF which had the N1N2Subscription cannot reach the UE. AMF pages the UE and if the UE is not reachable, AMF sends a failure with "retryAfter" timer in the payload. During this time, the UE may have moved to another AMF within the same or different AMF/NFSet Or it may be possible that the UE has moved to 4G/Evolved Packet System (EPS).

AMF sends a `504 Gateway Timeout error` indicating `N1N2MessageTransferError` (`UE_NOT_REACHABLE`) and also includes `retryAfter` in the response.

AMF requests the PCF to stop sending the N1/N2 message before timeout, and to retry the N1/N2 message transfer request that was rejected with `504 Gateway timeout error` (`UE_NOT_REACHABLE` cause) after a timeout. As per the `retryAfter` parameter, PCF defers retries for failed N1N2Transfer requests.

> **Note**
>
> This functionality requires UE Policy service to register with the Timer Service.
>
> Also, make sure to enable `CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.ENABLED` Advanced Settings key to enable RetryAfter timer expiry notification.

When Timer Notifications Are Received While RetryAfter IE Is Disabled

Consider a situation when `RetryAfter` timer was scheduled using Timer service before receiving the expiry notification, and the feature toggle was set to `off`. Currently, the timer notification works on the basis of `CANCEL.ON.NEW.TRIGGER` field. If `CANCEL.ON.NEW.TRIGGER` field is set to `true`, the timer is cancelled and the policies are evaluated. But, if the `CANCEL.ON.NEW.TRIGGER` field is configured as `false`, the policy decisions are sequenced and wait for the `retryAfterTimer` to expire. Send the policies with the expiry notification trigger. Even if the feature toggle is off , if the timer is already scheduled using Timer service, the notification is processed normally.

Copyright © 2019, 2026, Oracle and/or its affiliates.

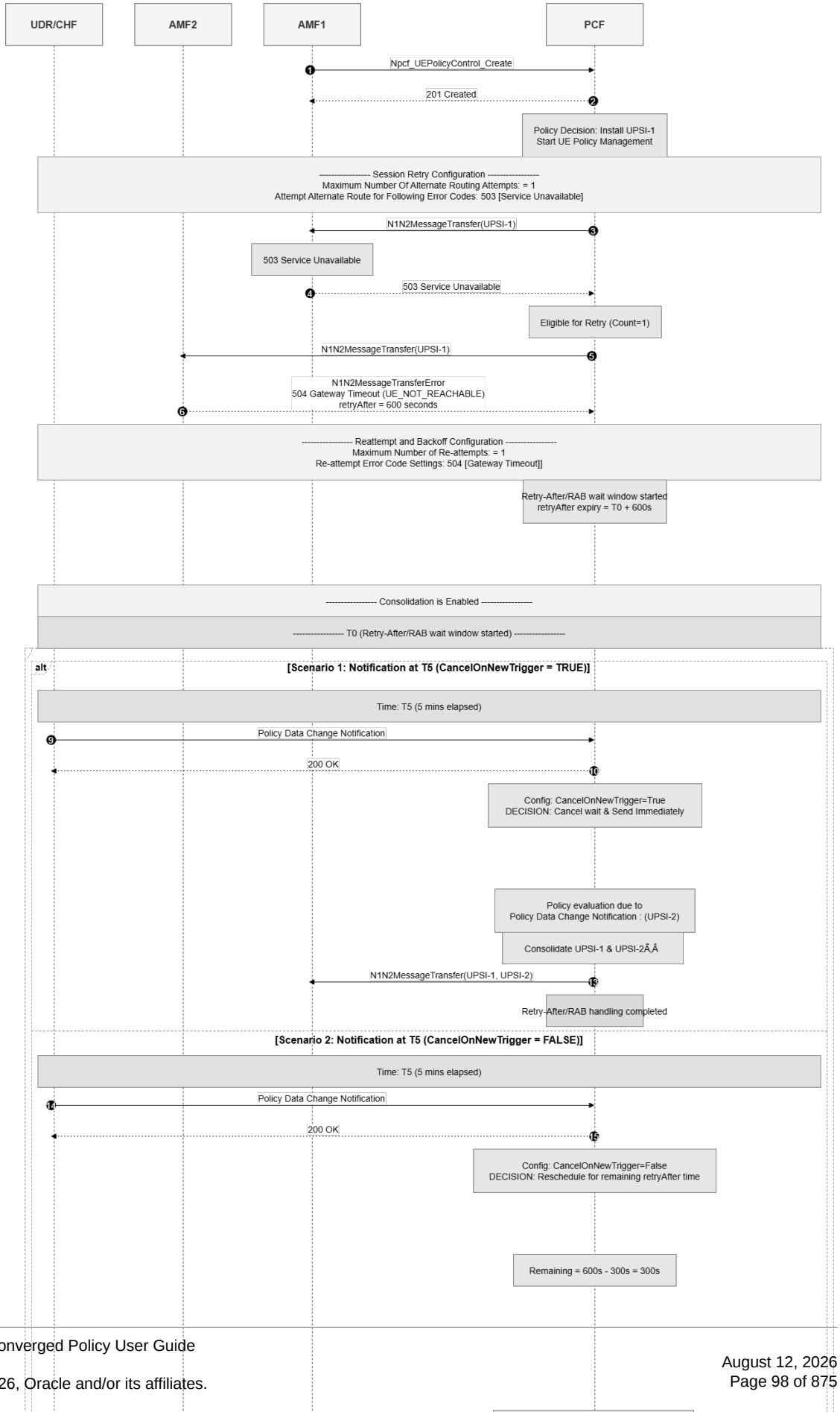
> **Note**
>
> - retryAfter count also called as the persisted alternate-route attempt counter is used by the UE Policy service for retryAfter based retransmissions. It is stored in retryAfter context for persistence and is copied to the routing context during routing context preparation.
> - The maximum retryAfter count is limited by the `Max Alternate Route Count` configured in the **Retry Profile** (retryAfter is a special case of Alternate Routing). Each scheduled retryAfter timer consumes one alternate-route attempt from this limit.
> - When UE receives a new trigger (such as update/delete/new) during an active retryAfter window, UE Policy service evaluates the final policy content to be transferred after expiry and compares it with the last failed transfer transaction:
>   - If the content is the same (same transaction): UE proceeds with the transaction using the same PTI as the failed transaction, and does not reset the retryAfter count (only the remaining alternate-route attempts are allowed).
>   - If the content is different (new transaction): UE increments PTI and resets the retryAfter count (alternate-route attempt budget restarts from the configured max).

Handling N1N2MessageTransferError Responses with "retryAfter"

This sequence diagram describes how the PCF handles an `N1N2MessageTransferError` response from the AMF when the UE is temporarily unreachable and a retryAfter value is provided. It also shows different behaviors when policy data changes occur during the retry period.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-46 RetryAfter IE Scenario



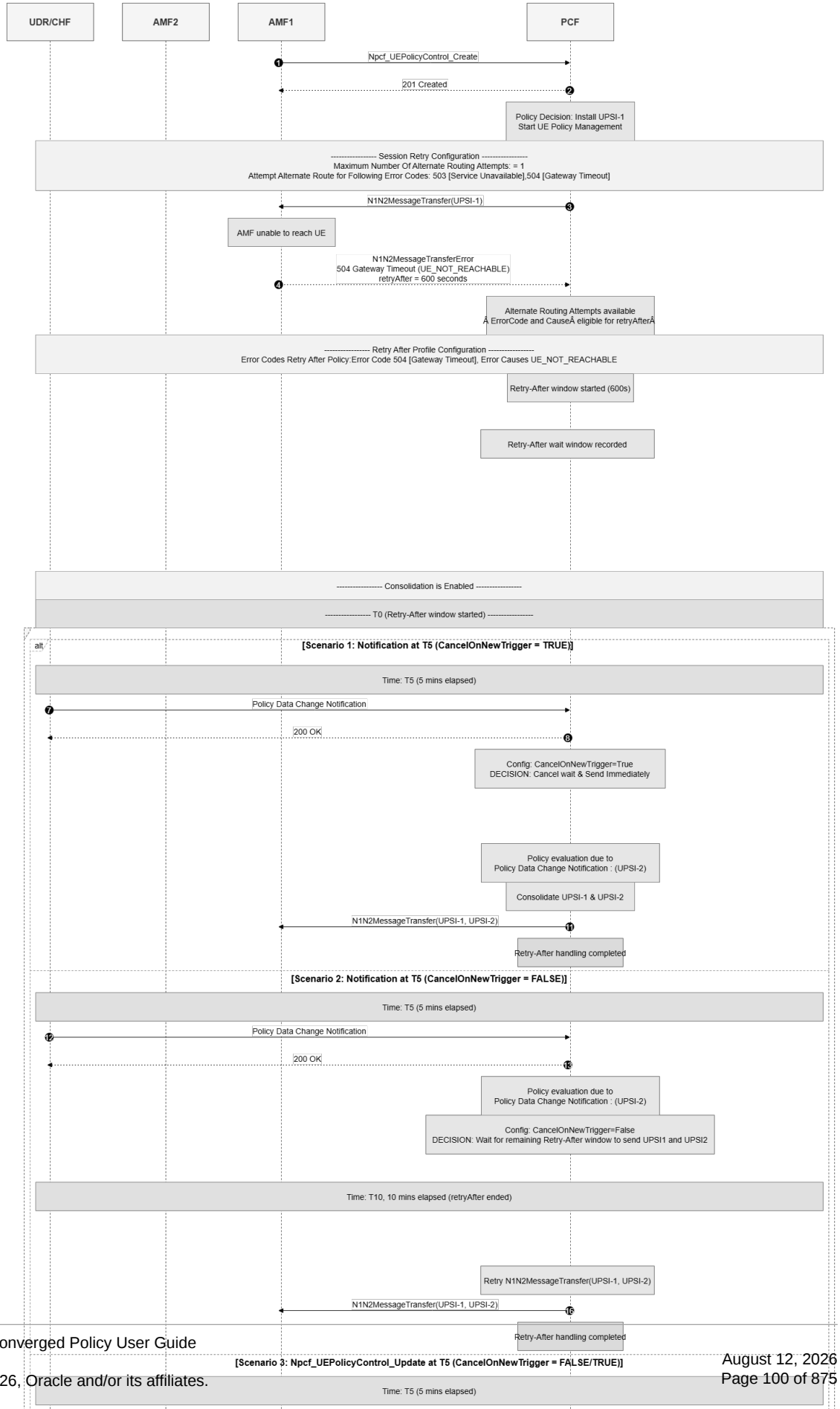
Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> When an AMF returns a retryAfter IE, PCF retries the N1N2Transfer to the same AMF after the specified wait period. The alternate-routing step shown before receipt of retryAfter IE is normal routing behavior and is not a retryAfter retry.

The above RetryAfter IE scenario depicts when AMF1 initially fails to deliver an N1N2 message because the target service is unavailable. The PCF configures retry behavior, including alternate routing error codes and a retryAfter value. When the first transfer fails with `503 Service Unavailable`, the system starts a retryAfter/RAB wait window and consolidates later policy data change notifications during that window. Depending on whether a new trigger cancels the wait or the retryAfter timer expires, the system either sends immediately or reschedules the N1N2 message transfer.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-47 RetryAfter IE with Reattempt and Backoff Scenario



Copyright © 2019, 2026, Oracle and/or its affiliates.

The RetryAfter IE with Reattempt and Backoff scenario focuses on the reattempt or backoff behavior when AMF cannot reach the UE and returns a `504 Gateway Timeout (UE_NOT_REACHABLE)` error with a retryAfter value. The PCF records the retryAfter wait window, consolidates repeated policy updates, and avoids repeatedly sending messages while the wait is active. Once the retryAfter period ends, the system retries the N1N2 transfer. It also shows how later update or delete notifications can cancel the retryAfter wait and trigger immediate sending or cleanup behavior.

Note

- Timer Service Registration happens on a single separate thread, and if registration request fails, it retries after every 10 secs. The maximum number of retries allowed is 30. It can be configured using the following Helm parameters: `TIMERSERVICE_REGISTRATION_RETRY_BACKOFF_SECS` and `TIMERSERVICE_REGISTRATION_MAX_RETRIES`.
- The default retryAfter IE timer expiry-notification rate is 50 per second and the default timer capacity is 50,000.
- Since RetryAfterIE rate and capacity are configured using the advanced settings keys, the maximum allowed rate and capacity is 700 and 360000 respectively.
- The timer duration can be from 1 to 600 seconds, depending on the retryAfter IE value received from AMF.
- Number of retries for:
  - Timer create is 3
  - Timer Delete is 1
  - Timer Notification is 3
- Graceful interval for minimum timer expiry is 5 secs.
- Minimum value of timer that can be created, and can be overridden by advance setting keys is 1 second.
- Timer create rate limit per pod is set as 25 reqs per second.

Upgrade and Rollback Scenario

When UE Policy service is rolled back while Timer Service is in upgraded version: Timer Service sends Timer Expiry Notification towards UE Policy service, and returns `404 NOT FOUND`. The Timer Service deletes the timer Data in the Timer service database (no impact when subsequent call flows arrive, such as UE Update, UDR Notify, or CHF Notify as UE service falls back to performing N1 transfer).

UE Policy service schedules retryAfter internally within the UE Policy service pod.

When Timer service is rolled back while UE Policy service is in upgraded version: UE Policy service sends Timer Create towards Timer service in a usual way and Timer Service saves the timer data for retryAfter.

- When retryAfter Expiry is less than the Rollback window, (when Timer service sends Timer Expiry Notification before UE Policy service is rolled back), UE Policy service continues to retransmit N1 message (no impact on the service).
- When retryAfter Expiry is more than the rollback window (when Timer service sends Timer Expiry Notification after UE Policy service is rolled back), Timer service sends Timer Expiry Notification towards UE Policy service. But, returns `404 NOT FOUND`. Therefore, Timer

Copyright © 2019, 2026, Oracle and/or its affiliates.

service deletes the timer data in Timer service database. (There is no impact when subsequent call flows arrive, such as UE Update or UDR Notify, or CHF Notify as the UE Policy service falls back to performing N1 transfer).

After the rollback operation is complete, when UE Policy service and Timer service are both in the rolled back version: UE Policy service continues to schedule retryAfter internally within the UE Policy service pod, considering AMF is still giving error response with retryAfterIE.

Multi-site Scenario

When a UE CREATE request is received at site 1 (which is upgraded), UE Policy service sends Timer Create towards Timer service and retryAfter is backed off.

When site 1 goes down and a UDR Notify request is received at site 2 (which is using older version), UE Policy service sends the N1 transfer immediately. If AMF responds with a transfer error containing retryAfterIE, the UE Policy service internally schedules a retry at the pod level according to the retryAfter value.

Managing Handling of AMF Updates with Change in AMF ID - Interaction with N1N2Communication Session Retry and Backoff with retryAfter Timer

Enable and Configure
Configure Using CNC Console

The retryAfter feature can be enabled using **Enable Retry After IE** field under **Retry After** section on **Retry Profile** page for **Common Data under Service Configurations** on CNC Console.

When **Enable Retry After IE** field is enabled, UE Policy service registers with the Timer service. A new timer, `UE_N1N2MessageTransferErrorRetryAfterIe` is registered and the duration of these timers can be from 1 second to 10 minutes (depending on the retryAfter value).

Also, the following advanced settings keys can be used to configure the retryAfter functionality:

- CANCEL.ON.NEW.TRIGGER.ENABLED
- CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.ENABLED
- CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_LEASE_DURATION
- CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_BACKOFF
- CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_COUNT
- CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_WAIT_DURATION
- RETRY.AFTER.IE.MAX.SECONDS
- RETRY.AFTER.IE.TIMER.CAPACITY
- RETRY.AFTER.IE.TIMER.RATE
- TIMER_EXP_RANGE_MIN_SEC

For more details, see PCF UE Policy Service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> The error codes and causes (not limited to `UE_NOT_REACHABLE with a 504 Gateway Timeout` error is configured using **Attempt Alternate Route for Following Error Codes** on **Retry Profiles** page under **Common Data** for **Service Configurations** on CNC Console. For more details on configuring Retry Profiles, see Retry Profiles.

Configure Using REST API

The retryAfter feature can be enabled using `retryAfterSettings.enableRetryAfterIE` parameter in Retry Profiles API:

For more information, see *UE Policy* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics

The following metrics are used to monitor this feature:

- occnp_ue_update_guami_change_count
- occnp_ue_update_resubscription_condition_change
- occnp_ue_update_guami_change_during_retryafter_cancelled_total
- occnp_ue_delete_during_retryafter_total
- occnp_ue_http_in_request_during_retryafter_total
- occnp_n1n2transfer_error_with_retryafter_seconds
- occnp_n1n2transfer_error_retryafter_invalid_total

For more information, see UE Service Metrics

Alerts

The following alerts are used for this feature:

- UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD
- UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD
- UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MINOR_THRESHOLD
- UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_CRITICAL_THRESHOLD

For more information, see PCF Alerts.

4.15 Expiry Handling for Policy Data Subscriptions

Policy subscribes with UDR to receive notifications on updates to Policy Data stored.

Copyright © 2019, 2026, Oracle and/or its affiliates.

This feature enables Converged Policy to manage the validity and expiry of Policy Data Subscriptions, as defined in 3GPP TS 29.519 Clause 5.4.2.10.

3GPP recommends using an expiry time associated with the subscription, beyond which the subscription is considered as invalid and notifications are no longer initiated.

For this purpose, Policy uses the "expiry" attribute within the PolicyDataSubscription data structure . It detects when a subscription is approaching expiry and trigger renewal of the associated subscription.

Policy supports receipt and handling of the "expiry" attribute in the PolicyDataSubscription data structure, as provided in POST/PUT responses from the UDR, regardless of whether "expiry" was included in the original request.

The "expiry" value returned by the UDR always takes precedence; if not provided, the subscription is considered perpetual (no monitoring/re-subscription needed).

`Notification Rate` provides the maximum rate at which re-subscription requests are sent to UDR.

`Pre_Expiry Period` is the buffer time before expiry when re-subscription attempts begin. This should be in proportionate to expiry set by UDR. For example, 24 to 36 hours for 15 to 30 day expiry and 3 to 4 hours for 3 to 5 day expiry. If expiry is around 15 to 30 days, `Pre_Expiry Period` can be 24 to 36 hrs.

Time between retry attempts during the pre-expiry window is referred to as `Frequency`. To guarantee at least 4 retry intervals before expiry:

```
frequency ≤(expiry − preExpiry) / 4
```

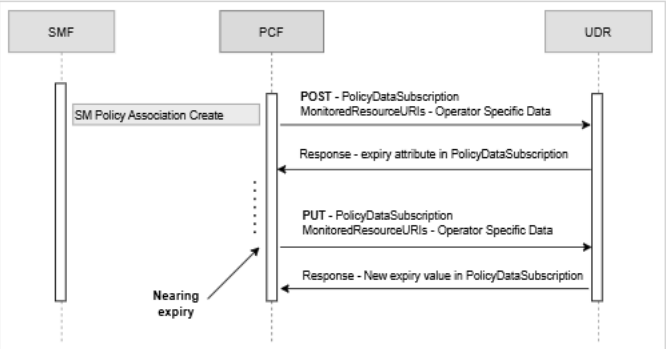
`Max TTL` is the percentage of the total re-subscription or audit attempts available within the pre-expiry window that can be used by the alternate (GR) site if Site 1 cannot handle the attempts. For example, if `Pre_Expiry Period = 3 hours` and `frequency = 30 minutes`, then re-subscription attempts, `x= 6` attempts. With `Max TTL = 50%`, the alternate (GR) site is allowed 3 attempts (x/2) in case of failures at Site 1.

> **Note**
>
> Currently, Policy supports this functionality only for subscriptions to “Operator Specific Data” resource, created during Gx/N7 policy association procedures. This functionality is not supported for AM, UE, and SM Policy Data.

Call Flow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-48 Subscription Monitoring and Re-Subscription



- Policy supports UDR subscription expiry through the audit capability by monitoring the “expiry” time of the subscription.
- During each of the audit cycles, Policy considers the subscriptions that satisfy the below conditions for re-subscriptions:

  ```
  (Expiry time received - Current Time Stamp) <= Period suitable for
  Re_subscription
  ```

  or

  ```
  “Expiry” time received <= Current Time Stamp
  ```

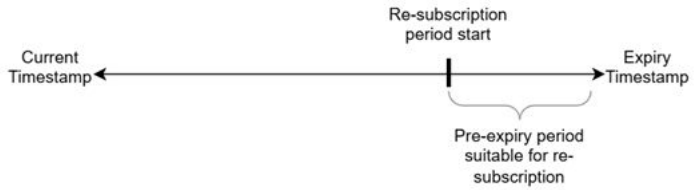
  > **Note**
  >
  > These conditions are checked only during the audit cycles and not when the subscription is created or returned to Policy.

  PCF supports audit of such subscriptions, but immediate re-subscription will not be done; the standard monitoring/re-subscription cycle applies.

  - If identified as already expired, handling follows established procedures like deletion, logging and relevant metric increment .
  - The pre-expiry monitoring window is configurable, enabling retry cycles before expiry .
  - Multiple re-subscription attempts are supported if failures occur before expiry.
  - The feature supports dynamic inclusion or removal of "expiry" in UDR responses throughout the subscription lifecycle.
  - Monitoring/re-subscription continues until the subscription is terminated by policy or "expiry" is omitted in received response from UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-49 Re-subscription Period Chart



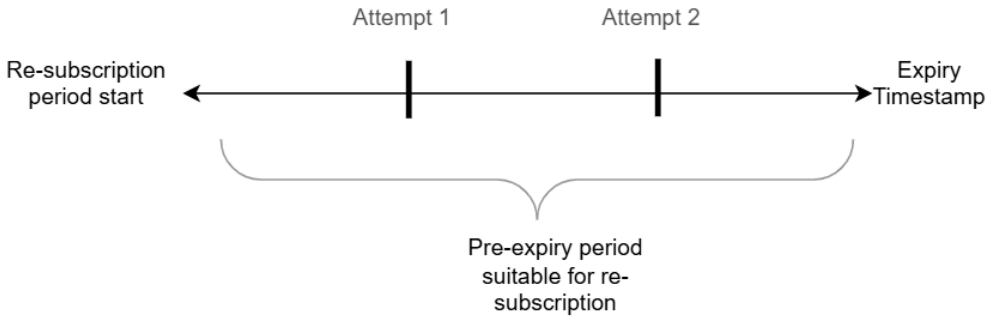
Audit cycles removes stale Policy Subscription Data if no valid sessions exist, taking precedence over expiry status.

Handling Expired Subscriptions: During the audit cycle, if it is identified that the subscription is already expired, then Policy does not attempt a re-subscription. The internal subscription record maintained within Policy is deleted. Policy creates the subscription in UDR by sending a POST request, on next Policy Association Create or Update request for that subscriber. Associated metrics are incremented. Logs (indicate the default log level) are created indicating the Subscriber and Subscription ID.

Error Handling & Logging:

- If Policy receives HTTP 404 error during re-subscription, Policy deletes the subscription, logs the event and increments relevant metrics.
- If Policy receives HTTP 5XX and 4XX errors other than 404 error during re-subscription, within the expiry period, Policy generates logs and retries re-subscription. Also, Policy increments relevant metrics.
- Policy indicates that the session retry functionality is achieved through re-attempts of subscription through multiple audit cycles before the expiry, only if the features such as session-retry and alternate route selection are enabled.

Figure 4-50 Re-subscription Attempts



> **Note**
>
> SAL messages are not logged for pre-expiry re-subscription requests that are triggered from audit.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Upgrade and Rollback Impact

Upon software upgrade to a version supporting this functionality or upon enabling the feature, Policy monitors all newly created and updated subscriptions based on their expiry.

To avoid data inconsistency, the feature must be enabled only after all the sites are upgraded.

In case of rollback, the feature must be disabled before rolling back to the previous version.

Managing Expiry Handling for Policy Data Subscriptions

Enable

This feature can be enabled using CNC Console and REST API.

Enable using CNC Console

This feature can be enabled using **Policy Data Subscription Enabled** field under **Policy Data Subscription Expiry** section on **Settings** page for **PDS Service Configurations** in CNC Console.

For more information, see PDS Settings.

Enable using REST API

This feature can be enabled `audit.policyDataSubscriptionExpiry.policyDataSubsEnabled` parameter in PDS Settings API: `{apiRoot}/oc-cnpolicy-configuration/v1/services/pds/pdsSettings`.

For more information, see *PDS Settings* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

This feature can be configured using CNC Console as well as REST API.

Observability

Metrics

The following metrics are used to support Expiry Handling for Policy Data Subscriptions:

- occnp_policy_data_subscription_expiry_status_total
- occnp_policy_data_resubscription_request_total
- occnp_policy_data_resubscription_response_total

For more information, see Policy DS Metrics.

Alerts

The following alerts are used to support Expiry Handling for Policy Data Subscriptions:

- POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MINOR
- POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MAJOR
- POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_CRITICAL
- POLICYDS_EXPIRED_SUBSCRIPTION

For more information, see Common Alerts.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.16 Application Framework Change

Policy supports Micronaut from 25.2.200 onwards.

With this feature, Spring Boot has been replaced with Micronaut as the framework for microservices. Following are the impacts as part of this replacement:

- Updated name of the following Diameter Gateway Metrics:

Table 4-19 Updates in Diameter Gateway Metrics

Old Metric Name	New Metric Name
occnp_diam_pending_requests_total	occnp_diam_pending_requests
occnp_diam_service_overall_processing_time_seconds	occnp_diam_service_overall_processing_time_seconds_bucket

- Updated name of the following PCRF-core Metrics:

Table 4-20 Updates in PCRF-core Metrics

Old Metric Name	New Metric Name
occnp_diam_pending_requests_total	occnp_diam_pending_requests
occnp_http_pending_requests_total	occnp_http_pending_requests

- Updated name of the following Diameter Connector Metrics:

Table 4-21 Updates in Diameter Connector Metrics

Old Metric Name	New Metric Name
occnp_diam_pending_requests_total	occnp_diam_pending_requests
occnp_http_pending_requests_total	occnp_http_pending_requests

- Updated name of the following SM Service Metrics:

Table 4-22 Updates in SM Service Metrics

Old Metric Name	New Metric Name
jvm_gc_overhead_percent	jvm_gc_overhead
jvm_memory_usage_after_gc_percent	jvm_memory_usage_after_gc
occnp_pending_binding_site_takeover_total	occnp_pending_binding_site_takeover
occnp_lease_duration_seconds	occnp_lease_duration_seconds_bucket

- Updated name of the following AM Service Metrics:

Table 4-23 Updates in AM Service Metrics

Old Metric Name	New Metric Name
occnp_lease_duration_seconds	occnp_lease_duration_seconds_bucket

- Updated name of the following UE Service Metrics:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-24 Updates in UE Service Metrics

Old Metric Name	New Metric Name
occnp_lease_duration_seconds	occnp_lease_duration_seconds_bucket

- Updated name of the following NWDAF Agent Metrics:

Table 4-25 Updates in NWDAF Agent Metrics

Old Metric Name	New Metric Name
spring_data_repository_invocations_seconds_sum	data_repository_invocations_seconds_sum
spring_data_repository_invocations_seconds_count	data_repository_invocations_seconds_count
spring_data_repository_invocations_seconds_max	data_repository_invocations_seconds_max

- Updated name of the following Audit Service Metrics:

Table 4-26 Updates in Audit Service Metrics

Old Metric Name	New Metric Name
spring_data_repository_invocations_seconds_sum	data_repository_invocations_seconds_sum
spring_data_repository_invocations_seconds_count	data_repository_invocations_seconds_count
spring_data_repository_invocations_seconds_max	data_repository_invocations_seconds_max

- Updated name of the following Binding Service Metrics:

Table 4-27 Updates in Binding Service Metrics

Old Metric Name	New Metric Name
occnp_http_out_conn_processing_latency_seconds	occnp_http_out_conn_processing_latency_seconds_bucket
occnp_http_in_conn_processing_latency_seconds	occnp_http_in_conn_processing_latency_seconds_bucket

- Updated name of the following PDS Metrics:

Table 4-28 Updates in PDS Metrics

Old Metric Name	New Metric Name
spring_data_repository_invocations_seconds_sum	data_repository_invocations_seconds_sum
spring_data_repository_invocations_seconds_count	data_repository_invocations_seconds_count
spring_data_repository_invocations_seconds_max	data_repository_invocations_seconds_max
occnp_http_out_conn_processing_latency_seconds	occnp_http_out_conn_processing_latency_seconds_bucket

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-28 (Cont.) Updates in PDS Metrics

Old Metric Name	New Metric Name
occnp_http_in_conn_processing_latency_seconds	occnp_http_in_conn_processing_latency_seconds_bucket

- Updated name of the following CM Service Metrics:

Table 4-29 Updates in CM Service Metrics

Old Metric Name	New Metric Name
spring_data_repository_invocations_seconds_sum	data_repository_invocations_seconds_sum
spring_data_repository_invocations_seconds_count	data_repository_invocations_seconds_count
spring_data_repository_invocations_seconds_max	data_repository_invocations_seconds_max

- Updated name of the following usage-mon Metrics:

Table 4-30 Updates in usage-mon Metrics

Old Metric Name	New Metric Name
usage_mon_rollover_def_created	usage_mon_rollover_def_create
occnp_http_pending_requests_total	occnp_http_pending_requests

- Updated name of the following Config Server Metrics:

Table 4-31 Updates in Config Server Metrics

Old Metric Name	New Metric Name
jetty_connections_request_seconds	occnp_config_server_overall_processing_time_seconds
jetty_connections_request_seconds_max	occnp_config_server_overall_processing_time_seconds_max
jetty_connections_messages_in_messages_total	occnp_config_server_overall_processing_time_seconds_count
jetty_connections_messages_out_messages_total	occnp_config_server_overall_processing_time_seconds_count
jetty_threads_busy	executor_active_threads
jetty_threads_config_min	executor_pool_core_threads
jetty_threads_config_max	executor_pool_max_threads
jetty_threads_current	executor_pool_size_threads
jetty_threads_jobs	executor_queued_tasks

- Updated name of the following Common Metrics (applicable to all the services):

Table 4-32 Updates in Common Metrics

Old Metric Name	New Metric Name
jdbc_connections_idle	hikaricp_connections_idle

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-32 (Cont.) Updates in Common Metrics

Old Metric Name	New Metric Name
jdbc_connections_max	hikaricp_connections_max
jdbc_connections_min	hikaricp_connections_min
jdbc_connections_active	hikaricp_connections_active
undertow_worker_queue_size	executor_queued_tasks
undertow_busy_worker_thread_count	executor_active_threads
undertow_worker_pool_max	executor_pool_max_threads
undertow_worker_pool_size	executor_pool_size_threads

- Removed the following metrics:
  - occnp_lease_duration_seconds
  - occnp_http_out_conn_processing_latency_seconds
  - occnp_http_in_conn_processing_latency_seconds
  - occnp_diam_response_latency_seconds
  - occnp_diam_service_overall_processing_time_seconds

> **Note**
>
> The following metrics in the following services are removed:
>
> - **AM Service, SM Service, UE Service:** occnp_lease_duration_seconds
> - **Binding and Policy DS:** occnp_http_out_conn_processing_latency_seconds
> - **Diameter Gateway:** occnp_diam_service_overall_processing_time_seconds
>
> In order to get quantile data, use Prometheus Histogram (which contains bucket). You can use histogram_percentile from PQL to get much more accurate data from the bucket as per the use cases.
> Use the following metrics to fetch the quantile data:
>
> - **AM Service, SM Service, UE Service:** occnp_lease_duration_seconds_bucket
> - **Binding and Policy DS:** occnp_http_out_conn_processing_latency_seconds_bucket
> - **Diameter Gateway:** occnp_diam_service_overall_processing_time_seconds_bucket

- Removed the **Support for Prevention of Requests Accumulation at Undertow Worker Queue** feature.
- Added the following helm parameters for the **TLS 1.3 Support for Kubernetes API Server** feature:
  - global.kubeApiServerTlsEnabled
  - global.kubeApiServerTlsVersion
  - global.kubeApiServerTlsCipherSuites

  For more information about these helm parameters, see *Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Removed the isIpvSixSetup Helm parameter.
- Enum for wrapped_exception dimension in the metric occnp_error_handler_in_total is changed from WebClientResponseException to HttpClientResponseException.

Changes in FluentID and Opensearch to Support Micronaut Logging

Add the following new configurations in config-map for Fluentd:

1. Add below filter in the config-map of fluentd-config-occne-fluentd-opensearch inside 02_filters.conf section using the following commands:

   ```
   kubectl edit cm fluentd-config-occne-fluentd-opensearch -n
       occne-infra
   ```

   After all the </filter> tags, add the below as a last filter:

   ```
   <filter kubernetes.**>
           @id normalize_thrown_extendedStackTrace_object
           @type record_transformer
           enable_ruby true
           <record>
             thrown ${ t=record["thrown"]; if t.is_a?(Hash); if t.key?
   ("extendedStackTrace"); v=t["extendedStackTrace"];
   t["extendedStackTrace"]= v.is_a?(Hash) ? v : (v.is_a?(Array) ?
   {"frames"=>v} : {"message"=>v.to_s}); end; c=t["cause"]; if c.is_a?(Hash)
   && c.key?("extendedStackTrace"); v=c["extendedStackTrace"];
   c["extendedStackTrace"]= v.is_a?(Hash) ? v : (v.is_a?(Array) ?
   {"frames"=>v} : {"message"=>v.to_s}); end; end; t }
   ```

2. Cleanup your indeces using the following commands:

   ```
   GET _cat/indices
   DELETE <index-name>
   ```

3. Restart the Fluentd DaemonSet pods.

   ```
   kubectl get daemonset -n occne-infra
   ```

   ```
   NAME                                          DESIRED   CURRENT   READY   UP-TO-
   DATE   AVAILABLE   NODE SELECTOR            AGE
   occne-egress-controller                            16        16        7
   16          7           <none>                   291d
   occne-fluentd-opensearch                           16        16        16
   16          16          <none>                   291d
   occne-kube-prom-stack-prometheus-node-exporter   19        19        19
   19          19          kubernetes.io/os=linux   291d
   occne-metallb-speaker                              16        16        16
   16          16          kubernetes.io/os=linux   291d
   occne-tracer-jaeger-agent                          16        16        16
   16          16          <none>                   291d
   ```

4. Monitor Fluentd logs.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.17 Support to Display the Text Names of URSP and UPSI Rules in Logs

This feature enhances monitoring capabilities by ensuring that application logs for the UE and PRE services display both the name and the corresponding identifiable hexadecimal ID (UUID) for each User Plane Subscription Information (UPSI) and User Routing Selection Policy (URSP). This feature is only applicable for UPSI/URSP IDs that are in the form of 24 character UUID.

Sample UUID format:

```
d0b2f362-ac20-2935-0007-41d64ce106f0
```

This feature is not required for use cases where UPSI/URSP details are logged in the format,

```
"mcc-mnc-upsc"
```

With this feature, every TRACE/DEBUG/INFO/ERROR/WARN logs that print only UUID(hex), will include the name of corresponding UPSI/URSP UUID. Logs that already contain only the name will remain unchanged.

For Example- **upsiId='d0b2f362-ac20-2935-0007-41d64ce106f0', name='upsiname'**

In order to enable the capability, a new advance setting, **UE.POLICY.ACTION.NAME.AND.ID** is added in UE service. **UE.POLICY.ACTION.NAME.AND.ID** is applicable only to MARKER logs of the "Subscriber Activity Logging" type, and only when this logging is enabled for the specific subscriber. It does not apply to non-MARKER logs. However, updates to the logs will be reflected in non-MARKER logs regardless of the value of **UE.POLICY.ACTION.NAME.AND.ID**.

For more information about the advance setting, **UE.POLICY.ACTION.NAME.AND.ID**, see "Add Advanced Settings Configurations" in the PCF UE Policy Service section.

PRE RESPONSE CHANGE:

PRE Response structure containing **UPSI** or **URSP** rules based on advanced setting **UE.POLICY.ACTION.NAME.AND.ID** such that the UPSI/URSP names are added corresponding to their UUID into the PRE Response payload towards UE service. Following code snippet is a sample of PRE response which will be visible in console logs when you enable Subscriber Activity Logging in CNC Console. For more information about Subscriber Activity Logging, see Subscriber Activity Logging.

```
{
    "actions": [],
    "customAttributeActions": [],
    "variables": {},
    "umActions": [],
    "uePolicyActions": [
        {
            "actionType": "INSTALL",
            "upsiList": [
                {
                    "upsiId": "10b6e993-3993-4ca6-8993-c17e0eef5b49",
```

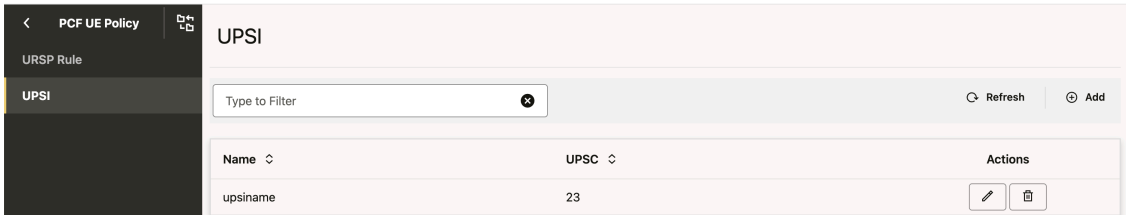

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                    "name": "upsiname"
                }
            ],
            "ruleType": "UPSI"
        }
    ],
    "mandatoryAction": "accept message"

}
```

The following image illustrates the section in the UPSI table where the name of UPSI 'upsiname' is displayed:

Figure 4-51 Displaying the UPSI Details



For more information about UPSI And URSP pages, see PCF UE Policy.

4.18 Support for Sponsored Data Connectivity When AF/NEF Provides the Support Over Policy Authorization Service

The Sponsored Data Connectivity (SDC) defines standard method for Application Function (AF) to provide usage threshold information and requests usage report for sponsored data used by the subscriber. PCF allocates usage monitoring keys, grants SMF usage threshold, and delivers the usage report received from AF/NEF to SMF through PCF when the threshold is reached or the session is terminated.

PCF installs PCC Rules on SMF that tracks the usage and provides a report when the usage threshold is reached or when a session is terminated for the sponsored data.

This capability offers `sponsored` value-added application services to subscribers using a standard based mechanisms that allows associated data flows with a particular sponsor and limit that sponsored data usage.

PCF supports SDC when the AF or Network Exposure Function (NEF) provides this support through the Policy Authorization Service. It allows subscriber application traffic to be sponsored by an application service provider.

PCF handles SDC for a subscriber session when it receives a Policy Authorization (PA) request over the N5 or N30 interface, containing relevant sponsored connectivity data, which includes:

- The sponsor identity (`sponId`), representing the entity sponsoring or being charged for the subscriber's session and data usage.
- The application service provider identity (`aspId`), identifying the provider offering the sponsored service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- The sponsorship status (`sponStatus`), which indicates whether sponsored connectivity is enabled (`SPONSOR_ENABLED`) or disabled (`SPONSOR_DISABLED`).

PCF supports indicating and providing the SDC parameters for inclusion in the PCC rules and charging data profile in update notification requests. This is applicable only if the SMF which created the associated PDU session supports Sponsored Data Connectivity as part of its supported features.

Also, PCF supports the usage monitoring of sponsored data connectivity, when the AF subscribes with the PCF by generating usage monitoring information and sending it to SMF with `UsageThreshold` and `USAGE_REPORT` event provided by AF/NEF.

Based on the information provided by the AF and the supported features by the SMF, PCF determines whether to send a notification to the SMF containing sponsored data connectivity and usage monitoring details, or, if applicable, to reject the request.

> **Note**
>
> This feature is applicable only for SBI requests received as HTTP message from AF/NEF to PCF. Currently, Policy does not support this feature for Rx calls or Diameter messages.

Assumptions/Limitations

- Currently, Policy supports:
  - Receiving the Sponsored Data parameters and status from AF/NEF, optionally, the `USAGE_REPORT` and `usageThreshold` in `Npcf_PolicyAuthorization_Create`, `Npcf_PolicyAuthorization_Subscribe`, and `Npcf_PolicyAuthorization_Update` operation and sends it to SMF in PCC Rules Charging Data, only for Home Subscribers.
  - Deleting PDU session and its associated AF session when Sponsored Data and Usage monitoring data is enabled for the session. But this does not include receiving usage report from SMF in Update or Delete request and does not send it to AF/NEF.
  - Deleting AF session when NEF/AF sends Delete request to PCF with Usage Monitoring event. PCF deletes the AF session and removes the PCC rules towards SMF. But it does not support sending usage monitoring to SMF on receiving it in Delete request from AF/NEF. It does not include receiving usage report from SMF in Update request and does not send it to AF/NEF.
  - The sponId/aspId can not be updated once it has been received, either using PA CREATE or PA UPDATE.
- Currently, Policy does not support:
  - Usage Reporting from SMF.
  - Receiving usage report during Deletion or Termination of the AF session.
  - Support for roaming subscribers.
  - Support for standalone Usage Monitoring between PCF and SMF even if both PCF and SMF support UMC.
  - Any configured or provisioned usage threshold in PCF to SMF, in case AF/NEF does not provide usage threshold and only provides `USAGE_REPORT` event.
  - Error Handling scenarios except few mandatory ones such as 400 and 403 error codes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - Interaction with UDR for `SponsorConnectivityData` or `UsageMonData`.
  - Support for sending default charging data when a PCC rule gets generated based on the attributes received in the request from AF. The only way of doing it is by explicitly installing or overriding an already existing one.
  - The functionality to measure how many sponsors are currently active, how many providers are currently active, and how many sponsored sessions are currently active is out of scope.
  - Only a count of how many requests in total are sponsored, how many requests are sent to the SMF, how many requests are rejected due to sponsor connectivity, and the corresponding alerts are tracked.
- Rating Groups and Online or Offline Charging are provided only using Policy action.
- Bulwark is not supported for PA service.

PCF Interaction with SMF

PCF receives the list of supported features from SMF. This information is included in the `suppFeat` attribute within the SM Create request (`SmPolicyContextData`). If a feature is supported by both SMF and PCF, PCF includes the corresponding feature value in the `suppFeat` attribute in its response (`SmPolicyDecision`) to SMF.

- `SponsoredConnectivity`: indicates support for sponsored data connectivity feature. If SMF supports this feature, PCF authorizes the sponsored data connectivity to the subscriber.
- `UMC`: Indicates that the usage monitoring control is supported.

Sample SM Create request containing `suppFeat` attribute (`SmPolicyContextData`):

```
{

    "3gppPsDataOffStatus": true,
    "accNetChId": {
        "accNetChaIdValue": "01020304",
        "sessionChScope": true
    },
    "accessType": "3GPP_ACCESS",
    "dnn": "dnn1",
    "gpsi": "{{gpsi_1}}",
    "supi": "{{supi_1}}",
    "ipv4Address": "10.1.1.5",
    "ipv6AddressPrefix": "2800:a00:cc01::/64",
    "notificationUri": "http://{{sm_notify_ip}}:{{sm_notify_port}}/smf/
notify",
    "offline": false,
    "online": false,
    "pduSessionId": 1,
    "pduSessionType": "IPV4",
    "pei": "imei-313350100000064",
    "ratType": "NR",
    "servingNetwork": {
        "mcc": "313",
        "mnc": "350"
    },
    "sliceInfo": {
        "sd": "abc123",
        "sst": 11
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    },
    "smPoliciesUpdateNotificationUrl": "npcf-smpolicycontrol/v1/sm-policies/
{ueId}/notify",
    "subsSessAmbr": {
        "downlink": "1000000 Kbps",
        "uplink": "10000 Kbps"
    },
    "chargEntityAddr": {
        "anChargIpv4Addr": "11.111.10.10"
    },
    "InterGrpIds": "group1",
    "ipDomain": "dish.com",
    "subsDefQos": {
        "5qi": 23,
        "arp": {
            "priorityLevel": 3,
            "preemptCap": "NOT_PREEMPT",
            "preemptVuln": "NOT_PREEMPTABLE"
        },
        "priorityLevel": 34
    },
    "numOfPackFilter": 33,
    "chargingCharacteristics": "CHARGING",
    "refQosIndication": true,
    "qosFlowUsage": "IMS_SIG",
    "suppFeat": "0810",
    "traceReq": {
        "traceRef": "23322-ae34a2",
        "traceDepth": "MINIMUM",
        "neTypeList": "32",
        "eventList": "23",
        "collectionEntityIpv4Addr": "12.33.22.11",
        "collectionEntityIpv6Addr": "2001:db8:85a3::37:7334",
        "interfaceList": "e2"
    },
    "ueTimeZone": "+07:00",
    "userLocationInfo": {
        "nrLocation": {
            "ncgi": {
                "nrCellId": "51234a243",
                "plmnId": {
                    "mcc": "313",
                    "mnc": "350"
                }
            },
            "tai": {
                "plmnId": {
                    "mcc": "313",
                    "mnc": "350"
                },
                "tac": "1801"
            }
        },
        "eutraLocation": {
            "tai": {
                "plmnId": {
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                    "mnc": "350",
                    "mcc": "313"
                },
                "tac": "1801"
            },
            "ecgi": {
                "plmnId": {
                    "mnc": "350",
                    "mcc": "313"
                },
                "eutraCellId": "23458da"
            },
            "ageOfLocationInformation": 233,
            "ueLocationTimestamp": "2019-03-13T06:44:14.34Z",
            "geographicalInformation": "AAD1234567890123",
            "geodeticInformation": "AAD1234567890123BCEF",
            "globalNgenbId": {
                "plmnId": {
                    "mnc": "350",
                    "mcc": "313"
                },
                "n3IwfId": "n3iwfid"
            }
        },
        "n3gaLocation": {
            "n3gppTai": {
                "plmnId": {
                    "mnc": "350",
                    "mcc": "313"
                },
                "tac": "1801"
            },
            "n3IwfId": "234",
            "ueIpv4Addr": "10.1.1.5",
            "ueIpv6Addr": "2001:db8:85a3::370:7334",
            "portNumber": 30023
        }
    }
}
```


Sample response for SM Create request by PCF to SMF containing `suppFeat` attribute:


```
{
    "sessRules": {
        "0_1": {
            "authSessAmbr": {
                "uplink": "10000 Kbps",
                "downlink": "1000000 Kbps"
            },
            "authDefQos": {
                "5qi": 23,
                "arp": {
                    "priorityLevel": 3,
                    "preemptCap": "NOT_PREEMPT",
                    "preemptVuln": "NOT_PREEMPTABLE"
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                },
                "priorityLevel": 34
            },
            "sessRuleId": "0_1"
        }
    },
    "pccRules": {
        "0_0": {
            "flowInfos": [
                {
                    "flowDescription": "permit in ip from any to any",
                    "flowDirection": "UPLINK"
                },
                {
                    "flowDescription": "permit out ip from any to any",
                    "flowDirection": "DOWNLINK"
                }
            ],
            "pccRuleId": "0_0",
            "precedence": 3000,
            "refQosData": [
                "qosdata_0"
            ]
        }
    },
    "qosDecs": {
        "qosdata_0": {
            "5qi": 23,
            "qosId": "qosdata_0",
            "arp": {
                "priorityLevel": 3,
                "preemptCap": "NOT_PREEMPT",
                "preemptVuln": "NOT_PREEMPTABLE"
            },
            "priorityLevel": 34
        }
    },
    "policyCtrlReqTriggers": [
        "PLMN_CH",
        "UE_IP_CH",
        "DEF_QOS_CH",
        "AC_TY_CH"
    ],
    "qosFlowUsage": "IMS_SIG",
    "suppFeat": "0810"
}
```

PCF Interaction with AF/NEF

PCF receives the list of supported features from AF/NEF. This information is included in the `suppFeat` attribute in the PA request (`AppSessionContextRequestData`). If a feature is supported by both the AF/NEF and PCF, PCF includes the corresponding feature value in the `suppFeat` attribute in its response (`AppSessionContextRespData`).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-33 PCF Interaction with AF/NEF

Feature number	Feature Name	Description
2	SponsoredConnectivity	Indicates support of sponsored data connectivity. If PCF supports this feature, the AF can provide sponsored data connectivity to the SUPI.
28	PatchCorrection	It indicates that PCF supports the data type AppSessionContextUpdateDataPatch. If PCF supports this feature, the AF can send the request with a patch-type body.

> **Note**
>
> When the PatchCorrection feature is supported and negotiated, but the PCF still receives an Npcf_PolicyAuthorization_Update request using the HTTP PATCH method, containing the AppSessionContextUpdateData data type for the resource representing the Individual Application Session Context, along with modifications to apply:
>
> - The PCF supports processing this request.
> - The PCF encodes the modifications using the JSON Merge Patch format, which is the behavior followed when PatchCorrection is not enabled, not supported, or not negotiated.

Sample PA Create request containing suppFeat and sponsored connectivity and usage monitoring attributes that include sponsored connectivity and usage monitoring attributes.

```
{
    "ascReqData": {
        "afAppId": "urn:urn-7:3gpp-service.ims.icsi.ootel",
        "afChargId": "edc02a5f2721fc7148b3dc023a68e24e",
        "aspId": "asp1",
        "sponId": "sponsor1",
        "sponStatus": "SPONSOR_ENABLED",
        "evSubsc": {
            "events": [
                {
                    "event": "USAGE_REPORT"
                }
            ],
            "notifUri": "<URI>",
            "usgThres": {
                "duration": "1000",
                "totalVolume": "999"
            }
        },
        "medComponents": {
            "1": {
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                "afAppId": "urn:urn-7:3gpp-service.ims.icsi.ootel",
                "fStatus": "ENABLED",
                "marBwDl": "20 Mbps",
                "marBwUl": "20 Mbps",
                "medCompN": 1,
                "medSubComps": {
                    "1": {
                        "fNum": 1,
                        "fDescs": [
                            "permit in ip from 192.168.10.10 to 192.168.11.60
49121",
                            "permit out ip from 192.168.11.60 to
192.168.10.10 36004"
                        ],
                        "fStatus": "ENABLED",
                        "flowUsage": "NO_INFO"
                    },
                    "2": {
                        "fNum": 2,
                        "fDescs": [
                            "permit in ip from 192.168.10.10 to 192.168.11.60
49121",
                            "permit out ip from 192.168.11.60 to
192.168.10.10 36004"
                        ],
                        "fStatus": "ENABLED",
                        "flowUsage": "RTCP"
                    }
                },
                "medType": "AUDIO"
            }
        },
        "notifUri": "<URI>",
        "supi": "imsi-450055000000119",
        "suppFeat": "02",
        "ueIpv4": "45.0.55.140",
        "dnn": "dnn1"
    }
}
```


Sample response for PA Create by PCF containing `suppFeat`:


```
{
    "ascReqData": {
        "medComponents": {
            "1": {
                "afAppId": "urn:urn-7:3gpp-service.ims.icsi.mmtel",
                "medCompN": 1,
                "medSubComps": {
                    "1": {
                        "fNum": 1,
                        "fStatus": "ENABLED",
                        "flowUsage": "NO_INFO"
                    },
                    "2": {
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                        "fNum": 2,
                        "fDescs": [
                            "permit in ip from 192.168.10.10 to 192.168.11.60
49121",
                            "permit out ip from 192.168.11.60 to
192.168.10.10 36004"
                        ],
                        "fStatus": "ENABLED",
                        "flowUsage": "RTCP"
                    }
                },
                "medType": "AUDIO",
                "marBwDl": "20 Mbps",
                "marBwUl": "20 Mbps",
                "fStatus": "ENABLED"
            }
        },
        "notifUri": "<URI>",
        "supi": "imsi-450081000008001",
        "suppFeat": "02",
        "ueIpv4": "10.1.1.5"
    },
    "ascRespData": {
        "suppFeat": "02"
    }
}
```

Sample PA Subscribe request with usage monitoring attributes:

```
{
    "events": [
        {
            "event": "USAGE_REPORT",
            "notifMethod": "EVENT_DETECTION"
        }
    ],
    "notifUri": <URI>,
    "usgThres": {
        "duration": "1000",
        "downlinkVolume": "888"
    }

}
```

Sample PA Update request body with sponsored connectivity and usage monitoring attributes (AppSessionContextUpdateData):

```
{
        "afAppId": "urn:urn-7:3gpp-service.ims.icsi.mmtel",
        "ueIpv6": "2600:1009:1017:4d46::16d1:c3df",
        "evSubsc": {
      "events": [
        {
          "event": "USAGE_REPORT",
          "notifMethod": "EVENT_DETECTION"
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
        }
      ],
      "notifUri": "http://<host:port>/smservicenotify/",
      "usgThres": {
        "duration" : "100",
        "totalVolume" : "100",
        "downlinkVolume" : "100",
        "uplinkVolume" : "100"
      },
      "reqAnis": null
    },
        "medComponents": {
            "1": {
                "codecs": [
                    "uplink\noffer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n",
                    "downlink\nanswer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n"
                ],
                "fStatus": "ENABLED",
                "marBwDl": "38000 Kbps",
                "marBwUl": "38000 Kbps",
                "medCompN": 1,
                "medSubComps": {
                    "1": {
                        "fNum": 1,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ]
                    },
                    "2": {
                        "fNum": 2,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ],
                        "flowUsage": "RTCP"
                    }
                },
                "medType": "AUDIO",
                "rrBw": "2500 Kbps",
                "rsBw": "2500 Kbps"
            },
            "2": {
                "codecs": [
                    "uplink\noffer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n",
                    "downlink\nanswer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n"
                ],
                "fStatus": "ENABLED",
                "marBwDl": "38000 Kbps",
                "marBwUl": "38000 Kbps",
                "medCompN": 2,
                "medSubComps": {
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                    "1": {
                        "fNum": 1,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ]
                    },
                    "2": {
                        "fNum": 2,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ],
                        "flowUsage": "RTCP"
                    }
                },
                "medType": "VIDEO",
                "rrBw": "2500 Kbps",
                "rsBw": "2500 Kbps"
            }
        },
        "resPrio": "PRIO_13",
        "supi": "imsi-450081000008001",
        "gpsi": "msisdn-13710008001",
        "mpsId": "4e532f4550",
        "aspId": "update_asp_id",
    "sponId": "update_spon_id",
    "sponStatus": "SPONSOR_ENABLED"
}
```

Sample PA Update Patch request body with sponsored connectivity and usage monitoring attributes (`AppSessionContextUpdateDataPatch`):

```
{
    "ascReqData": {
        "afAppId": "urn:urn-7:3gpp-service.ims.icsi.mmtel",
        "ueIpv6": "2600:1009:1017:4d46::16d1:c3df",
        "evSubsc": {
      "events": [
        {
          "event": "USAGE_REPORT",
          "notifMethod": "EVENT_DETECTION"
        }
      ],
      "notifUri": "http://<host:port>/smservicenotify/",
      "usgThres": {
        "duration" : "100",
        "totalVolume" : "100",
        "downlinkVolume" : "100",
        "uplinkVolume" : "100"
      },
      "reqAnis": null
    },
        "medComponents": {
            "1": {
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                "codecs": [
                    "uplink\noffer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n",
                    "downlink\nanswer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n"
                ],
                "fStatus": "ENABLED",
                "marBwDl": "38000 Kbps",
                "marBwUl": "38000 Kbps",
                "medCompN": 1,
                "medSubComps": {
                    "1": {
                        "fNum": 1,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ]
                    },
                    "2": {
                        "fNum": 2,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ],
                        "flowUsage": "RTCP"
                    }
                },
                "medType": "AUDIO",
                "rrBw": "2500 Kbps",
                "rsBw": "2500 Kbps"
            },
            "2": {
                "codecs": [
                    "uplink\noffer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n",
                    "downlink\nanswer\nm=audio 8500 RTP/AVP 98\r\na=rtpmap:98
EVRC/8000\r\na=fmtp:98 silencesupp=0\r\na=maxptime:120\r\na=ptime:120\r\n"
                ],
                "fStatus": "ENABLED",
                "marBwDl": "38000 Kbps",
                "marBwUl": "38000 Kbps",
                "medCompN": 2,
                "medSubComps": {
                    "1": {
                        "fNum": 1,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ]
                    },
                    "2": {
                        "fNum": 2,
                        "fDescs": [
                            "permit in 17 from any to any",
                            "permit out 17 from any to any"
                        ],
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                        "flowUsage": "RTCP"
                    }
                },
                "medType": "VIDEO",
                "rrBw": "2500 Kbps",
                "rsBw": "2500 Kbps"
            }
        },
        "resPrio": "PRIO_13",
        "supi": "imsi-450081000008001",
        "gpsi": "msisdn-13710008001",
        "mpsId": "4e532f4550",
        "aspId": "update_asp_id",
    "sponId": "update_spon_id",
    "sponStatus": "SPONSOR_ENABLED"
    }
}
```

Sponsored Connectivity Data in UpdateNotify Request from PCF to SMF

When Sponsored Data Connectivity feature is enabled, PCF allows to configure whether to send the Sponsored Connectivity data in Charging Data to SMF in offline or online mode. For this purpose, `Offline` and `Online` attributes are used.

If the `Offline` attribute in Charging data is enabled, by default, PCF disables the `Online` attribute while sending the Sponsored Connectivity data in Charging Data. The Charging Data is sent with`"sponsorId" = "sponId", "appSvcProvId" = "aspId" and "reportingLevel" = "SPON_CON_LEVEL"`, referred by PCC Rules installed for the AF Association.

The `SmPolicyAssociation` contains `sponsoredConnSession` attribute inside `AppSessionInfos` parameter that is used to identify if sponsored data is sent in a session. When the value of `sponsoredConnSession` attribute is `true`, the SDC parameters are sent in the `UpdateNotify` request to SMF.

UMC Data in UpdateNotify request from PCF to SMF

PCC rules are sent to SMF with the value of `umDecs` and `PolicyControlRequestTrigger` parameters set to *US_RE*.

The `SmPolicyAssociation` contains `umcSession` attribute inside `AppSessionInfos` parameter that is used to identify if usage monitoring data is sent in a session. When the value of `umcSession` attribute is `true`, usage monitoring data is sent in the `UpdateNotify` request to SMF.

Rejection or acceptance of requests

PCF decides whether to accept or reject a PA Create request depending on the attributes received in the request body related to `SponsoredConnectivity` and if it is supported by SMF, AF/NEF and PCF.

When Policy receives a PA Create request, Policy checks if `SponsoredConnectivity` is one of the values of **Override Supported Features** parameter under **System** section in **PCF Session Management** Configuration and **Policy Authorization** configuration.

If the `SponsoredConnectivity` feature is enabled, Policy checks if this feature is mentioned in the received Create request from AF. If the feature is mentioned, it checks if the feature is supported by the SMF that created the PDU session.

Copyright © 2019, 2026, Oracle and/or its affiliates.

If the details of the Sponsored Connectivity feature received are from the same SMF that created the PDU session:

1. If the details of the Sponsored Connectivity feature received are from the same SMF that created the PDU session, Policy saves the details for the AF session and adds them to the `suppFeat` attribute in its response to AF.
2. If the value of `sponStatus` is `SPONSOR_ENABLED`, Policy sends the PCC rules SMF for the sponsored AF session with the corresponding charging data set.
3. If the value of `sponStatus` is `SPONSOR_DISABLED`, Policy checks if `sponId` and `aspId` are present in the request. If these IDs are present, PA Create request is processed.
4. If the `sponId` and `aspId` are not present in the request and if Policy is configured to accept the request when the value of `sponStatus` is `SPONSOR_DISABLED`, PA Create request is processed.
5. If `sponId` and `aspId` are not present in the request and if Policy is not configured to accept the request when the value of `sponStatus` is `SPONSOR_DISABLED`, Policy rejects the Create request with the message `400 MANDATORY_IE_MISSING`.

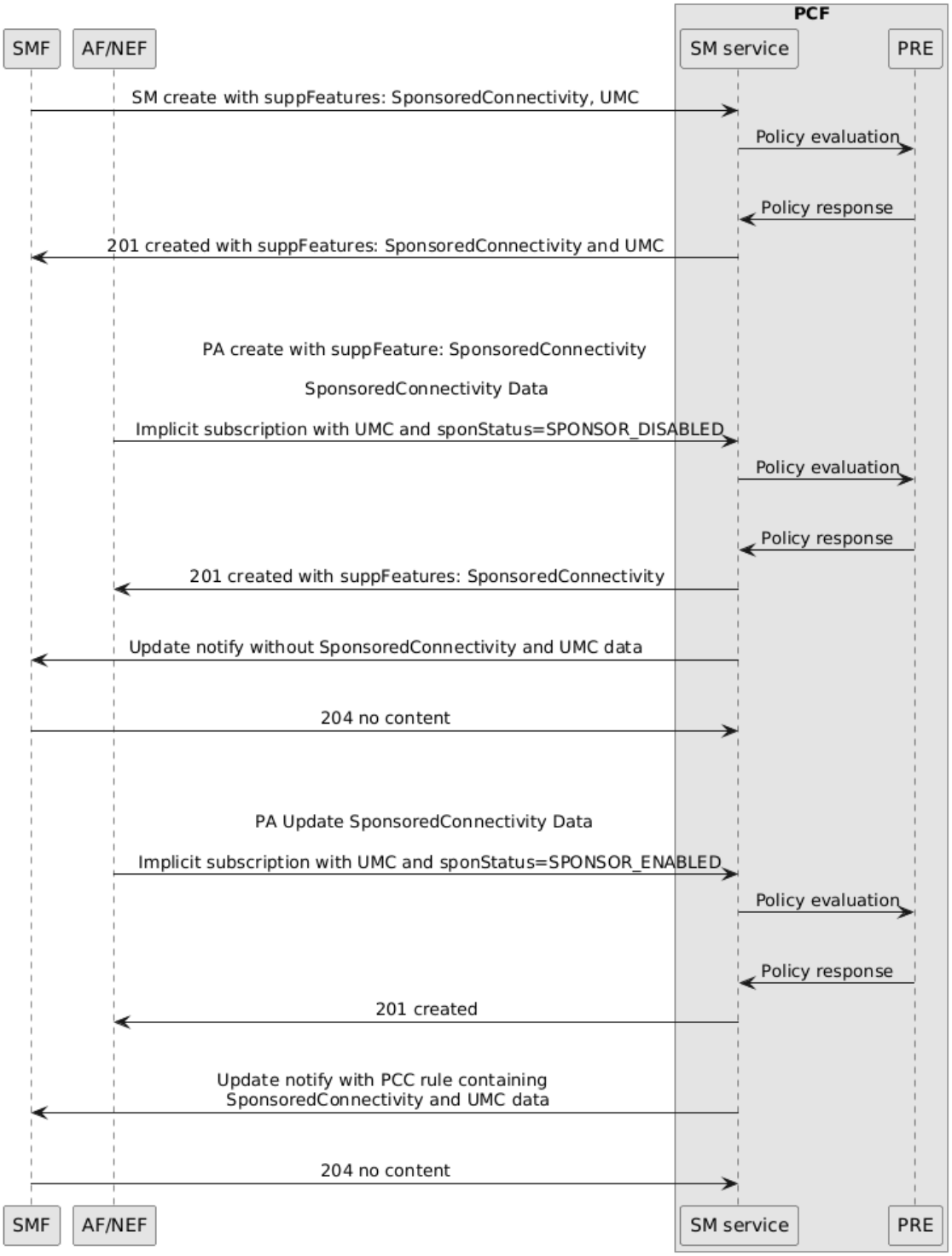
If the details of the Sponsored Connectivity feature received are not from the same SMF that created the PDU session:

1. If the Sponsored Connectivity feature details received are not from the same SMF that created the PDU session, Policy checks if the `SponStatus` is `SPONSOR_ENABLED`, and if `sponId` and `aspId` are present in the request.
2. If yes, Policy rejects the request with `403 REQUESTED_SERVICE_NOT_AUTHORIZED` message.
3. Otherwise, the PA create request is processed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

Figure 4-52 PA create request with sponStatus=SPONSOR_DISABLED implicit subscription and UMC data

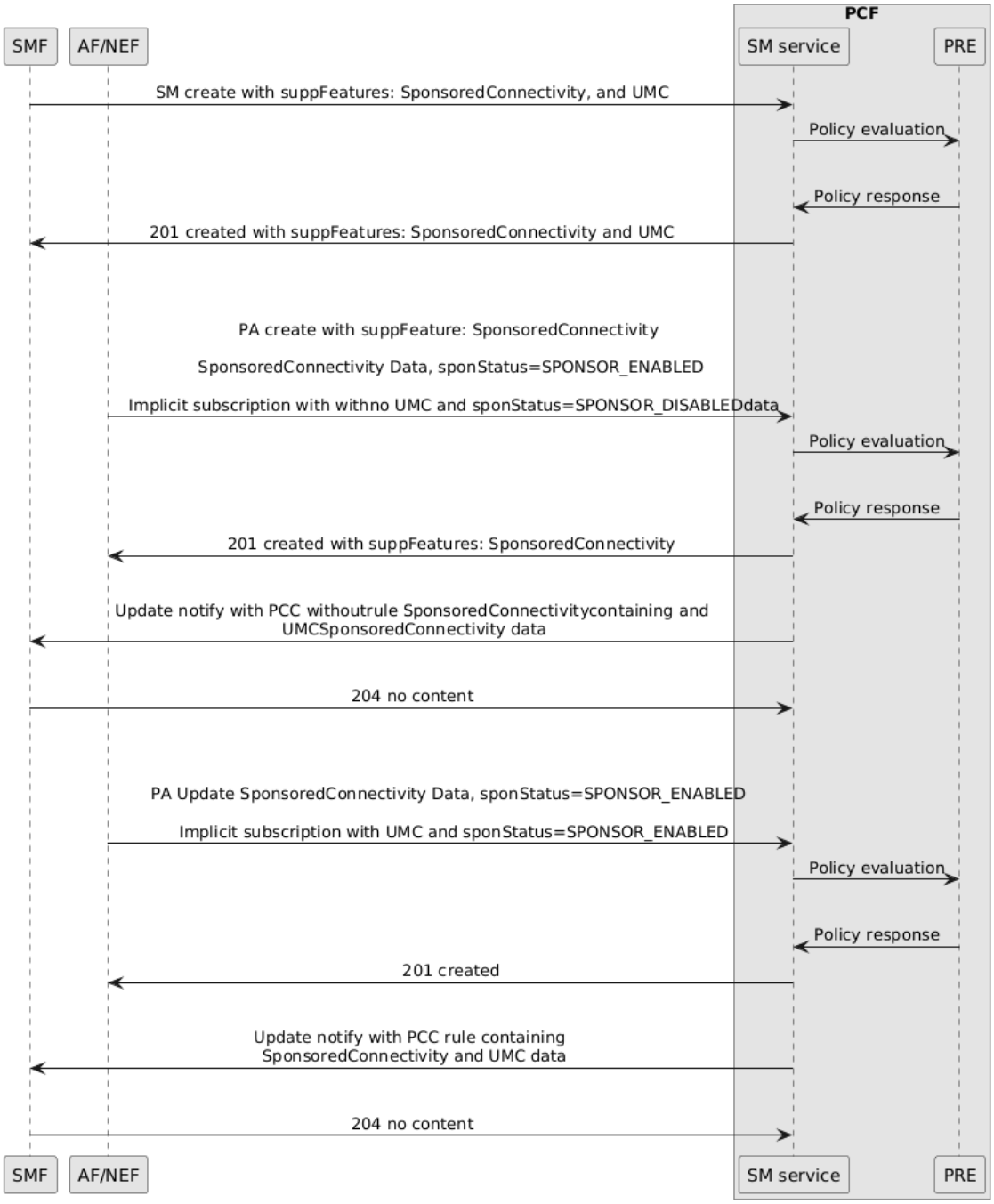


Copyright © 2019, 2026, Oracle and/or its affiliates.

1. SM service receives SM create supporting `SponsoredConnectivity` and UMC from SMF.
2. SM service interacts with PRE for Policy evaluation.
3. SM service responds to SMF with 201 successful response with `suppFeatures: SponsoredConnectivity` and UMC.
4. SM service receives PA create from AF/NEF with `SponsoredConnectivity` and UMC and SC Data with `sponStatus=SPONSOR_DISABLED`.
5. SM service interacts with PRE for Policy evaluation.
6. SM service responds to AF/NEF with 201 successful response with `suppFeatures: SponsoredConnectivity`.
7. SM service sends UpdateNotify to SMF without sponsored connectivity and UMC data and receives a 204 response.
8. SM service receives PA Update from AF/NEF with `SponsoredConnectivity` and implicit subscription with UMC and `sponStatus=SPONSOR_ENABLED`.
9. SM service interacts with PRE for Policy evaluation.
10. SM service responds to AF/NEF with 201 successful response with `suppFeatures: SponsoredConnectivity`.
11. SM service sends UpdateNotify to SMF with PCC rule having sponsored connectivity and UMC data and receives a 204 response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-53 PA create request with implicit subscription but no UMC data



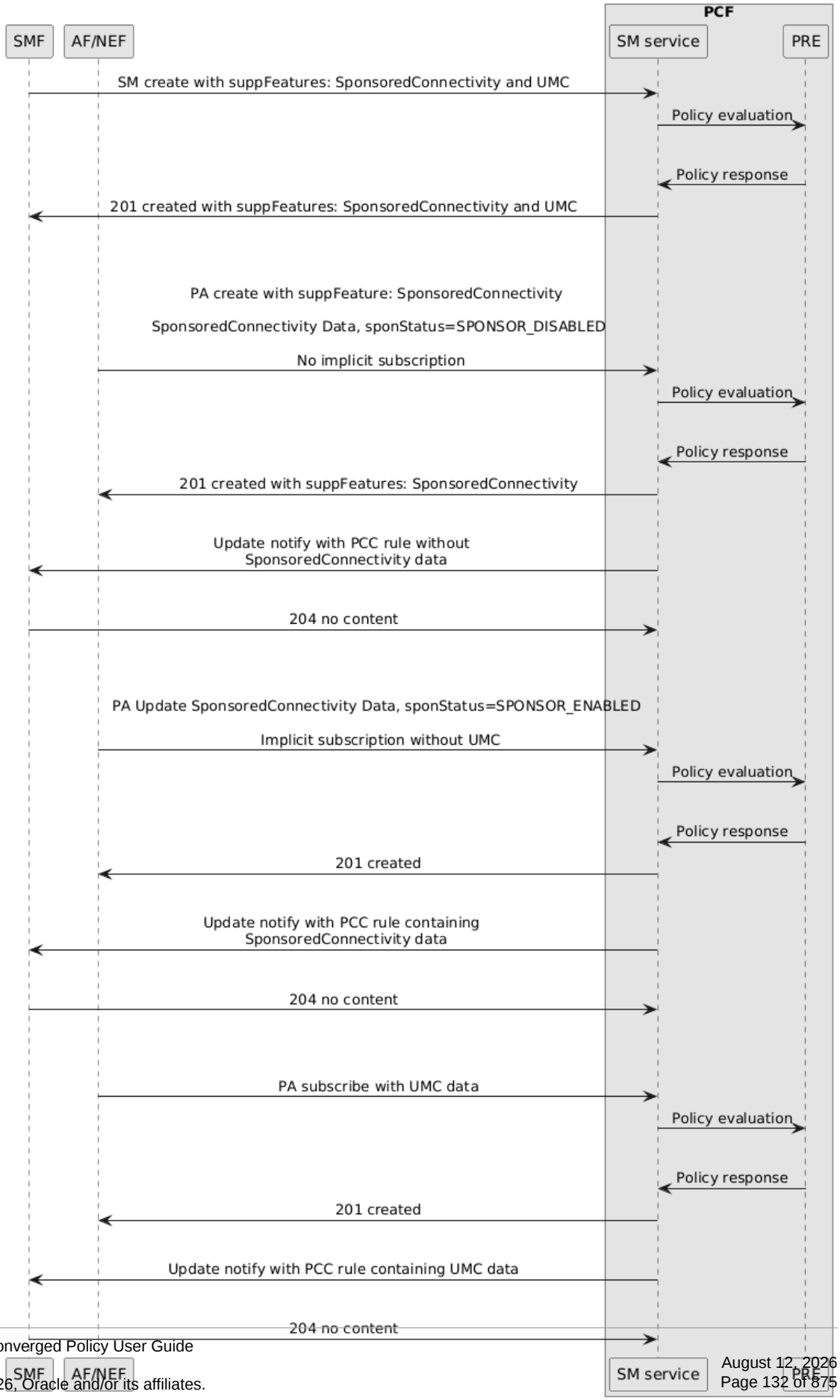
1. SM service receives SM create supporting `SponsoredConnectivity` and UMC from SMF.
2. SM service interacts with PRE for Policy evaluation.
3. SM service responds to SMF with 201 successful response with `suppFeatures: SponsoredConnectivity` and UMC.
4. SM service receives PA create with sponsored connectivity data and `sponstatus=SPONSOR_DISABLED` with implicit subscription but no UMC data from AF/NEF.
5. SM service interacts with PRE for Policy evaluation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

6. SM service responds to AF/NEF with 201 successful response with `suppFeatures: SponsoredConnectivity`.
7. SM service sends UpdateNotify to SMF with PCC without rule having sponsored connectivity and receives a 204 response.
8. SM service receives PA update request with sponsored connectivity data and `sponstatus=SPONSOR_ENABLED` with implicit subscription and UMC data from AF/NEF..
9. SM service interacts with PRE for Policy evaluation.
10. SM service responds to AF/NEF with 201 Created message.
11. SM service sends an UpdateNotify to SMF with PCC rule containing sponsored connectivity and UMC data and receives a 204 no content response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-54 PA create request without implicit subscription

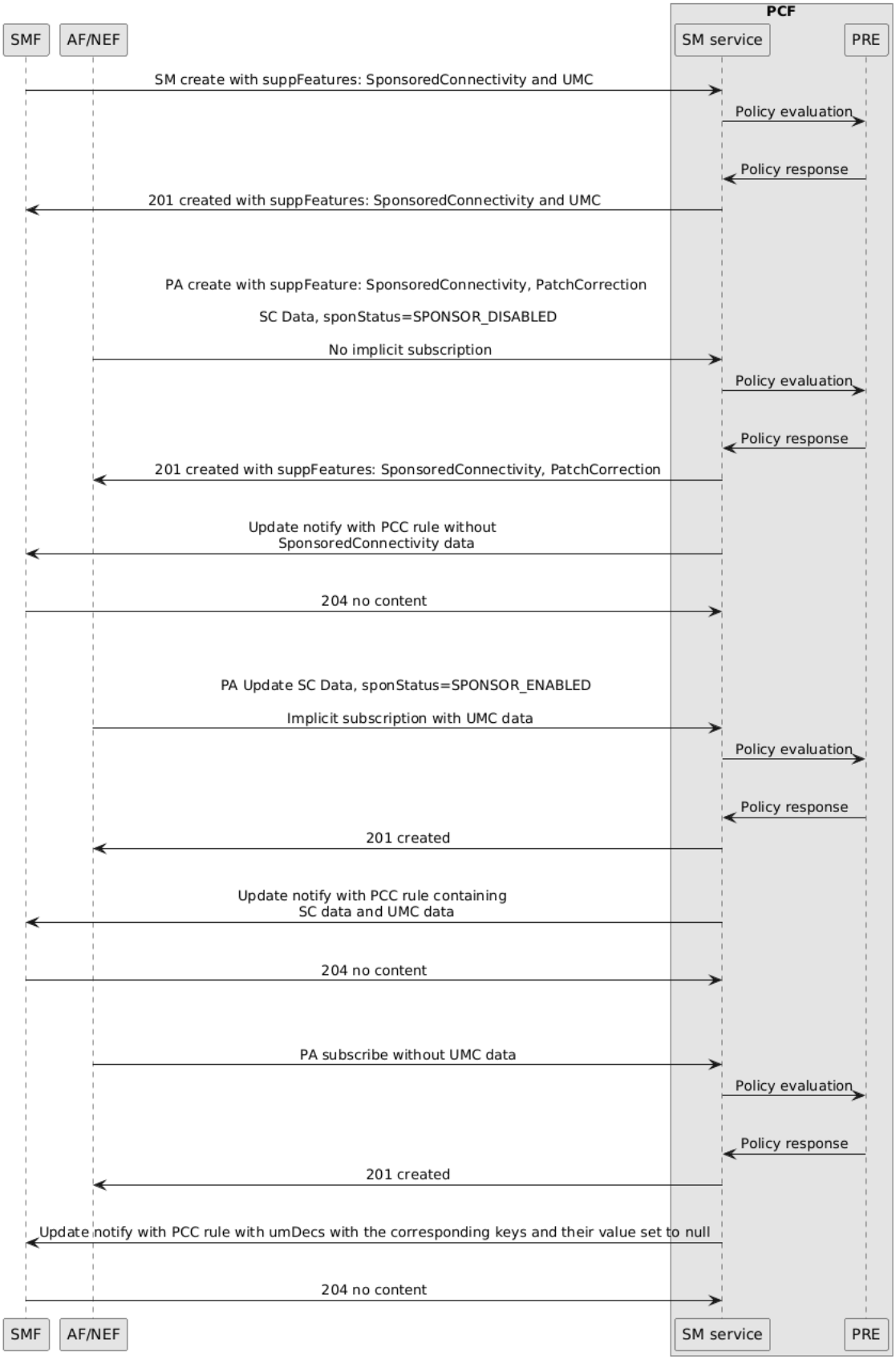


Copyright © 2019, 2026, Oracle and/or its affiliates.

1. SM service receives SM create supporting `SponsoredConnectivity` and UMC from SMF.
2. SM service interacts with PRE for Policy evaluation.
3. SM service responds to SMF with 201 Created response with `suppFeatures: SponsoredConnectivity` and UMC.
4. SM service receives PA create with sponsored connectivity data, `sponStatus=SPONSOR_DISABLED`, and without implicit subscription from AF/NEF.
5. SM service interacts with PRE for Policy evaluation.
6. SM service responds to AF/NEF with 201 Created response with `suppFeatures: SponsoredConnectivity` and without UMC data.
7. SM service sends UpdateNotify to SMF with PCC rule without sponsored connectivity data and receives a 204 response.
8. SM service receives PA update with sponsored connectivity data, `sponStatus=SPONSOR_ENABLED`, implicit subscription without UMC data from AF/NEF.
9. SM service interacts with PRE for Policy evaluation.
10. SM service responds to AF/NEF with 201 Created message.
11. SM service sends an UpdateNotify to SMF with PCC rule containing Sponsored Connectivity data and receives a 204 response.
12. SM service receives PA Subscribe with UMC data from AF/NEF.
13. SM service interacts with PRE for Policy evaluation.
14. SM service responds to AF/NEF with 201 Created message.
15. SM service sends an UpdateNotify to SMF with PCC rule containing UMC data and receives a 204 response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-55 PA create request without implicit subscription, PA update with data patch structure, implicit subscription and UMC data, PA subscribe updating UMC data



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. SM service receives SM create supporting `SponsoredConnectivity` and UMC.
2. SM service interacts with PRE service for Policy evaluation.
3. SM service responds to SMF with 201 Created message containing Sponsored Connectivity Data and UMC Data.
4. SM service receives a PA Create request from AF/NEF supporting `SponsoredConnectivity` and `PatchCorrection` with Sponsored Connectivity data and `sponStatus=SPONSOR_DISABLED`, and without any implicit subscription.
5. SM service interacts with PRE service for Policy evaluation.
6. SM service responds to AF/NEF with 201 Created message containing Sponsored Connectivity Data and `PatchCorrection`.
7. SM service sends an Update Notify to SMF with PCC rule and without Sponsored Connectivity data and receives a 204 no content response.
8. SM service receives a PA Update request with `AppSessionContextUpdateDataPatch` structure, sponsored connectivity data, `sponStatus=SPONSOR_ENABLED` and UMC data from AF/NEF.
9. SM service interacts with PRE service for Policy evaluation.
10. SM service responds to AF/NEF with 201 Created message.
11. SM service sends an Update Notify to SMF with PCC rule having sponsored connectivity and UMC data and receives a 204 no content response.
12. SM service receives a PA subscribe with `usageThreshold` as null values in UMC data from AF/NEF.
13. SM service interacts with PRE service for Policy evaluation.
14. SM service responds to AF/NEF with 201 Created message.
15. SM service sends an Update Notify to SMF with PCC rule deleting the UMC data and receives a 204 no content response.

Managing Support for Sponsored Data Connectivity When AF/NEF Provides the Support Over Policy Authorization Service

Enable

To enable support for Sponsored Data Connectivity when SMF sends SM Create requests, add **SponsoredConnectivity** to **Override Supported Features** field under **System** section on **PCF Session Management** page in CNC Console.

To enable support for **UMC** when SMF sends SM Create requests, add UMC to **Override Supported Features** field under **System** section on **PCF Session Management** page in CNC Console.

For more information, see PCF Session Management.

To enable support for Sponsored Data Connectivity when AF/NEF sends PA create requests, add **SponsoredConnectivity** and **PatchCorrection** to **Override Supported Features** field under **System** section on **PCF Policy Authorization** page in CNC Console.

When **SponsoredConnectivity** is added to **Override Supported Features**, besides being considered as supported by PCF, Sponsored Connectivity is also enabled for PA requests.

For more information, see PCF Policy Authorization.

Configure

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following Advanced Settings keys can be used to configure this feature:

- To send Usage Monitoring data to SMF when both the `USAGE_REPORT` event and the `usagethresholds` are received from AF/NEF, for monitoring the Sponsored Data Connectivity but UMC is not supported by the SMF, add `SYSTEM.SEND_UMC_DATA_WHEN_NOT_SUPPORTED_BY_SMF` Advanced Settings key on **PCF Session Management** page for **Service Configurations** in CNC Console.
  For more information, see PCF Session Management.
- Add the following Advanced Settings key on **PCF Policy Authorization** page for **Service Configurations** in CNC Console:
  - Configure `SYSTEM.ACCEPT_REQUEST_WHEN_MISSING_SPONSORED_CONNECTIVITY_DATA` key to indicate whether to accept or reject the Policy Authorization Create and Policy Authorization Update request.
  - When Sponsored Data connectivity feature is enabled, configure `SYSTEM.ENABLE_ONLINE_ATTRIBUTE_IN_CHARGING_DATA` to enable or disable the `Online` attribute in Charging data.
  - Configure `SYSTEM.INCLUDE_SPONID_ASPID_DIMENSIONS` to control whether the dimensions sponId and aspId are added to the `pa_sponsored_sessions_total` and `pa_sponsored_session_update_notify_total` metrics.
  - Configure `SYSTEM.RETAIN_USAGE_REPORT_WHEN_USG_THRES_NULL` to retain (keeps the previously saved value) the USAGE_REPORT subscription for the NEF/AF.

For more information, see PCF Policy Authorization.

Use the following blocklys to configure support for PRE in evaluating the sponsored data in `AppSessionContextReqData` that it receives from SM Service:

- `AppSessionContextReqData`
- `UsageThreshold`
- `SMF request contains supported feature`
- `AF/NEF request contains supported feature`

Use the following blocklys to add necessary attributes to PCC rules:

- `PCC Rule Dynamic Override`
- `Policy Trigger`

For more information on these blocklys, see *Oracle Communications Cloud Native Core, Policy Design Guide*.

Observability

Metrics

The following metrics are used for this feature:

- `pa_sponsored_sessions_total`
- `pa_sponsored_session_update_notify_total`

For more information, see PA Service Metrics.

The `SPONID_ASPID_PAIR_CARDINALITY_LIMIT` Helm parameter can be used to configure limitation on the cardinality of the metric that can be generated by the `aspID` and `sponId` dimensions.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information on SPONID_ASPID_PAIR_CARDINALITY_LIMIT, see *Configuration for metrics* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Alerts

The following alerts are used for this feature.

- SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERCENT
- SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCENT
- SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCENT
- AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT
- AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT
- AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT

For more information, see PCF Alerts.

4.19 Optimizing N7 Session Lookup for AAR messages in Rx Call flows

> **Important**
>
> This feature is supported only on Oracle Communications Cloud Native Core, Converged Policy used with Oracle Communications Cloud Native Core, Binding Support Function.

Policy supports to optimize the N7 session lookup for AAR-I messages in Rx call flows.

Optimizing N7 session lookup for Rx-AAR-I when BSF is enabled at Binding service

This section describes N7 session lookup process when BSF is enabled and CustomAVP is received from BSF.

Whenever SM service receives a Create request for an Rx session over N7 interface, if this feature is enabled, during binding registration, SM service sends the session details such as SmPolicyAssociationId and contextOwner (PCF-SM) in a header ocnf-service-cookie to Binding Service and BSF. Binding Service stores the details in contextInfoCookie column in contextBinding database. BSF stores the details sent in the cookie in BSF Management service database.

Whenever Policy receives AAR-I request from BSF, the AAR-I request from BSF includes a OCNF-SERVICE-COOKIE Custom AVP that contains the Rx session details such as session owner and the session identifier such as SmPolicyAssociationId (Primary Key).

If OCNF-SERVICE-COOKIE is present in the AAR-I request and the cookie-owner is PCF-SM, Diameter Gateway skips calling the Binding service for primary key lookup. Diameter Gateway processes the details in OCNF-SERVICE-COOKIE Custom AVP and decides whether to route the request to PCRF Core or for Diameter Connector.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> If the cookie-owner is anything apart from `PCF-SM`, Diameter Gateway calls Binding service for Primary key lookup, since this feature is only implemented for PCF-SM.

Diameter Connector converts the Custom AVP to `ocnf-service-cookie-header` header (cookie) and sends it to SM service as part of the PA create request. SM service will use the primary key in the cookie to perform a primary key-based lookup to find the related SM session.

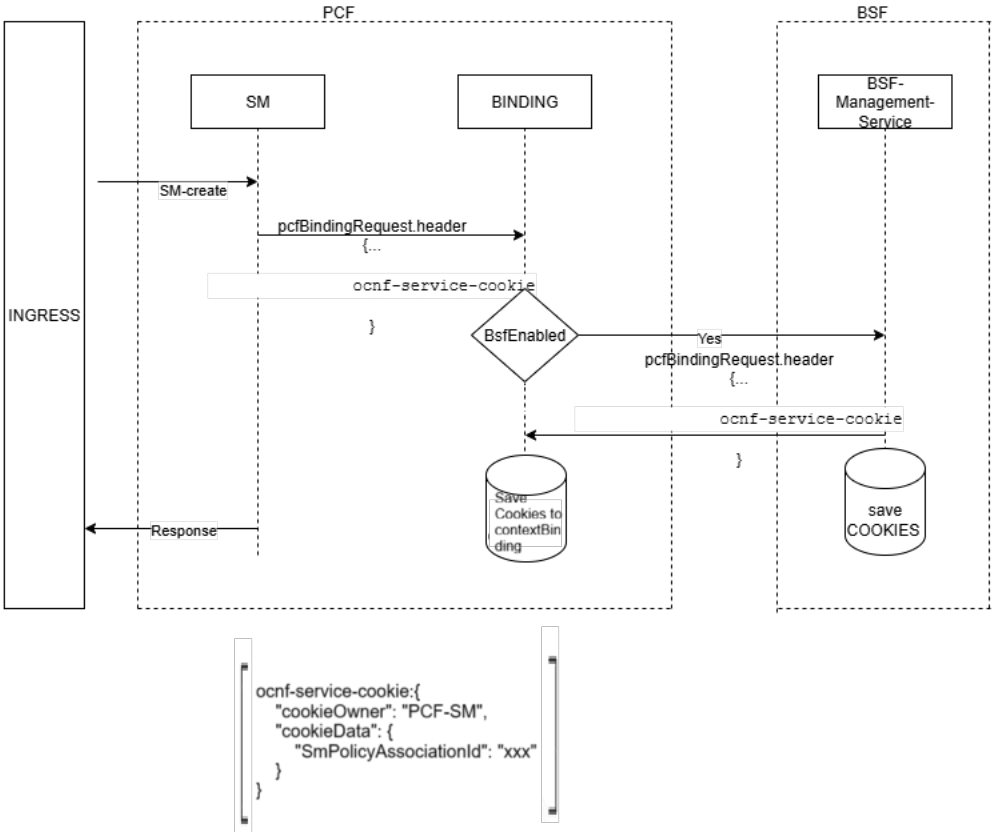
> **Note**
>
> If the N7 session from the cookie is missing or not matching (validation based on binding data available in PA request and binding data available in SM session fetched by `smPolicyAssociationId` present in cookie), Policy performs a secondary key lookup using existing logic.

Data propagation to BSF

SM service receives a Rx session Create request. If Binding is enabled and `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key is enabled for SM service and Diameter Gateway, during binding registration, SM service sends a request to Binding service containing cookie details in `ocnf-service-cookie header`. Binding service stores the details in `contextInfoCookie` column in `contextBinding` database and also sends `ocnf-service-cookie` header in a pcfBinding request to BSF. BSF processes the details in the `ocnf-service-cookie` header and stores them in BSF Management database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-56 ocnf-service-cookie sent to BSF



Sample `ocnf-service-cookie` header that Policy sends to BSF is as follows:

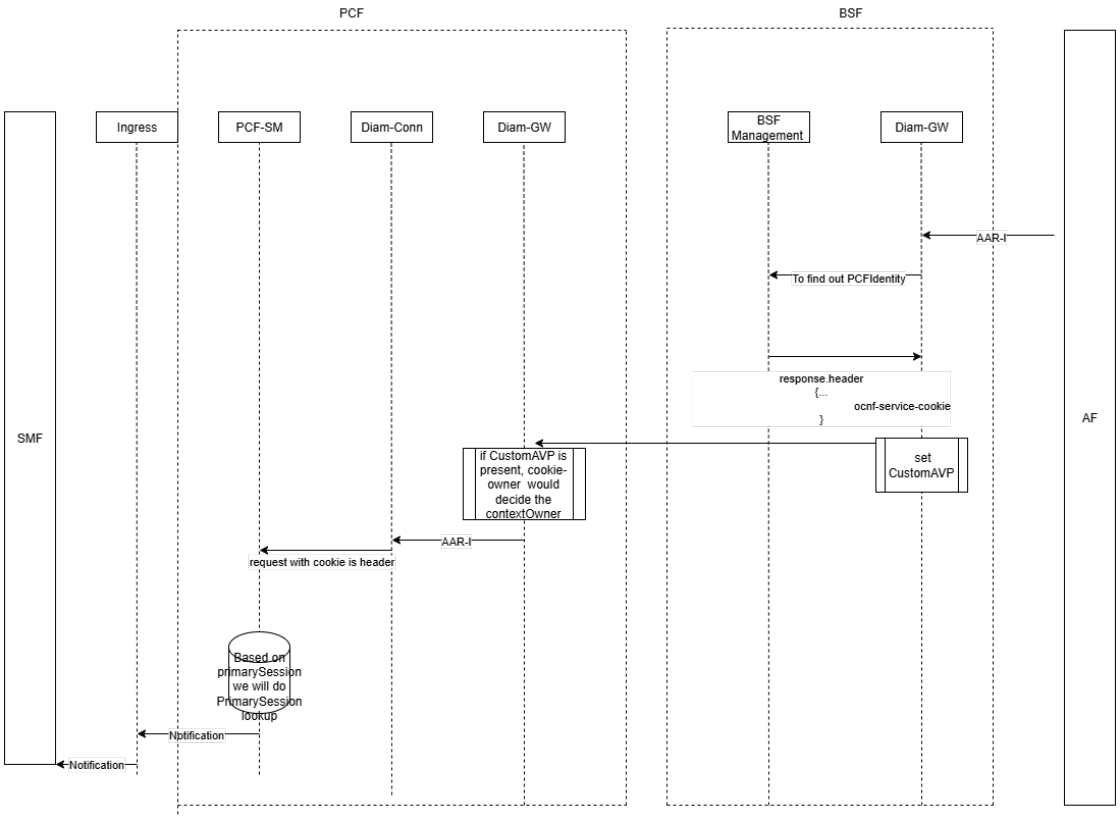
```
ocnf-service-cookie:{
    "cookieOwner": "PCF-SM",
    "cookieData": {
        "SmPolicyAssociationId": "xxx"
    }
}
```

For details on how BSF processes and stores the details in BSF Management service database, see *Support for Optimizing N7 Session Lookup for AAR messages in Rx Call Flows* section in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

`OCNF-SERVICE-COOKIE` Processing and N7 Session Lookup

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-57 OCNF-SERVICE-COOKIE Processing in Policy



When Policy receives an AAR-I request from BSF with `OCNF-SERVICE-COOKIE` Custom AVP, if Binding is enabled, and `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key is enabled for SM service and Diameter Gateway, Diameter gateway extracts the cookie-owner to determine the request ownership by decoding the TLV encoded cookie. Diameter Gateway forwards the request depending on the request owner.

If the request owner is `PCF-SM`, Diameter Connector extracts `OCNF-SERVICE-COOKIE` from Custom AVP and adds it to the HTTP header of the PA Create request. Diameter Connector sends the HTTP request to SM service.

The following is an example for Custom AVP:

```
avp name="OCNF-SERVICE-COOKIE"
code = "3014"
type="octetString"
```

If case of any error while decoding the `OCNF-SERVICE-COOKIE` cookie and adding the details to HTTP header of the PA Create request, Diameter Connector drops the `OCNF-SERVICE-COOKIE`.

SM service parses the `ocnf-service-cookie` header to extract the request owner from the cookie. If it is SM service, it extracts cookie data `smPolicyAssociationId`. SM services validates the session based on PA session binding details.

SM service performs a primary session lookup using the extracted `smPolicyAssociationId`. Otherwise, SM service performs a secondary key lookup.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Optimizing N7 session lookup for Rx-AAR-I when BSF is disabled at Binding service

This section describes N7 session lookup process when BSF is disabled or when `CustomAVP` is not sent by BSF.

During Binding registration, if Binding Service receives `ocnf-service-cookie`, Binding service saves it under `contextInfoCookie` in `contextBinding` database.

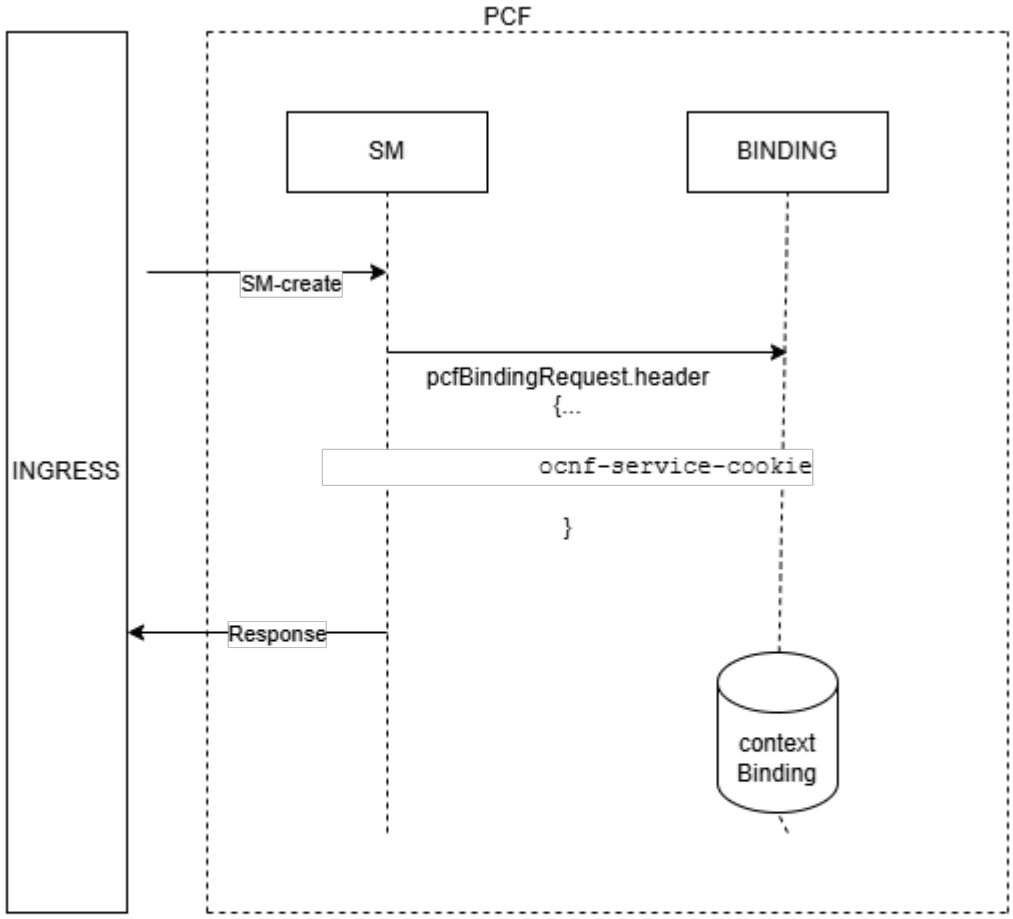
When Policy receives a AAR-I message, Diameter Gateway interacts with Binding service to retrieve the context owner for the request and `ocnf-service-ccokie` is passed in response header if available. Diameter Gateway then forwards the request to Diameter Connector, which extracts the details in the AVP, adds it to the HTTP request of the PA Create request and sends the same to SM service.

> **Note**
>
> This is applicable only for Converged Policy mode, as in PCF mode, Binding service is not queried.
>
> When Policy receives AAR without Request Type AVP, the Diameter Gateway treats it as an initial request and sends it to Binding service. Binding service verifies the dependent context information. If the dependent context information exists, Binding service returns the data. Otherwise, it queries `contextBinding` database. If the cookie is stored in `ContextBinding` for the request, it returns the header.
>
> Diameter Connector verifies if the received AAR request is an initial request or an update request. If it is an AAR-U request, Diameter Connector drops the cookie.

Data Propagation from SM service to Binding service

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-58 ocnf-service-cookie From SM Service is Received by Binding Service




```
ocnf-service-cookie{
    "cookie-owner": "PCF-SM"
    "cookie-data":"{
    smPolicyAssociationId": "XXX"
    }"
  }
}
```

When SM service receives a SM Create request, if `ENABLE_N7_SESSION_LOOKUP_COOKIE` advanced settings key is enabled for SM service, it adds `ocnf-service-cookie` in the `pcfBindingRequest.header` and sends the request to Binding service.

The `ocnf-service-cookie` contains:

- `cookie-owner`
- `cookie-data` that includes `smPolicyAssociationId`)

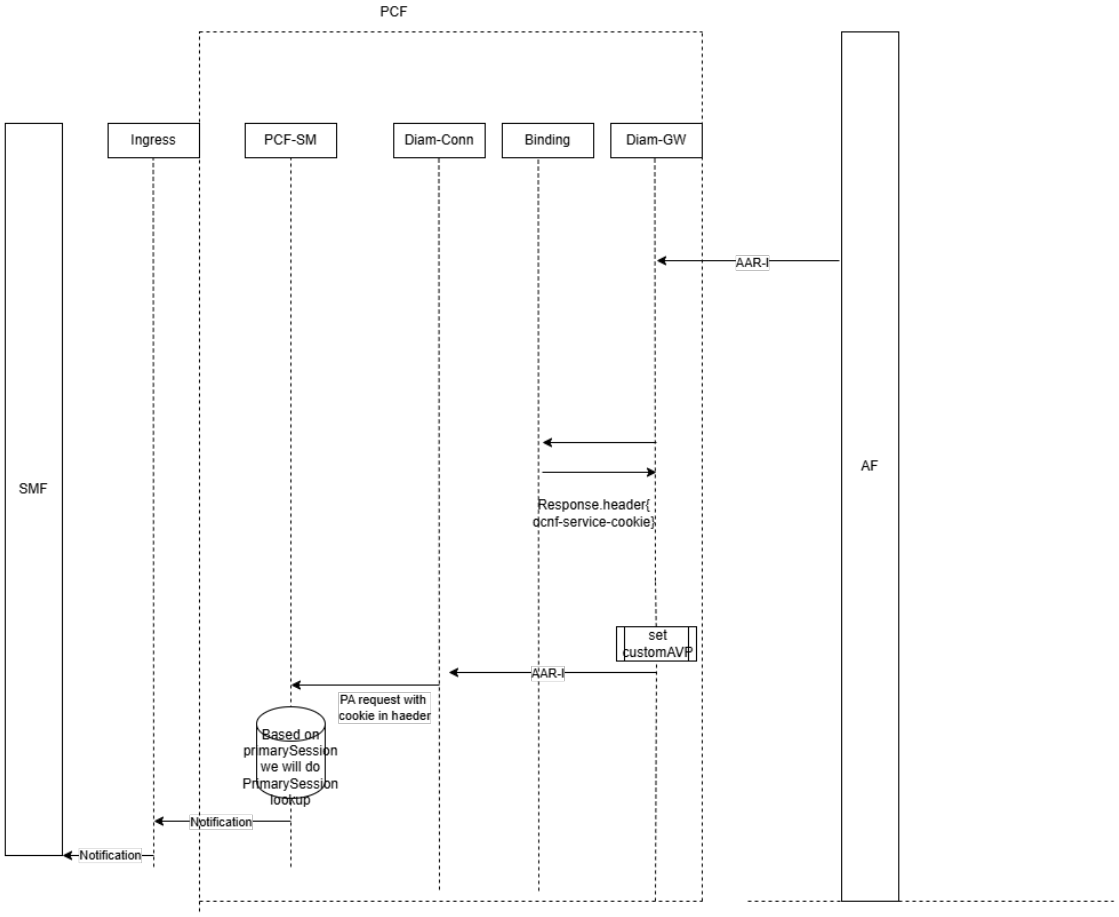
Binding service receives the `ocnf-service-cookie` in the HTTP header from SM service.

Binding service stores the details contained in `ocnf-service-cookie` in `contextInfoCookie` column in `occnp_binding.contextbinding` database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

`OCNF-SERVICE-COOKIE` Processing and N7 Session Lookup

Figure 4-59 OCNF-SERVICE-COOKIE Processing and N7 Session Lookup



When Policy receives an AAR-I request from BSF without the `CustomAVP` or `OCNF-SERVICE-COOKIE`, and if `ENABLE_N7_SESSION_LOOKUP_COOKIE` advanced settings key is enabled at Diameter Gateway, Diameter Gateway queries the Binding service to get the `contextOwner` of the request.

Binding services retrieves the data from `occnp_binding.contextbinding`, add the details in a `ocnf-service-cookie` and sends it to Diameter Gateway in the HTTP response header.

Diameter Gateway processes the `ocnf-service-cookie` received from Binding service, adds it as custom AVP `OCNF-SERVICE-COOKIE` (TLV encoded), and forwards the same to Diameter Connector.

Diameter Connector extracts the details contained in `OCNF-SERVICE-COOKIE`. Diameter Connector adds these details to HTTP header of PA create request and forwards the same to SM service.

If `ENABLE_N7_SESSION_LOOKUP_COOKIE` advanced settings key is enabled at SM service, SM service processes the `ocnf-service-cookie` in header of the received PA Create request. SM service parses the `smPolicyAssociationId` from `cookie-data` and performs primary key lookup.

Copyright © 2019, 2026, Oracle and/or its affiliates.

After processing the request, SM services sends the notification to SMF through Ingress Gateway.

Upgrade Impact

For this feature to work, make sure that both Policy and BSF are upgraded to 25.2.100 or later versions.

Managing Optimizing N7 Session Lookup for AAR messages in Rx Call flows

Enable and Configure

This feature can be enabled using CNC Console and REST API.

To enable this feature, make sure that Binding is enabled.

Enable using CNC Console

To enable the support for optimizing N7 session lookup for AAR-I messages in Rx call flows:

- Configure the value of `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key on **PCF Session Management** page to `true`. For more information, see PCF Session Management.
- Configure the value of `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key on **Settings** page under **Diameter Configurations** to `true`. For more information, see Settings.

Enable using REST API

To enable the support for optimizing N7 session lookup for AAR-I messages in Rx call flows:

- configure the value of `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key in **Session Management Service** API to `true`: `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm`
- configure the value of `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key in **Diameter Settings** API to `true`: `{apiRoot}/oc-cnpolicy-configuration/v1/diameter/settings`

For more information on configuring the feature using REST API, see *Session Management Service* and *Diameter Settings* sections in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics

The `occnp_optimized_smpolicyAssociation_lookup_query_total` metric is used to support optimizing N7 session lookup for AAR-I messages in Rx call flows. For more information, see SM Service Metrics.

The following metrics are used to support optimizing N7 session lookup for AAR-I messages in Rx call flows at Diameter Gateway:

- occnp_ocnf_service_cookie_total
- occnp_context_owner_source_total

For more information, see Diameter Gateway Metrics.

Alerts

The following alerts are used for this feature:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT
- N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT
- N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

For more information, see List of Alerts.

4.20 Conflict Resolution for URSP Rules N1N2 transfer to UE

The feature introduces a conflict resolution module within the Policy Control Function (PCF). This module analyzes conflicting actions of UPSI/URSP rules in UE Policy actions section received from PRE within a single Policy evaluation resulted action. Based on the chosen conflict resolution strategy, the conflict gets resolved accordingly. This ensures that policy actions are consistent, and any discrepancies are addressed during evaluation.

The UE Policy can be evaluated by the PCF during the processing of specific SBI (Service-Based Interface) defined triggers. For more information, see Handling of Multiple N1N2Transfer Messages.

When these triggers occur, the PCF evaluates the necessary policies for a subscriber by sending a policy evaluation request to the Policy Rules Engine (PRE). The evaluation by PRE is performed based on predefined policy rules configured via a Policy Blockly interface. The resulting UE Policy Actions from the PRE may include actions such as install or remove for UPSIs (UE Policy Section Identifier) or URSPs (UE Route Selection Policies). The evaluated policy is then transferred to the UE via the UE Policy Management procedure.

As per the default behavior (where features such as Optimization and Consolidation are not enabled) on PCF UE Service, If both “Install” and “Remove/RemoveAll” actions are specified for a UPSI in the same policy, the PCF defaults to only installing the conflicting UPSI and ignoring the remove action. And, in case of URSP if there is a conflict between “Install” and “Remove”, the conflicting URSP from the existing UPSI is removed and added as part of new UPSI.

When Install Optimization is enabled, it is applied to the policy actions before the N1MessageDelivery container is finalized. If a conflicting UPSI has an Install action that meets the criteria for optimization (already installed), that Install action is eliminated from the decision set. The remaining Remove action is then carried out. The result is that the final delivery for the conflicting UPSI becomes a REMOVE action.

With this feature, the operators are provided with the flexibility to configure how such conflicts are managed. They can choose to **Install**, **Remove**, or **Drop** the conflicting actions to suit their operational needs. In these situations, the PCF determines the appropriate action based on a configurable conflict resolution strategy defined by the policy user. When conflicting actions are identified, the PCF will follow the following strategy:

Table 4-34 Conflict Resolution strategy

Resolution Strategy	Description
INSTALL	Ignore "Remove" action and apply "Install" Action for conflicting UPSIs/URSP Rules.
REMOVE	Ignore "Install" action and apply "Remove" Action for conflicting UPSIs/URSP Rules
DROP	Drop all conflicts, execute none of the conflicting action.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> If no conflict resolution strategy is selected the feature is considered as disabled and the conflicts are handled as per the default behavior on PCF.

The conflict resolution strategy is limited to a single policy evaluation and is not used when resolving conflicts that arise during the consolidation of multiple policy decisions prior to N1Transfer, if policy consolidation is enabled. Conflict resolution takes place immediately following each individual policy evaluation. Policy consolidation, which involves merging several policy decisions, is performed later just before the N1 Message Delivery container is created for transfer.

Possible conflicts that will be resolved:
For UPSIs

- Conflict between **Install UPSI** and **Remove UPSI**
- Conflict between **RemoveAll UPSI** and **INSTALL UPSI**
- Conflict between **RemoveAll UPSI , REMOVE UPSI** and **INSTALL UPSI**

For URSPs

- Conflict between **Install URSP** and **Remove URSP**

> **Note**
>
> The conflict between INSTALL URSP and RemoveALL URSP is not applicable, as RemoveALL is currently supported for UPSIs only.

Further, policy consolidation and optimization are performed before the final delivery of the UE policy if they are enabled. For more information, see Handling of Multiple N1N2Transfer Messages.

Use Case Scenario

- During Create, Install [UPSI-1, UPSI-2] and then N1_Notify successfully received with command `complete`.
- During UE Update or nUDR/nCHF Notify, if Policy Action is "Remove [UPSI-1, UPSI-2] or Install [UPSI-3, UPSI-2]" from PRE.

Case 1: Conflict Resolution Strategy=INSTALL
Action:

Conflicting action identified = Install [UPSI-2] and Remove [UPSI-2].

With Conflict Resolution Strategy as "Install", Policy actions will be finalized to "Remove [UPSI-1] and Install [UPSI-3] and [UPSI-2]".

If install optimization is enabled then, there will be no install action on "UPSI-2" as it has already been installed previously.

So, PCF will finalize the delivery actions as "Remove [UPSI-1] and Install [UPSI-3]", with install optimization enabled.

Case 2: Conflict Resolution Strategy=REMOVE
Action:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Conflicting Action identified = Install [UPSI-2] and Remove [UPSI-2]

With Conflict Resolution Strategy as "Remove", Policy actions will be finalized to "Remove [UPSI-1, UPSI-2] and Install [UPSI-3]". Install Optimization is not applicable for this use case.

So, PCF will finalize the delivery actions as "Remove [UPSI-1, UPSI-2] and Install [UPSI-3]"

Use Case 3: Conflict Resolution Strategy=DROP
Action:

Conflicting Action identified = Install [UPSI-2] and Remove [UPSI-2]

With Conflict Resolution Strategy as "DROP", Policy actions will be finalized to "Remove [UPSI-1] and Install [UPSI-3]". Install Optimization is not applicable for this use case.

So, PCF will finalize the delivery actions as "Remove [UPSI-1] and Install [UPSI-3]"

Managing the Feature

Enable and Configure
You can enable this feature by configuring the `Conflict Resolution Strategy` field in the CNC Console by selecting any one of the configuration (Install, Remove, or Drop) in the drop-down list. For more information, see PCF UE Policy Service.

The following Policy blocks have been added to UE for policy blocks execution:

- *Installed UPSI List*: Allows the policy writer to retrieve and verify the previous successful delivery of UPSI.
- *Installed URSP List*: Allows the policy writer to retrieve and verify the previous successful delivery of URSP.

For more information, see "PCF UE Policy" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.

Observability
The "ue_n1_policy_rule_conflict_total" metric is used for this feature. For more information, see UE Service Metrics.

4.21 Support for Immediate Report Handling for SM-Data, AM-Data, and UE-Policy-Set on N36 Interface

Immediate Report Handling sends urgent notifications directly to the subscribed system as soon as a relevant change is detected. There is no need to wait for next polling cycle or batch update. This ensures the PCF receives up-to-date information in real-time, improving network efficiency and user experience.

Immediate Report Handling monitors changes to specific subscriber data categories (such as SM-Data, AM-Data, and UEPolicyData) on the N36 interface. Once a change occurs, the system immediately generates a notification and pushes it to pre-registered destinations, ensuring that dependent network functions or external systems stay updated with the latest information.

PCF enhances the management of UDR's "Immediate Reporting" feature by minimizing outgoing requests. It achieves this through a single request to UDR, enabling both querying and subscribing to Policy Data (SM-Data, AM-Data, and UE-Policy-Set).

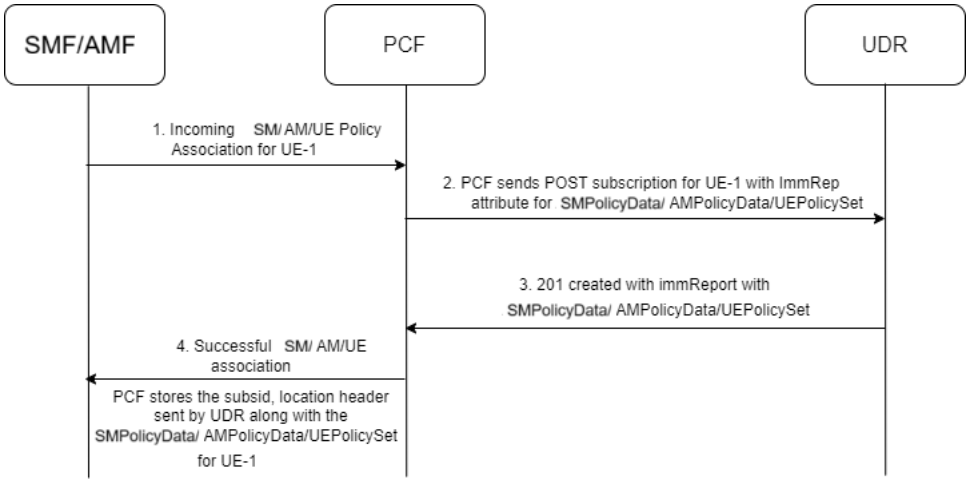
PCF excludes the `ImmediateReportPcc` feature as a supported feature parameter during both on-demand and autonomous discovery of the Unified Data Repository (UDR). When selecting

Copyright © 2019, 2026, Oracle and/or its affiliates.

a UDR, the PCF does not prioritize or rely on the `ImmediateReportPcc` capability, instead adhering to established selection criteria such as priority, load, capacity, and location. If the selected UDR does not include the `ImmediateReportPcc` capability in its registered NFProfile information, the PCF refrains from attempting an immediate report and falls back to the GET and POST method.

> **Note**
>
> The capability check can be disabled through `IMM_REP_CAPABILITY_CHECK` advanced setting configuration. For more information, see PCF User Connector.

Figure 4-60 SM, AM, and UE Policy Association



1. An incoming SM/AM/UE Policy Association for UE-1 is received.
2. The PCF sends a POST subscription for UE-1 with ImmRep attribute for SMPolicyData/ AMPolicyData/UEPolicySet to the UDR.
3. The UDR responds with a 201 created status along with an `immReport` containing SMPolicyData/AMPolicyData/UEPolicySet.
4. The SM/AM/UE association is successfully established and the PCF stores the relevant data.

Preconditions for fallback to UDR GET:

PCF uses the fallback method of issuing a separate GET request for the query of SM-Data, AM-Data, or UE-Policy-Set. It then validates the user by enabling the `Validate User` flag, upon receiving the response to the GET Query. For more information, see PCF Session Management and PCF Access and Mobility and PCF UE Policy Service.

Scenario 1:

1. The UDR POST request did not return subscriber data.
2. Feature negotiation with the UDR failed.
3. The configuration parameter **Enable Data Retrieval Fallback for Immediate Report** is set to **true**.

Scenario 2:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. The advanced setting flag **IMM_REP_CAPABILITY_CHECK** is set to **false**.
2. The UDR POST request did not return subscriber data, regardless of the feature negotiation outcome.
3. The configuration parameter **Enable Data Retrieval Fallback for Immediate Report** is set to **true.**

Managing the Feature

Enable
By default, this feature is disabled. The operator can enable this feature through the CNC Console configurations.

Before enabling the Immediate Report feature at the PCF, ensure that all discoverable UDRs within the mated region support this capability. This feature should not be enabled for Model-D deployments.

In case of fallback scenarios, both UDR POST and GET operations will trigger the registration towards Alternate Route Service

Operators must be aware that enabling Immediate Reporting feature extends the existing `Supported Features` configuration in the User Connector. It is important to understand Immediate Reporting feature capability and the `Supported Features` configuration. By enabling Immediate Reporting feature, UDR Connector combines its capabilities with those already configured in `Supported Features`. For more information on `Supported Features`, see PCF User Connector.

> **Note**
>
> Enabling Bulwark is recommended for this feature to avoid risk of errors or inconsistent data.

After enabling the Immediate Report feature on the PCF, subscription GET messages from the PCF to the UDR will not be seen unless selected UDR Profile does not have Immediate Reporting Capability. This change will impact the outgoing messages from the PCF, as it is a result of the expected optimization in the traffic pattern.

Configuration Using CNC Console
You can configure this feature using the **Enable Immediate Report on Subscription** toggle button. Also, you can enable data retrieval fallback for Immediate Report using the **Enable Data Retrieval Fallback for Immediate Report** toggle button.

These toggle buttons are available in PCF User Connector under Service Configurations on CNC Console for Policy. For information about how to configure for Policy Management Service, see PCF User Connector.

Moreover, advanced setting key **IMM_REP_CAPABILITY_CHECK** can be set to `false` for PCF to ignore the capability check for UDR and send POST with immediate Reporting. By default, the value of **IMM_REP_CAPABILITY_CHECK** key is set to `true`. For more information, see advanced settings of PCF User Connector.

To configure timer for `Subscribe with Immediate Report` POST request, navigate to **Timer Profile** screen, and for PCF User Connector service type, add a new entry under `Timeout for specific message`, with a range of 0-15000 ms and a default of 3000 ms. With the **Immediate Report** feature enabled, the PCF-UDR communication becomes synchronous. PCF waits for UDR's response, containing subscriber data, before policy evaluation and response to SMF/

Copyright © 2019, 2026, Oracle and/or its affiliates.

AMF. This configuration option allows operators to customize UDR timers for synchronous versus asynchronous POST requests.

> **Note**
>
> If not configured, the system defaults to the timer value in the nudr-dr configured field.

For more information, see Timer Profiles.

Configuration Using REST API
The following request/response body parameters have been added in the User Service for this feature:

- ImmRep
- enableImmRepGetFb

For more information, see *User Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability
Metrics

The following metrics are used for this feature:

- occnp_immrep_request_total
- occnp_immrep_response_total
- occnp_immrep_skipped_total

For more information, see User Service Metrics.

Alerts

The following alerts are used for this feature:

- UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR
- UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR
- UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL
- UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
- UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
- UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL
- UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR
- UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR
- UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL
- UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
- UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
- UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL
- UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR
- UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR
- UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Copyright © 2019, 2026, Oracle and/or its affiliates.

- UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
- UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
- UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

For more information, see PCF Alerts.

4.22 Support for Optimized POD Management Using maxSurge and maxUnavailable During Policy Upgrade

Policy supports managing Pods in different deployment strategies. It provides a fine-grained control over how updates are rolled out to applications, ensuring minimal downtime and controlled resource usage during the deployment process.

Policy allows to optimize management of Pods using `maxSurge` and `maxUnavailable` parameters under the `rollingUpdate` and `pdb` categories[1] in `custom-values.yaml` file.

- `maxSurge`: Defines the maximum number of Pods that can be created above the desired number of Pods during an update. It controls how many additional Pods can be scheduled beyond the target replica count to ensure faster rollouts. This parameter is configured only under `rollingUpdate` category in `custom-values.yaml` file. By default, the value of this parameter is set to 25%.

  For example, if a deployment has a replica count of 3 and `maxSurge` is set to 1, the system can temporarily create up to 4 Pods (3 desired + 1 surge) during the update. This allows for quicker rollouts by temporarily exceeding the desired number of Pods, which can be useful when minimizing downtime is critical.
- `maxUnavailable`: Defines the maximum number of Pods that can be unavailable during an update. It ensures that a minimum number of Pods remain available to handle traffic while the update is in progress. This parameter can be set under `rollingUpdate` and `pdb` categories in `custom-values.yaml` file.

  For example, if a deployment has a replica count of 3 and `maxUnavailable` is set to 1, at least 2 Pods will remain available during the update (3 desired - 1 unavailable). This ensures high availability by limiting the number of Pods that can be down at any given time, reducing the risk of service disruption.

Example use cases:

- In case of site isolation based upgrade that are bound by resource constraint, `maxSurge` can be set to 0% and `maxUnavailable` set to 50% to trigger incapacity and quick upgrade.
- In case of `In service upgrade` that are within the restricted resources, `maxSurge` can be set to 0% and `maxUnavailable` can be set to 10% (considering N+K for pods is set to 10%).
- In case of `In service upgrade` that do not have any restricted resources capacity, `maxSurge` can be set to 25% and `maxUnavailable` can be set to 25%.

Sample configuration of `maxSurge` and `maxUnavailable` for Notifier service in `Custom-values.yaml` file:

```
rollingUpdate:
    maxUnavailable: '20%'
```

[1] A rolling update is a deployment strategy where new Pods are gradually rolled out while old Pods are terminated. This approach ensures that the application remains available during the update process, as there is always a sufficient number of Pods running.

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
      maxSurge: '25%'
pdb:
    maxUnavailable: '20%'
```

Note

Currently, Policy supports this feature for all the Policy microservices:

- App Info
- Bulwark service
- Notifier service
- NWDAF agent
- Binding service
- Diameter Connector
- User service
- Config server
- Audit service
- CM service
- LDAP Gateway
- PDS service
- PRE service
- Query service
- AM service
- UE service
- SM service
- PCRF Core
- SOAP Connector
- Perf Info
- Usage Monitoring

Also, Policy supports this feature for 5G Common services: Ingress Gateway, Egress Gateway, and Alternate Route Service, and NRF Client.

Policy does not support this feature for stateful microservices like Diameter Gateway as StatefulSets do not support `maxSurge`. Rolling updates in StatefulSets are done sequentially to preserve Pod identity and storage.

Upgrade and Rollback Impact

The default value of `maxSurge` and `maxUnavailable` parameters are applied to ensure backward compatibility with older `values.yaml` files. This allows upgrade and rollback without requiring any change to existing configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing Support for Optimized POD Management During Policy Upgrade

Management of Pods can be configured using `maxSurge` and `maxUnavailable` parameters under the `rollingUpdate` and `pdb` categories in `custom-values.yaml` file.

For more information, see *Mandatory Configurations* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

4.23 Optimizing PolicyDS Database Query With Configurable UE IDs

When PDS receives a request from any of the microservices, it queries the PolicyDS database to retrieve the details.

PolicyDS database includes:

- `PDSProfile`: Contains PDS Profile information that includes subscriber ID related information such as SUPI and GPSI.
- `PDSSubscriber`: Contains subscriber information.

Policy supports configuring the query on PolicyDS database based on single UE ID, multi UE IDs or based on a specific preference using the subscriber IDs.

Type of search to query and view details from PolicyDS database

Depending on the selected type of search, single UE ID, multi UE IDs, or preferential query, PDS queries data from `PDSProfile` and `PDSSubscriber`.

If the selected type of search is single UE ID, PDS queries all the details from `PDSSubscriber`.

If the selected type of search is multi UE IDs, or preferential query, PDS queries the details from `PDSProfile`.

The details of current and historical type of search configurations on various site is managed in `pdssettings` table.

PDS refers to `pdssettings` table to identify the siteID's and the configuration in each site.

Single UE ID Based Query

PDS query on PolicyDS database using Single UE ID approach allows to query `PDSSubscriber` using a primary key combination.

The primary key can be SUPI, GPSI or a combination of SUPI and GPSI. There must be at least a single SUPI or a GPSI for a given subscriber.

> **Note**
>
> There cannot be multiple SUPIs for one GPSI or multiple GPSIs associated with one SUPI.

The primary key combination for Single UE ID based search can be modified. That is, primary key can be changed from SUPI to GPSI or from GPSI to SUPI.

On selecting the required primary key combination, the requests to PDS is expected to mandatorily contain that ID. Otherwise, the request is rejected with 400 HTTP error code. For

Copyright © 2019, 2026, Oracle and/or its affiliates.

example, when the primary key combination is SUPI, the request to PDS must contain a valid SUPI value. Otherwise, the request is rejected with 400 HTTP error code. For more information on primary key combination, see PDS UE ID Configuration.

> **Note**
>
> This validation is not applicable in case of PDS notification call flows.

Multi UE ID Based Query
Multi UE ID based query is the default type of querying PolicyDS database when the type of search is not selected.

Multi UE ID indicates that there can be multiple SUPIs for one GPSI or multiple GPSIs associated with one SUPI.

> **Note**
>
> Multi UE ID based search query uses OR criteria and the search time taken is higher.

Preferential Query
Preferential query allows to specify a key preference for PDS search query used to look up for a `pdsprofile` record.

Preferential query allows to specify a list of PDS search indexes that can be selected in any order of preference. The search order can be:

- SUPI: `pdsprofile` is queried based on the given SUPI value.
- GPSI: `pdsprofile` is queried based on the given GPSI value.
- SUPI, GPSI: `pdsprofile` is queried first based on the given SUPI value and then based on the given GPSI value.
- GPSI, SUPI: `pdsprofile` is queried first based on the given GPSI value and then based on the given SUPI value.

> **Note**
>
> For notification and audit query the preference order is not considered.

Migration of database records

Policy allows to switch from one type of search to the other type.

For example, the type of search can be switched from Multi UE ID based search or Preferential search to Single UE ID based search.

When the type of search is switched, the database records in `PDSProfile` and `PDSSubscriber` tables are updated accordingly in a lazy manner. For example, if search type is switched from Multi UE ID based search or Preferential search to Single UE ID based search, the records in `PDSSubscriber` are updated with the information present in `PDSProfile` table, provided there is unique SPI/GPSI combination associated to that profile.

Copyright © 2019, 2026, Oracle and/or its affiliates.

CNC Console for Policy displays if the migration of records is in progress. If so, how many records are still to be migrated (that is, total number of non-migrated records). For more information, see PDS UE ID Configuration.

Important

When the type of query is switched from one type of search to another type, the dashboards that are used to identify unique subscriber count will be affected.

Note

Whenever PDS queries PolicyDS database, it stores the results in cache. If a PolicyDS database query is triggered within the cached period, PDS displays the results stored in the cache. PDS does not query the database every time the query is triggered.

Important

While switching from one type of search to the other, (for example, while switching from Multi UE ID based search or Preferential search to Single UE ID based search or vice versa) make sure that the migration of records is complete.

Note

In case of multi-site deployment, Policy supports displaying the migration status at each of the sites.

To disable the migration status for one of the sites, all the sites should be in migration enabled state with the updated configuration. Otherwise, the migration status cannot be disabled.

Migration should be disabled in all the sites almost simultaneously to avoid stale subscriptions being left in PDS.

Migration from Single UE ID to Single UE ID with different primary key combinations should be done in all sites almost simultaneously to avoid stale subscription being left in PDS.

Sample data migration scenario

Note

The switching of the search types and the migration of PDS data is supported only in case of CREATE and audit requests.

Whenever PDS receives a request from any of the PCF microservices such as SM service, AM service, or UE Policy service, PDS queries its PolicyDS database to retrieve the existing data

Copyright © 2019, 2026, Oracle and/or its affiliates.

based on the configured query type such as Multi UE ID or Single UE ID based search. In case, there is any change in the query type, PDS uses the latest query type to search for the data.

Here is a sample scenario when PDS receives a CREATE request for a subscriber for which PDS updates the `pdsprofile` details using a single UE ID query using SUPI.

PDS receives a CREATE request with SUPI= supi1 and GPSI=gpsi1 for the site Site1, and the query type is changed from Multi UE ID based search to Single UE ID based search using SUPI as the primary key. PDS queries the `pdsprofile` database for the given `profileID` having the given SUPI.

If there is no matching record found for the `pdsprofileId` with the given SUPI, PDS updates the SUPI, GPSI, and other profile details for the `profileID` in `pdsprofile` database.

PDS then queries the subscriber details in `pdssubscriber` database using the `pdsprofileID`. If there is a matching record found with the `pdsprofileID`, PDS updates the SUPI, GPSI, and other details of the profile corresponding to the subscriber (`pdsuserID`).

If there is no matching record found for the given `pdsprofileID`, PDS adds the new profile details for the subscriber based on `pdsuserID`.

It is mandatory to manually enable audit to support the migration.

When Audit service is performed on `pdssubscriber` database, it identifies the subscriber details (`pdsuserIDs`) that are deleted in `pdssubscriber` database. The corresponding `profileIDs` are then removed from the `pdsprofile` database.

Similarly, when Audit service is performed on `pdsprofile` database, it identifies the `profileIDs` that are deleted in `pdsprofile` database. The subscriber details in `pdssubscriber` database is then updated to remove the non existent `pdsprofileID`.

Managing Optimization of PolicyDS Database Query With Configurable UE IDs

This section describes how to enable and configure the feature using CNC Console and REST API.

Configure

Multi UE ID based search is the default type, if the type of search is not explicitly configured. The type of searching PolicyDS database can be configured either using CNC Console or using REST API.

Configure using CNC Console

To configure the UE ID based configuration using CNC Console, perform the configurations on **PDS UE ID Configuration** page under **Service Configurations**.

For more information, see PDS UE ID Configuration.

Configure using REST API

To configure the UE ID based configuration using REST API, configure the parameters for `PDS UE ID Configuration Settings` API.

For more information see, *PDS UE ID Configuration Settings* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics

Copyright © 2019, 2026, Oracle and/or its affiliates.

`occnp_db_processing_latency_seconds_count` metric is used to monitor the UE ID based query on PolicyDS database.

For more information, see Policy DS Metrics.

The `ENABLE_PDS_DB_HISTOGRAM_METRICS` advanced settings key for PDS must be enabled to use `occnp_db_processing_latency_seconds_count` metric.

For more information on `ENABLE_PDS_DB_HISTOGRAM_METRICS` key, see PDS Settings.

Installation and Upgrade Impact

Upgrade impact:

- During installation/upgrade, UE ID configuration selected is validated before updating the `pdssettings` table.
- In case of duplicate configuration, a warn log is printed without any update to `pdssettings` database.
- Partition-based approach can be enabled only through the fresh installation
- In case of other invalid configuration (Site1 with Partition enabled and Site2 with Partition disabled and vice versa), a warn log is printed and the configuration updated in `pdssettings` database is the same as previous sites.
- On fresh installation of cnPolicy with Single UE-ID search type, due to implication of migration, replication, and upgrade-rollback, switching back to Multi_UE_ID is not supported.
  In case any issue found, follow these steps:
  1. Move traffic to another cnPolicy set.
  2. Follow the Oracle standard support procedure to debug and fix the issue before moving traffic back to the fresh installed set.

Logging

The following logs from PDS info are used to verify the type of search:

```
{"instant":
{"epochSecond":1744551776,"nanoOfSecond":106606704},"thread":"boundedElastic-6
","level":"DEBUG","loggerName":"ocpm.uds.policyds.util.PdsUserIdGeneratorUtil"
,"message":"PdsUserId generated for SINGLE_UE_ID_PREFERENTIAL_SEARCH with
primaryKeyCombination : SUPI
      is :imsi-450081000000001##0##fe7d992b-0541-4c7d-ab84-
c6d70b1b0123","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jL
ogger","threadId":102,"threadPriority":5,"messageTimestamp":"2025-04-13T13:42:
56.106+0000","ocLogId":"1744551775993_152_policy-occnp-ingress-gateway-
f88679cd9-6j79l"}
```

The PDS logs display the type of search and also how the primary key is generated.

```
{"instant":
{"epochSecond":1744551776,"nanoOfSecond":307685362},"thread":"boundedElastic-1
0","level":"DEBUG","loggerName":"ocpm.uds.policyds.db.helper.PdsSubscriberV2He
lper","message":"Updating mode: 16768 in pdssubcriber for user id:
      imsi-450081000000001##1##fe7d992b-0541-4c7d-ab84-
c6d70b1b0123","endOfBatch":true,"loggerFqcn":"org.apache.logging.slf4j.Log4jLo
gger","threadId":140,"threadPriority":5,"messageTimestamp":"2025-04-13T13:42:5
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
6.307+0000","ocLogId":"1744551775993_152_policy-occnp-ingress-gateway-
f88679cd9-6j79l"}
```

Checkpoints

- Migration of records is not required when the type of search is switched between Multi UE ID search and Preferential search, as both these type of searches query `pdsprofile` and `pdssubscriber` tables.
- While switching to Single UE ID search, `siteId` can have a maximum of 80 characters when both SUPI and GPSI are used.
- The prerequisite for switching to Single UE ID search is that there should be multiple UE ID configurations. That is, one SUPI cannot have multiple GPSIs or one GPSI cannot have multiple SUPIs.
- All the sites should be upgraded to new release before modifying the **PDS Settings** configurations.
- In case of multi-site deployment, in order to disable the migration at one site, all the sites should be in migration enabled state with the updated configuration. Otherwise, migration at the specified site cannot be disabled.
  The following are the key points to remember while disabling the migration in any of the sites in a multi-site deployment:
  - Migration can be disabled at any of the sites, only if all the sites are using the same type of query. Migration can not be disabled at any one site if any of the sites are using a different query type.

    For example, in a three site deployment, if Single SUPI query is used in Site1 and Site3, while Multi UE ID query is used in Site2, migration can not be disabled in Site1 or Site3.
  - Query type can be changed at a site only if all the sites are using the same query type.

    For example, if Site1 and Site3 are using Single SUPI query and Site2 is using Multi UE ID query, type of query at Site1 or Site3 cannot be changed from Single SUPI query to Single SUPI/GPSI until the type of query at Site2 is also changed to Single SUPI. When all the three sites are using Single SUPI query, query type can be changed to Single SUPI/GPSI or any other query type.
  - Migration from one query type to another is not allowed at one site when one of the other sites is using a different query type.

    For example, if Site1 is migrated from Single SUPI to Single SUPI/GPSI while Site2 and Site3 are still using Single SUPI, Site2 or Site3 cannot be migrated from Single SUPI to Multi UE ID type.

    Since Site1 is already migrated to Single SUPI/GPSI, Site2 and Site3 must also be migrated to Single SUPI/GPSI completely before attempting to migrate Site2 or Site3 to Multi UE ID type.
  - Migration at one site cannot be disabled, if the query type at that site is migrated to a different one while the other sites are yet to be migrated.

    For example, if Site1 is migrated from Single SUPI/GPSI to Multi UE ID while Site2 and Site3 are yet to be migrated from Single SUPI/GPSI to Multi UE ID, migration cannot be disabled at Site1.

    Migration at Site1 can not be disabled only after Site2 and Site3 are also migrated from Single SUPI/GPSI to Multi UE ID type.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- When a new site is added, by default the query type at that site will be in Multi UE ID mode. Suppose, the other sites are using a different query type, the new site should also be migrated to that query type.

  For example, while Site1 and Site2 are using Single SUPI query type, if a new site Site3 is added, the default query type at Site3 is Multi UE ID, which must be migrated to Single SUPI type as in Site1 and Site2.
- Migration should be disabled in all the sites almost simultaneously to avoid stale subscriptions being left in PDS.
- Migration from one Single UE ID search to another Single UE ID search with different primary key combination should be done in the all the sites almost simultaneously to avoid stale subscription being left in PDS.
- The value of **SiteID** field on **PDS UE ID Configuration** page in CNC Console should match with the actual siteIDs.
- When migration is disabled, any non migrated records can not be gracefully deleted if `pdsprofile` is deleted.
- A record can be deleted, if the configured primary key combination (UE ID) is not present in the record.
- Records in `Pdsprofile` are deleted once the migration is turned off in the subsequent audit notification for the `pdsprofile` table.
- Audit notification on `Pdsprofile` can not handle migration of the corresponding subscribers. Only the audit notification on `pdssubscriber` can handle the migration.
- Partition-based approach can be enabled only through the fresh installation.
- Configuration at all the sites must be the same. That is, if site1 is installed with a Multi UE ID configuration, then Site 2 should also be installed with a Multi UE ID configuration. Any other configuration apart from this will not be considered.
- If the configured primary key combination is not passed in the create request, the request is rejected with a `400 BAD request`.
- If the UE ID passed in the UDR or CHF notification is the same as the primary key combination configured, the lookup can happen with the primary key combination only.
- The following are the key points to remember while migrating records from different combination of the query types:
  - **Migration from Multi UE ID to Preferential search**:

    If a migration from Multi UE ID based query to Preferential based query is attempted, if the preference order and the requested subscriber IDs are the same, there can be an improvement in the turn around of the search result.

    Migration of records depends on the preference order. Migration is applicable only if the query uses specific subscription based on preference order.

    For example, if the preference order is SUPI, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 is treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are for the same subscriber.
  - **Migration from Preferential search to Multi UE ID search**:

    If an attempt is made to migrate the type of query from Preferential based query to Multi UE ID based query, migration of records are not applicable if the records are migrated from `pdsprofile` database with query using a preference order to new query on `pdsprofile` database using SUPI or GPSI.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Any combination of SUPI and GPSI if shared between subscribers are considered as one subscriber.

- **Migration from Single primary key search to Multi UE ID search**:

  While migrating from Single primary key to Multi UE ID based query, if the migration is enabled, records are migrated from one single primary key based query on `pdssubscriber` to a new query on `pdssubscriber`.

  In single primary key, the primary key uniquely identifies the subscriber. For example, SUPI.

  Suppose, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 is treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are same subscribers.

  If the migration is not enabled, there is no migration of records.

  Any combination of SUPI and GPSI, if shared between subscribers is considered as one subscriber.

- **Migration from Single primary key search to Preferential search**:

  In case of a migration from Single primary key based query to Preferential query, if the migration is enabled, migration of records depends on the preference order. Records are migrated from single primary key based search on `pdssubscriber` database to another primary key based search on `pdssubscriber` database.

  If the preference order is SUPI, the query must include at least one valid SUPI value.

  If the preference order is GPSI, the query must include at least one valid GPSI value.

  If the preference order is SUPI, GPSI, records are searched first based on the given SUPI value and then based on the given GPSI value. The query must include at least a valid SUPI or a valid GPSI value.

  If the preference order is GPSI, SUPI, records are searched first based on the given GPSI value and then based on the given SUPI value. The query must include at least a valid GPSI or a valid SUPI value.

  In single primary key, the primary key uniquely identifies the subscriber. For example, single SUPI.

  For example, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 is treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are same subscribers.

  If the migration is disabled, there is no migration of records.

  For example, if the preference order is SUPI, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 is treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are same subscribers.

- **Migration from Multi UE ID search to Single primary key search**:

  While switching from Multi UE ID based query to Single primary key search like Single SUPI or Single GPSI or a combination of SUPI and GPSI as primary key, if the migration is enabled, records are migrated from SUPI or GPSI based query on `pdsprofile` database to a new query using SUPI or GPSI on `pdsprofile` database.

  Any combination of SUPI and GPSI, if shared between subscribers is considered as one subscriber.

  If the migration is not enabled, there is no migration of records.

  SUPI or GPSI, or every combination of SUPI and GPSI is treated as a separate subscriber.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For example if the migration is to a Single SUPI query, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 are treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are same subscribers.

If the migration is to a combination of SUPI and GPSI as primary key, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 is treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are also different subscribers.

- **Migration from Preferential search to Single primary key search**:

  While switching from Preferential search to Single primary key search such as Single SUPI or Single GPSI, or a combination of SUPI and GPSI as primary key, if the migration is enabled, records are migrated from SUPI or a GPSI or a combination of SUPI, GPSI based query on `pdsprofile` database to a new query using SUPI or GPSI on `pdsprofile` database.

  Any combination of SUPI and GPSI if shared between subscribers is considered as one subscriber.

  If the migration is not enabled, there is no migration of records.

  SUPI or GPSI, or every combination of SUPI and GPSI is treated as a separate subscriber.

  For example if the migration is to a Single SUPI query, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 are treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are same subscribers.

  If the migration is to a combination of SUPI and GPSI as primary key, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 is treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are also different subscribers.

- **Migration from one Single primary key search to another Single primary key search**:

  During migration from one Single primary key search to another Single primary key search such as from Single SUPI or a Single GPSI based search to a combination of Single SUPI and GPSI based search, if migration is enabled, records are migrated from a query using one primary key on `pdssubscriber` database to a query based on another primary key on `pdssubscriber` database.

  SUPI uniquely identifies the subscriber.

  SUPI or GPSI, or every combination of SUPI and GPSI is treated as a separate subscriber.

  For example if the migration is to a Single SUPI query, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 are treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are same subscribers.

  If the migration is to a combination of SUPI and GPSI as primary key, S1:SUPI1-GPSI1 and S2:SUPI2-GPSI1 is treated as different subscribers. While S1:SUPI1-GPSI1 and S2:SUPI1-GPSI2 are also different subscribers.

4.24 Support for Monitoring Migration Status of Database Records

Policy supports assessing the status of DB records in Policy for various microservices.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Currently, Policy supports assessing the status of only the PolicyDS database records.

Migration status for following type of search can be viewed:

- Multi UE ID: Allows to use multiple search criteria based on a primary key combination using AND (Preferential) and OR (default).
- Single UE ID: Allows to use a specific criteria based on a primary key combination to query the database.
- Partition based: Allows to use search criteria based on a composite key formed with a combination of keys. All the keys can be present in a single table or in different data tables. Partition based search is applicable only in case of fresh installation.

  `enablePdsPartitionBasedSchema` Helm parameter must be configured to enable Partition based schema for PDS.

  When `PdsPartitionBasedSchema` parameter is enabled, the primary key combination for partition based search must be configured using `primaryKeyCombination` Helm parameter.

  For more details on `enablePdsPartitionBasedSchema` and `primaryKeyCombination` Helm parameters, see *Enabling/Disabling Services Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

For more details on the different type of search supported by Policy, see Optimizing PolicyDS Database Query With Configurable UE IDs.

The primary keys used for the query can be SUPI, GPSI, or a combination of SUPI and GPSI.

In case of Single UE ID search types, the primary key includes source type and siteIDs along with the selected SUPI or GPSI or a combination of SUPI and GPSI.

In case of partition based search type, a composite key is formed with subscriber IDs (SUPI, GPSI, or a combination of SUPI and GPSI), source type, and siteIDs stored in separate columns or data tables.

The following table depicts the possible primary key combination for each search type.

Table 4-35 Possible primary key combination for each search type

Search Type	Primary Key Combination
Multi UE ID	UUID
Single UE ID	SUPI##GPSI##source_type##siteid
Single UE ID	SUPI##source_type##siteid
Single UE ID	GPSI##source_type##siteid
Partition based Single-UE Id	SUPI##GPSI
Partition based Single-UE Id	SUPI
Partition based Single-UE Id	GPSI

Policy allows to switch the type of search. For example, it is possible to switch the type of search from Multi UE ID to Single UE ID type.

When the type of search is switched from one type to the other, tables within the database are updated to be in sync.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For example, when the type of search is switched from Multi UE ID to Single UE ID type, records are migrated from the tables used by Multi UE ID type to the tables used by Single UE ID type.

While the data migration is in progress, the database can be queried to get the count of database records that are pending to be migrated.

For example, while switching from Multi UE ID based query to Single UE ID based query, the database can be queried to get the count of records pertaining to the microservice or a subscriber that are yet to be migrated from one type of search to the other.

In case of multisite deployment, the query results such as count of records can be queried for specific sites.

The database migration status can be queried or viewed through CNC Console. For more information, see Custom Query.

Managing Custom Query

Configure

The **Custom Query** page under **Status and Query** in CNC Console can be used to query the database migration status.

For more information, see Custom Query.

4.25 Support for Signaling and DB Access Processing Latency Histogram Metrics

In order to provide sufficient insight into the microservices performance for incoming requests, Policy includes histogram metrics for the microservices.

These Histogram metrics enable Policy to observe data distribution by measuring the latency of multiple HTTP and database requests sent and received by the microservices.

Histogram Metrics for Binding Service

Enable

Histogram metrics for Binding service can be enabled either using Helm configuration or using CNC Console.

To enable histogram metrics for Binding service using CNC console, configure the `ENABLE_BINDING_HTTP_HISTOGRAM_METRICS` advanced settings key on **Binding Service Configuration** page under **Service Configurations** in CNC Console.

For more information about the advance settings keys, see Binding Service.

To enable histogram metrics for Binding service using Helm configuration, configure the value of `SIGNALING_DB_HISTOGRAM_METRIC_ENABLED` parameter to `true`.

For more information on Helm configuration, see *Binding Service Configurations* section in *Oracle Communications Cloud Native Core, Installation, Upgrade, and Fault Recovery Guide.*

Metrics

The following metrics are used to monitor the database processing latency in Binding service call flows, HTTP incoming and outgoing connections:

- occnp_db_processing_latency_seconds

Copyright © 2019, 2026, Oracle and/or its affiliates.

- occnp_http_in_conn_processing_latency_seconds

For more information, see Binding Service Metrics.

Histogram Metrics for PDS Service

The following metrics are used to monitor the database processing latency in PDS service call flows, HTTP incoming and outgoing connections:

- occnp_db_processing_latency_seconds
- occnp_http_in_conn_processing_latency_seconds

For more information, see Policy DS Metrics.

Histogram Metrics for PCRF Core Service

The following metrics are used to monitor the latency in PCRF Core service call flows, Diameter Gateway response time for the incoming requests, HTTP incoming and outgoing connections, and DB request processing:

- occnp_diam_response_local_processing_latency_seconds
- occnp_http_in_conn_processing_latency_seconds
- occnp_db_processing_latency_ms

For more information, see PCRF Core Metrics.

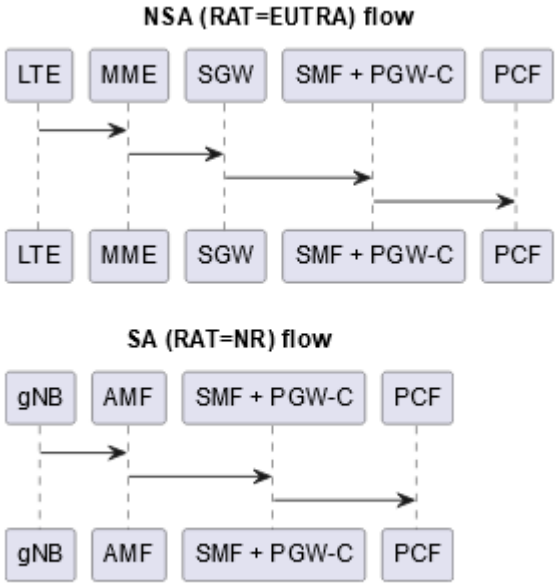
4.26 Support for NR vs EUTRA KPIs for N7 Interface

The 5G deployment can be broadly categorized into Non-Standalone (NSA) and Standalone (SA) architectures. The NSA deployments combines a 5G Radio Access Network (RAN) operating alongside a legacy 4G LTE core network. The SA deployments feature a 5G RAN and a cloud native 5G core. The 5G network operators may deploy their networks using both the NSA and SA deployment strategies.

The following diagram illustrates the NSA and SA subscriber flow:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-61 NSA and SA Flow



The NSA subscribers follows:

`Long Term Evolution (LTE) network → Mobile Management Entity (MME)→ Serving Gateway (SGW) → Session Management Function (SMF) → Policy Control Function (PCF)` with Radio Access Technology (RAT) value set to EUTRA. The Evolved Universal Terrestrial Radio Access (EUTRA) is the air interface technology used in 4G LTE networks.

The SA subscribers follows:

`Session Management Function (SMF) → PDN Gateway → Control Plane(PGW-C) → Policy Control Function (PCF)` with RAT value set to NR. New Radio (NR) is the air interface technology used in 5G networks.

Currently, the KPIs in PCF application do not differentiate between NSA and SA call flow. This feature provides KPI for N7 interface to differentiate between the NR and EUTRA radio access technology in the SM Service. The SM service will provide KPI to visualize in Grafana dashboard, and allows to measure the `SMPolicyCreate`, `SMPolicyUpdate` and `SMPolicyDelete` transactions per second (TPS) along with RAT type (NR or EUTRA).

> **Note**
>
> The error responses from Ingress Gateway microservice does not support the newly added dimensions.

The following existing metrics in SM service are modified to capture the radio access type (ratType) and access type (accessType) dimensions.

- `ocpm_ingress_request_total`
- `ocpm_ingress_response_total`
- `http_in_conn_request_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- `http_in_conn_response_total`

The following new metrics are added for SM update and delete requests.

- `http_in_conn_ext_request_total`
- `http_in_conn_ext_response_total`

The following new dimensions are added to above metrics to support NR vs EUTRA rat type over N7 interface:

Table 4-36 SM Dimensions

Dimension Name	Values	Description
accessType access_type	• 3GPP_ACCESS • NON_3GPP_ACCESS	Supported access types.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-36 (Cont.) SM Dimensions

Dimension Name	Values	Description
policyControlRequestTrigger	• AC_TY_CH • AN_CH_COR • AN_INFO • APP_STA • APP_STO • CM_SES_FAIL • DEF_QOS_CH • NO_CREDIT • NUM_OF_PACKET_FILTER • PLM_CH • PRA_CH • PS_DA_OFF • QOS_NOTIF • RAT_TY_CH • RE_TIM	Policy Control Request Trigger can have single value or comma separated list of values ordered alphabetically. The metrics using this dimension is not pegged if this field is not populated with either of the following mandatory values: • AC_TY_CH, • PRA_CH, • RAT_TY_CH. They can come individually, together, or along other values. When a list of values is received, at least one of the previous values must be present; otherwise, the metric is not pegged. If the received number of values for this dimension is greater than 5, the mandatory values are prioritized first among the received values. The remaining values are ordered alphabetically and combine them with the previously retrieved mandatory ones until we run out of remaining values, or we will reach the maximum number of values allowed (5), whichever occurs first. If more values do exist after this process, they are ignored. For example: **Table 4-37 `policyControlRequestTrigger` Dimension Scenario** For delete request this dimension can be empty; otherwise the rules in Table `policyControlRequestTrigger` Dimension Scenario is applied. For requests where value is not validated, sanitization is done, and invalid values are removed and ignored.

Table 4-37 `policyControlRequestTrigger` Dimension Scenario

Incoming Values	Output Dimension	Peg Values
`AN_CH_COR,RES_MO_RE,QOS_NOTIF`	""	The values are not pegged, since the mandatory values are not found.
`PRA_CH`	"PRA_CH"	The value is pegged, since one of the mandatory values exist.
`RAT_TY_CH,PRA_CH`	"PRA_CH,RAT_TY_CH"	The value is pegged, since one of the mandatory value exist.
`RAT_TY_CH,AC_TY_CH,QOS_NOTIF`	"AC_TY_CH,RAT_TY_CH,QOS_NOTIF"	The value is pegged, since one of the mandatory value exist.
`APP_STA,PRA_CH,RES_MO_RE,AC_TY_CH,QOS_NOTIF,UE_IP_CH,RAT_TY_CH`	"AC_TY_CH,APP_STA,PRA_CH,QOS_NOTIF,RAT_TY_CH"	The value is pegged, since the mandatory values exist, and the remaining values were ignored.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-36 (Cont.) SM Dimensions

Dimension Name	Values	Description
	EOUT • REF_QOS_IND_CH • RES_MO_RE • RES_RELEASE • SAREA_CH • SCELL_CH • SCNN_CH • SE_AMBR_CH • SUCC_RES_ALLO • UE_IP_CH • UE_MAC_CH • UE_STATUS_RESUME • UE_TZ_CH • US_RE	

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-36 (Cont.) SM Dimensions

Dimension Name	Values	Description
rat_type ratType	• EUTRA • EUTRA_U • GERA • LTE-M • NBIOT • NR • NR_GEO • NR_LEO • NR_MEO • NR_OTHER_SAT • NR_REDCAP • NR_U • TRUSTED_N3GA • TRUSTED_WLAN • UTRA • VIRTUAL • WIRELINE • WIRELI	Supported Radio Access Type (RAT).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-36 SM Dimensions

Dimension Name	Values	Description
	• NE_BBF • WIRELINE_CABLE • WLAN	
sourceAccessType	Single value	The previous access type before the update. The value can be empty if cannot be retrieved from a session. Dimension: accessType
sourceRatType	Single value	The previous radio access type before the update. The value can be empty if cannot be retrieved from a session. Dimension: ratType

A sample metric:

occnp_http_in_conn_ext_request_total{accessType="NON_3GPP_ACCESS",application="pcf_smservice",operationType="update",policyControlRequestTrigger="AC_TY_CH,NO_CREDIT,RAT_TY_CH,PRA_CH,UE_IP_CH",ratType="NR",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA"} 1.0

For more detailed information about the metrics, see SM Service Metrics section.

For more information about the dimensions `accessType`, `ratType`, and `policyControlRequestTrigger` details, see CNC Policy Metrics section.

4.27 Support of Traffic Detection on SMF-N7 and TDF using Sd Interface

> **Important**
>
> **Custom support for traffic detection on SMF-N7 and TDF using the Sd interface** is an experimental feature. It is subject to change and is not supported for production use (lab use only).

The PCF is responsible for defining and managing policies. It can be used for parental control by defining and enforcing policies related to network traffic and access based on user profiles. PCF monitors network traffic to detect and manage access to specific content or services based on pre-defined rules. Application Detection and Control (ADC) rules are used to enforce these policies, such as restricting access to certain websites or applications for specific users.

The CnPolicy provides ADC rules to the Traffic Detection Function (TDF) by using the Sd interface. The Sd interface enables to communicate with the TDF. CnPolicy uses a TDF to

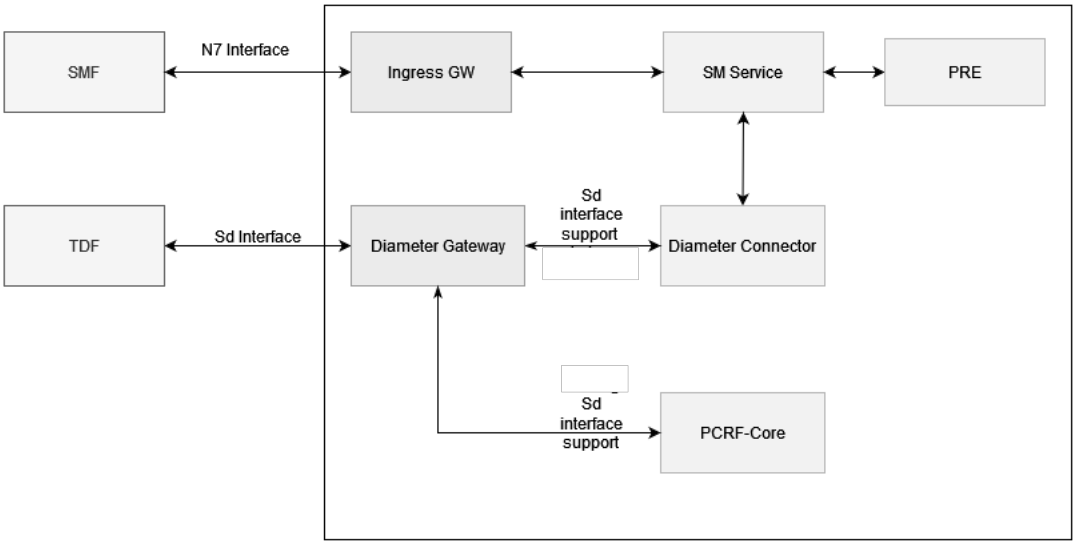
Copyright © 2019, 2026, Oracle and/or its affiliates.

detect and identify specific types of network. This allows it to understand which application or service is generating the traffic. Based on the detected traffic type, the CnPolicy applies predefined policies or rules to manage the traffic flow. In solicited reporting, CnPolicy instructs TDF to report traffic events, including application starting or stopping based on the appropriate ADC rules.

The support for Sd interface already exists between PCRF Core and Diameter Gateway, for a PCRF deployment. For more details about it, see Support for Sd Interface in PCRF section.

By implementing this feature in CnPolicy on SMF-N7 interface, it enables CnPolicy to determine the traffic detection on Sd interface for both the PCF and Converged Policy (PCF + PCRF) modes of deployment. The following diagram illustrates the architecture involved for PCF to support for Sd interface. This feature introduces Sd interface support between Diameter Connector and Diameter Gateway on SMF-N7 interface.

Figure 4-62 Sd interface in PCF



CnPolicy performs the following functionality to SMF-N7 to determine the traffic detection on Sd interface for both PCF and Converged Policy modes of Deployment:

- TDF session establishment between CnPolicy and TDF when the session request is initiated by PCF only. For changes made to this procedure, refer to **Sd Session Establishment from PCF to TDF** callflow.
- Update of TDF session, refer to **Sd Session Modification from PCF to TDF when PLMN Change** and **Sd Session Modification from PCF to TDF when Update Notification from OCS-Sy SNR** call flows.
- TDF session termination requests is initiated by PCF, refer to **Sd Session Termination Initiated by CnPolicy** callflow.
- TDF session termination requests is initiated by TDF, refer to **Sd Session Termination Initiated by TDF** callflow.
- Provisioning of ADC rules from CnPolicy for traffic detection and enforcement at the TDF.

Call Flows

This section describes the different SM service call flows that are modified to support TDF session in CnPolicy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

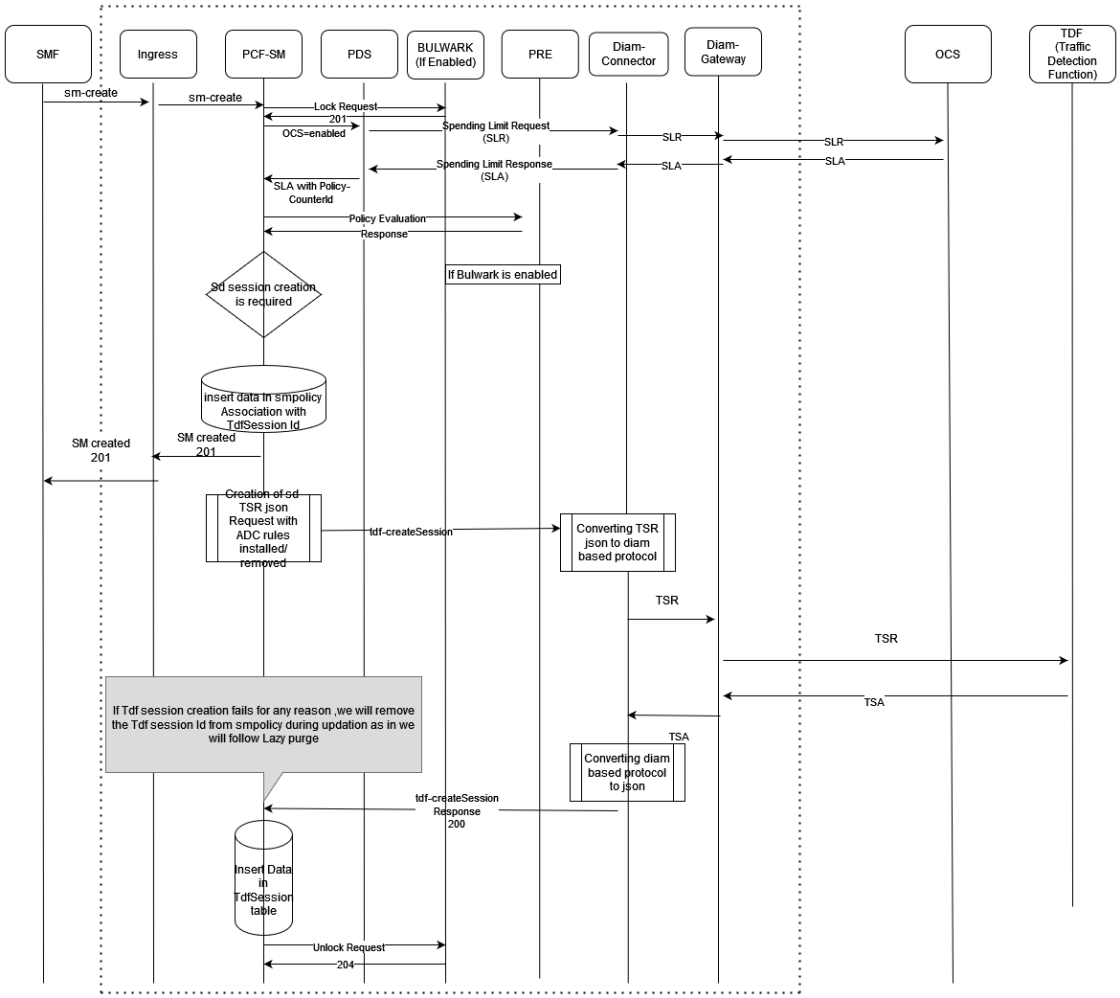
Sd Session Establishment from PCF to TDF

CnPolicy establishes a Sd session, based on a policy condition/action during SM-Create request received over N7 interface. The condition to establish a Sd session is based on data Packet Data Unit (PDU) session establishment on N7 create. CnPolicy supports asynchronous mode of communication between SMF-N7 and Sd interface.

> **Note**
>
> CnPolicy supports one Sd session per PDU session from SMF-N7. In case of multiple PDU sessions, the new Sd session is established to the same TDF for which the IPCAN session already exists.

The following procedure describes how CnPolicy initiates an Sd session from PCF-SM towards the TDF by sending a ADC Rule, using a TDF-Session-Request (TSR) message to the TDF and getting a successful TDF-Session-Answer (TSA) message to PCF-SM:

Figure 4-63 Sd Session Establishment (PCF→ TDF)



1. SMF sends a SM-Create request to PCF-SM.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. If the OCS is enabled, then Spending Limit Request (SLR) is sent by the Diameter Connector to OCS.
3. A Spending Limit Answer (SLA) is sent by OCS to Diameter Connector.
4. PCF-SM on receiving the Policy counter in SLA, initiates a policy evaluation request to PRE.
5. PCF-SM checks for any Sd session creation requirement in the PRE response.
6. If the Sd session needs to be created, a Tdf session id is created and added to the smPolicy association.
7. The smPolicy association along with Tdf session id is stored in the database.
8. PCF-SM does not wait for TDF response to come, response sent to SMF is irrespective of TDF response.
9. PCF-SM creates a Sd TDF-Session-Request (TSR) JSON text with Application Detection and Control (ADC) rules, and then initiates a tdf-creation request with the TSR JSON text toward Diameter Connector.
10. The Diameter Connector converts the TSR JSON to diameter based protocol, and sends a TSR request toward Traffic Detection Function (TDF).
11. The TDF responds with TDF-Session-Answer (TSA) to Diameter Gateway, and Diameter Connector converts this TSA to JSON text.
12. Diameter Connector responds to PCF-SM with HTTP 200 OK, and TSA JSON text. At PCF-SM the text is stored in the TDFSession table in the database.
13. If Tdf session creation fails then the TDF session id is removed from the smPolicy association during the database lazy purge.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

When PCF receives SM Context Create request from SMF with `anGwIpv4Addr` or `anGwIpv6Addr` populated, PCF forwards the `AN-GW-Address` AVP to the TDF in the TSR.

When PCF receives SM Context Update or SM Context Delete from SMF, the `AN-GW-Address` AVP is not included in the RAR (Re-Authorization Request) sent to the TDF.

If the `anGwAddr` is provided with an empty or invalid value in the SM Context Create request, PCF rejects the request and returns an `HTTP 400 (BAD_REQUEST)` response with the cause `OPTIONAL_IE_INCORRECT`. For more details on the error response, see Appendix HTTP Error Codes.

```
{
  "gpsi": "msisdn-131000000023",
  "supi": "imsi-450081000000023",
  "pduSessionId": 1,
  "pduSessionType": "IPV6",
  "dnn": "dnn1",
  "notificationUri": "http://nf1stub.ocats.svc:8080/smf/notify",
  "accessType": "3GPP_ACCESS",
  "ratType": "NR",
  "ipv6AddressPrefix": "2800:a00:cc01:c058:0:0:0:0/64",
  "subsSessAmbr": {
    "uplink": "1 Mbps",
    "downlink": "10 Mbps"
  },
  "subsDefQos": {
    "5qi": 9,
    "arp": {
      "priorityLevel": 2,
      "preemptCap": "NOT_PREEMPT",
      "preemptVuln": "PREEMPTABLE"
    },
    "priorityLevel": 1
  },
  "sliceInfo": {
    "sst": 11,
    "sd": "abc123"
  },
  "servNfId": {
    "anGwAddr": {
      "anGwIpv4Addr": "192.168.203.50",
      "anGwIpv6Addr": "2001:db8:85a3::370:7334"
    }
  }
}
```

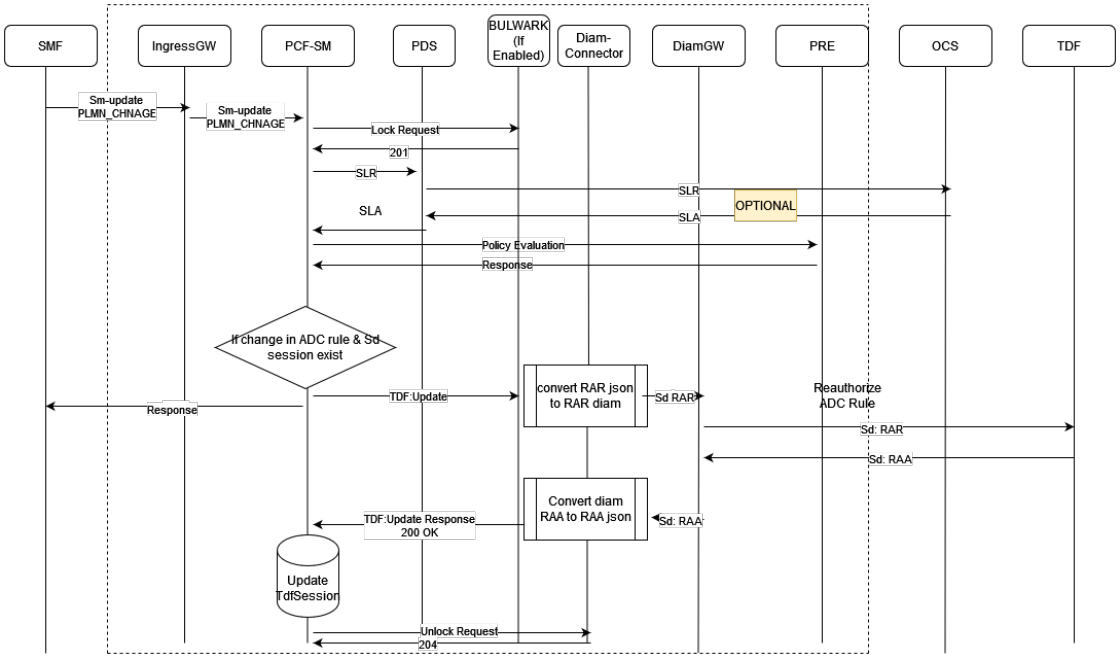
Sd Session Modification from PCF to TDF

Sd Session Modification from PCF to TDF when PLMN Change

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following procedure describes how CnPolicy on receiving PLMN change from SMF, triggers an SM update request. This request may result in policy re-evaluation with changes to ADC rules. Reauthorizing these ADC rule at TDF and storing the updated TDF session into database.

Figure 4-64 Sd Session Modification from PCF to TDF when PLMN Change



1. The SMF initiates a SM update request toward PCF on change in the Public Land Mobile Network (PLMN).
2. The PCF-SM service in PCF on receiving the SLA response from OCS, initiates a policy evaluation towards PDS.
3. After receiving the response from PDS, PCF-SM checks if there is any ADC rule changes and if the Sd session exists.
   - If the condition is true, then PCF-SM sends a TDF update request towards a TDF through Diameter Connector.
   - Diameter Connector sends a Sd RAR request towards Diameter Gateway.
   - Diameter Gateway forwards this Sd RAR request to the TDF. The ADC rules are reauthorized at TDF.
   - TDF responds with Sd RAA towards Diameter Gateway.
   - Diameter Gateway forwards this to Diameter Connector.
   - Diameter Connector converts the Sd RAA response object to JSON format, and sends this to PCF-SM.
   - PCF-SM stores the updated Tdfsession into the database.

The following Advanced Settings keys on PDS Settings page in CNC Console are used to specify the UE_ID while sending notification from PDS to Policy microservices, SM service, AM service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-38 Advanced Settings to configure UE IDs

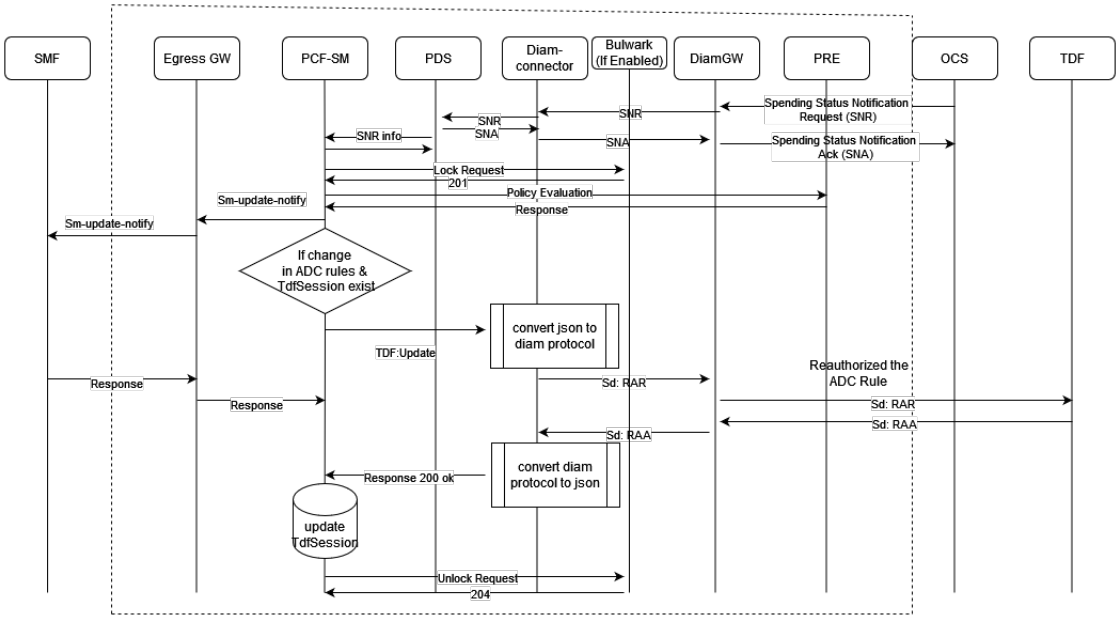
Key	Description
OCS_NOTIFICATION_UE_ID_PREFERENCE	Used to configure UE ID in OCS notification sent by PDS to Policy microservices. Possible values: • SUPI • GPSI **default value**: SUPI (Which will make it backward compatible)
CHF_NOTIFICATION_UE_ID_PREFERENCE	Used to configure UE ID in CHF notification sent by PDS to Policy microservices. Possible values: • SUPI • GPSI **default value**: SUPI (Which will make it backward compatible)

Sd Session Modification on Update Notification from OCS-Sy SNR:

The following procedure describes how CnPolicy on receiving Spending Notification Request (SNR) from OCS, can trigger a Sd session modification if Sd session exists. CnPolicy initiates a Sd rule modification resulting in reauthorized ADC rules at TDF and storing the updated TDF session into the database.

> **Note**
>
> TDF Session will only be created during SM-create..

Figure 4-65 Sd Session Modification on Update Notification from OCS-Sy SNR



Copyright © 2019, 2026, Oracle and/or its affiliates.

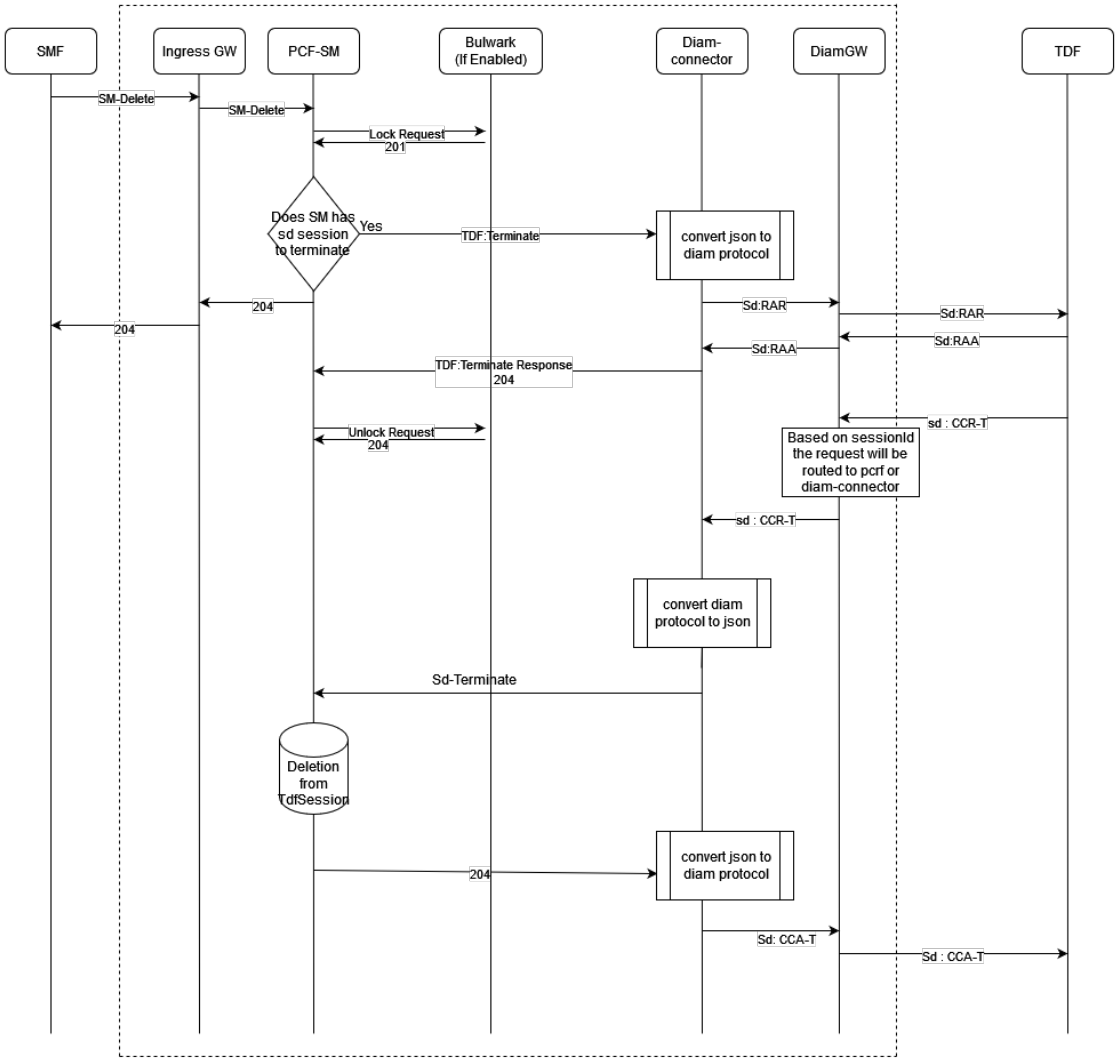
1. On OCS initiating a SNR request toward PCF, the PCF-SM initiates a policy evaluation request toward PDS.
2. In case of policy changes from PDS, PCF-SM triggers the SM update notify request toward SMF. PCF-SM also checks if there is any ADC rule changes and if the Sd session exists.
   - If the condition is true, then PCF-SM sends a TDF update request towards a TDF through Diameter Connector.
   - Diameter Connector sends a Sd RAR request towards Diameter Gateway.
   - Diameter Gateway forwards this Sd RAR request to the TDF. The ADC rules are reauthorized at TDF.
   - TDF responds with Sd RAA towards Diameter Gateway.
   - Diameter Gateway forwards this to Diameter Connector.
   - Diameter Connector converts the Sd RAA response object to JSON format, and sends this to PCF-SM.
   - PCF-SM stores the updated Tdfsession into the database.

Sd Session Termination Initiated by CnPolicy

The following procedure describes how CnPolicy on receiving SM delete from SMF, triggers an Sd session termination by sending the Sd RAR having `Session-Release-Cause` attribute set to `IP_CAN_SESSION_TERMINATION` towards TDF. CnPolicy sends delete response to SMF over N7 interface. It also supports receiving and processing of Sd CCR-T response have `CC-Request-Type` attribute set to `TERMINATION_REQUEST`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-66 Sd Session Termination (PCF → TDF)



1. SMF sends a SM-Delete request to PCF-SM.
2. PCF-SM checks if SM session has Sd session to terminate, if exists then it sends a TDF terminate request to Diameter Connector.
3. Diameter Connector converts the json to diameter protocol and sends Sd RAR towards Diameter Gateway.
4. Diameter Gateway on receiving the Sd RAA successful response, it is forwarded to Diameter Connector.
   - Diameter Connector responds with TDF terminate to PCF-SM, and PCF-SM also responds with terminate success to SMF.
   - TDF sends a Sd: CCR-T request to Diameter Gateway. Diameter Gateway based on the session id the request will be routed to either PCRF Core or Diameter Connector service.
   - If Diameter Connector receives an Sd: CCR-T request from Diameter Gateway, it converts the diameter protocol request to JSON, and sends it to PCF-SM.

Copyright © 2019, 2026, Oracle and/or its affiliates.

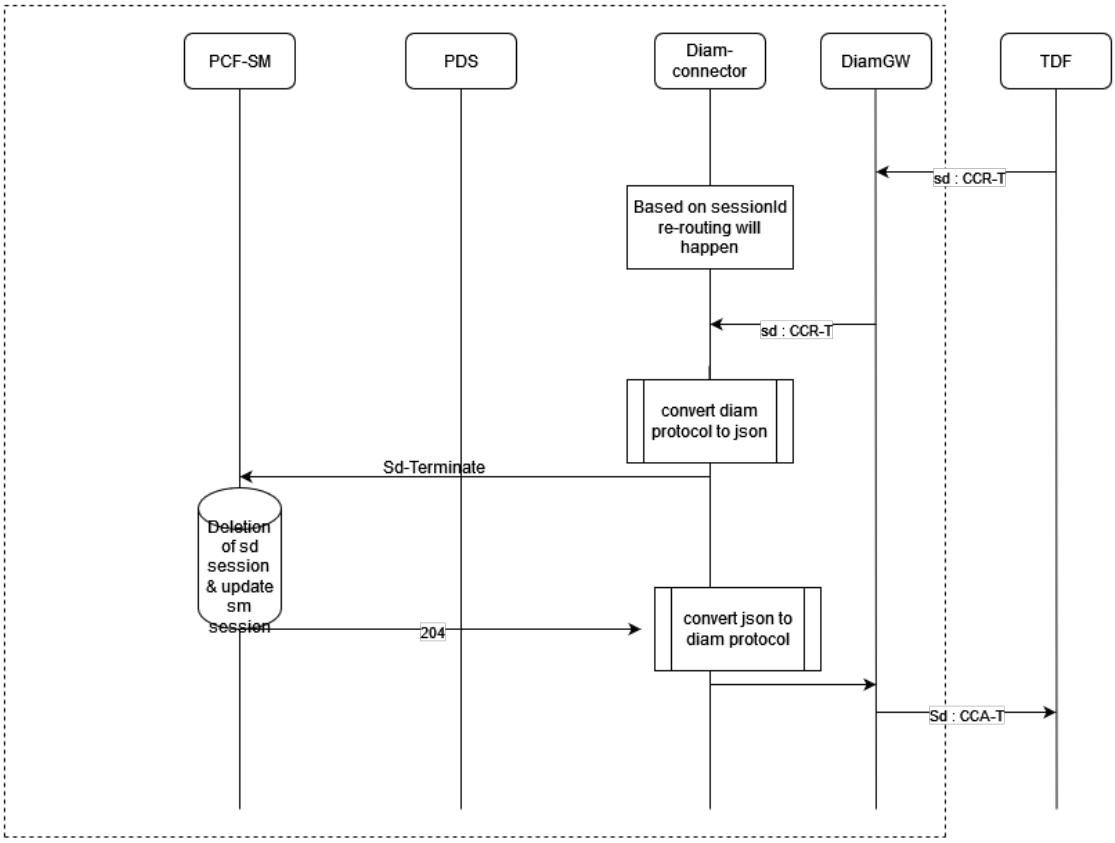
- PCF-SM deletes the associated Tdfsession in the database and send a request to Diameter Connector.
- Diameter Connector converts JSON data to diameter protocol, and sends a Sd: CCA-T request to Diameter Gateway.
- Diameter Gateway forwards the Sd: CCA-T to TDF.

5. Diameter Gateway on receiving the Sd RAA failure response, the Sd session is deleted and PCF does not wait for CCR-T from TDF.

Sd Session Termination Initiated by TDF

The following procedure describes how CnPolicy on receiving Sd session termination initiated by TDF by sending an Sd: CCR-T, shall clean up Sd session information and does not send any Update Notify request to SMF.

Figure 4-67 Sd Session Termination (TDF → PCF)



1. TDF initiates a Sd: CCR-T request toward Diameter Gateway.
2. Diameter Gateway sends this request to Diameter Connector.
3. Diameter Connector based on the session id, the request will be re-routed.

Diameter Gateway Routing Decision for CCR-U or CCR-T from TDF

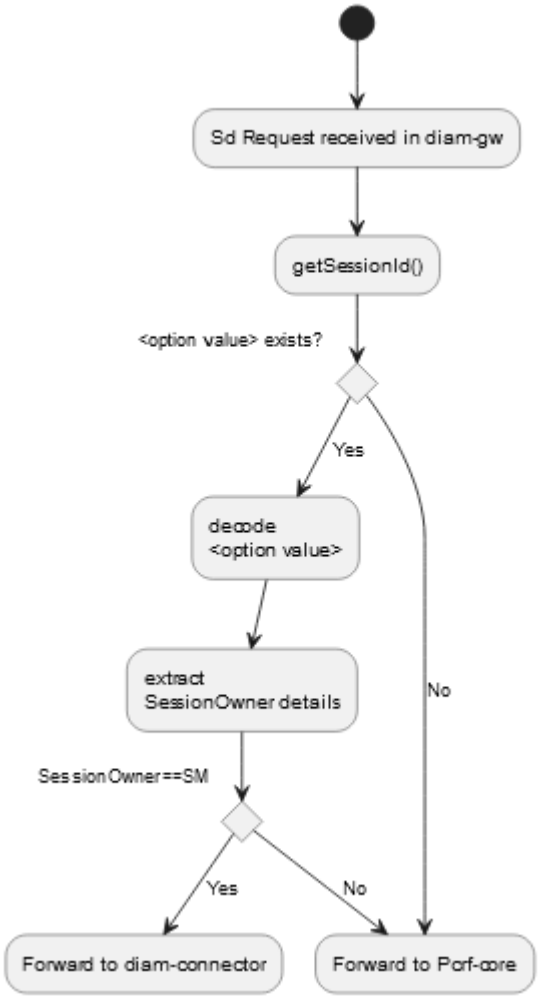
The Diameter Gateway on receiving the CCR-U or CCR-T request from TDF has to decide if the request has to be routed to PCRF Core or Diameter Connector. It uses the `<optional value>` of diameter session-id AVP, which is used to identify a specific session. An encoded

Copyright © 2019, 2026, Oracle and/or its affiliates.

<optional value> is appended with session-id and added to the Diameter Gateway header to differentiate between PCRF Core and PCF so that it can re-route the requests accordingly.

The diagram illustrates the flowchart for the Diameter Gateway making the routing decision based on <option value>.

Figure 4-68 Flowchart for Diameter Gateway Routing Decision



Diameter Gateway service uses RFC-6733 recommendation for the Session-id AVP format <DiameterIdentity>;<high 32 bits>;<low 32 bits>[;<optional value>].

Where,

- <high 32 bits> and <low 32 bits> are decimal representations of the high and low 32 bits of a monotonically increasing 64-bit value. The 64-bit value is rendered in two part to simplify formatting by 32-bit processors. At startup, the high 32 bits of the 64-bit value may be initialized to the time in NTP format RFC5905, and the low 32 bits may be initialized to zero. This will for practical purposes eliminate the possibility of overlapping Session-Ids after a reboot, assuming the reboot process takes longer than a second. Alternatively, an implementation may keep track of the increasing value in non-volatile memory.
- <optional value> is implementation specific.

A sample session-id AVP format:

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
sd1.oracle.com;5dd8b4b775-
fvwlg;1728285868;efac51ae-3d26-4632-9d3b-7ee3a5bbd207_101NTAyU00=
```

Where,

Table 4-39 Session-id AVP Format

Diameter Identity	High 32 bits	Low 32 bits	<option value>
sd1.oracle.com	5dd8b4b775-fvwlg	1728285868	efac51ae-3d26-4632-9d3b-7ee3a5bbd207_101NTAyU00=

Table 4-40 <option value> Format

AssociationID	Encoding_version_number	Number of Elements	Encoded_Key_Value_Pair
This is a random UUID generated number. Example: efac51ae-3d26-4632-9d3b-7ee3a5bbd207	This determines the encryption or decryption algorithm used for the particular ID to get the key-value pair information. Example: 1	This determines how many key-value pairs exists in the encoded format in **encoded_key_value_pair** Example: 01	This contains the key-value pair in a specific format used to decode the data. The `NTAyU00=`, decoded value is `502SM`.

Table 4-41 Decoded_Key_Value_Pair as TagID-Length-Value (TLV) format

AssociationIdTLV	length_of_AssociationIdTLV	Value
This is the enum for tag IDs. Example: In decoded `502SM` text, '5' represents the session or context owner.	This represents the length of the value string. Example: In decoded `502SM` text, '02' represents the value length.	This holds the value. Example: In decoded `502SM` text, 'SM' represents the value. **Note**: Currently only SM value is supported.

Diameter Gateway Force Routing for Sd Interface

In Policy converged mode deployment, both the HTTP and Diameter requests are handled by CnPolicy. In this mode of deployment if the Diameter Gateway is unable to identify the right session for the Sd CCR-T or CCR-U requests then the CnPolicy uses force routing mechanism. By default, this mechanism is disabled. It can be enabled by adding the following advanced setting keys to Diameter Gateway service configurations in CNC Console.

Following are the Diameter Gateway advanced settings keys and their default values for configuring force routing for Sd interface:

Table 4-42 Parameters for Advanced Settings

Key	Value
DIAMETER.gateway.sd.session.owner.failure.forcerouting.enabled	This is used to enable force routing to PCRF Core and/or Diameter Connector for Sd interface. Allowed values are true or false. **Default Value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-42 (Cont.) Parameters for Advanced Settings

Key	Value
DIAMETER.gateway.sd.session.owner.failure.forcerouting.service.list	This is used to set the force routing to PCRF Core and/or Diameter Connector. Default value is the string: • PCRF_CORE • DIAMETER_CONNECTOR
DIAMETER.gateway.sd.session.owner.failure.forcerouting.retry.timeout	This is used to enable force routing retry on the next service if the current selected service is throwing timeout error. Allowed values are true or false. **Default Value**: true
DIAMETER.gateway.sd.session.owner.failure.forcerouting.retry.diameter.unknown.session.id	This is used to enable force routing retry on the next service if the current selected service is throwing `DIAMETER_UNKNOWN_SESSION_ID`. Allowed values are true or false. **Default Value**: true
DIAMETER.gateway.sd.session.owner.failure.forcerouting.retry.error.code.list	Provide the list of diameter error code for which users want to retry force routing. If the diameter error code coming from the current selected service is present in this list then force routing is retried on the next service. Allowed value is a string, and default is empty string. Example: 3004, 5012 **Default Value:** ""

> **Note**
>
> If the TDF sends a empty or null, or encodes `SESSION_OWNER` as `UNKNOWN` in `session-id`, then the Diameter Gateway cannot find the session owner. The chances of these conditions are extremely less. Force routing is a precautionary mechanism to handle such extreme edge cases.

For more information about the advanced settings in Diameter Gateway service, see Settings section.

Changes in Congestion Control feature

SM Service Congestion Control

When SM service is in congestion state then based on request priority and discard priority messages are either accepted or rejected. The request priority is decided based on the priority order: `oc-message-priority` header → `3gpp-sbi-message-priority` header → `advanced settings priority` → `default priority`.

Following advanced keys are used to configure the message priorities for TDF messages at SM service:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-43 SM Advanced Settings

Key	Value
SM.TDF.SESSION.DELETE.PRIORITY	16
SM.TDF.SESSION.UPDATE.PRIORITY	18

For more details about the Congestion Control support in SM Service, refer to SM Service Pod Congestion Control.

Diameter Connector Congestion Control

When Diameter Connector service is in congestion state then based on request priority and discard priority messages are either accepted or rejected. The request priority is decided based on the priority order: `oc-message-priority header/OC-Message-Priority AVP` → `advanced settings priority` → `default priority`.

Following advanced keys are used to configure the message priorities for TDF and Sd messages at Diameter Connector service:

Table 4-44 Diameter Connector Advanced keys

Key	Value
SM.TDF.CREATE.SESSION.REQUEST.PRIORITY	24
SM.TDF.TERMINATE.REQUEST.PRIORITY	16
SM.TDF.UPDATE.REQUEST.PRIORITY	18
SD.CCR.TERMINATE.REQUEST.PRIORITY	16
SD.CCR.UPDATE.REQUEST.PRIORITY	18

For more details about the Congestion Control support in Diameter Connector, refer to Diameter Connector Pod Congestion Control.

Diameter Gateway Congestion Control

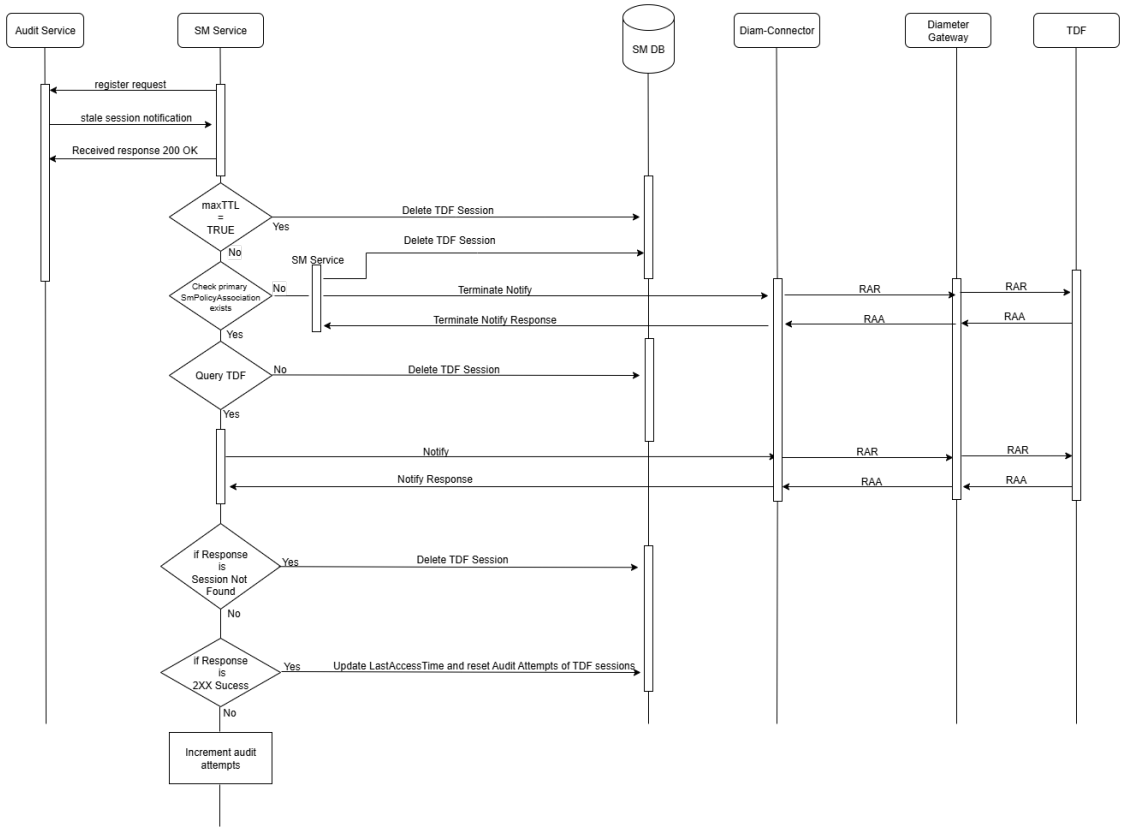
For more details about the Congestion Control support in Diameter Gateway, refer to Diameter Pod Congestion Control.

TDF Stale Session Cleanup in Database using Audit Service

Audit service supports auditing the TDF Session table periodically and remove the stale sessions. Based on the session's`sLastAccessTime` information the Audit service determines if the session is stale or not. If it is a stale session then it sends notification to SM service for cleaning the stale session.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-69 TDF Stale Session Cleanup



1. If Audit service is enabled for SM service, Audit service sends stale session notification towards SM Service.
2. In the stale session notification, if `maxTTL` is `true`, SM service deletes the stale TDF session from the its database.
3. In the stale session notification, if `maxTTL` is `false`:
   a. SM Service checks if primary `SMPolicyAssociation` exists or not.
   b. If primary SMPolicyAssocation does not exist:
      SM Service sends Sd-RAR with **Session-Release-Cause= IP_CAN_SESSION_TERMINATION**.
   c. If primary `SMPolicyAssociation` exists:
      i. If **queryTDF** field is `true`:
         i. SM service sends Notify request (RAR) towards TDF to check if `tdfSession` is still active or not.
         ii. If Notify response is `Session Not Found`, then SM service deletes the `tdfSession` from the SM service database.
         iii. If Notify response is `Success`, then SM service updates the `LastAccessTime` and the Audit attempts in the database.
         iv. If Notify response is any other error (except `Session Not Found`), then SM service increments audit attempts in the database.
      ii. If **queryTDF** field is **false**, then SM service deletes `tdfSession`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> UpdateNotify/TerminateNotify is sent to TDF only if `TDF.TDF_ENABLED` advanced settings key for SM service is set to `true`.

For more details about editing the audit information related to **TDF Session** in CNC Console, refer to PCF Session Management page.

Late Arrival and Stale Session Processing

Late arrival and stale session processing features are integrated with SM service and Diameter Connector for n7-sd interface.

For details on late arrival and stale requests cleanup in Policy, see Support for Stale Requests Cleanup.

CNC Console Configurations

The N7-Sd feature in PCF is not enabled by default. This can be enabled by adding the `TDF.TDF_ENABLED` advanced setting key on PCF Session Management page in CNC Console.

In SM service, the data stored in the SmAssociation table in the database can be compressed. This can also be applied to TdfSession table too. To enable the data compression in SM service, enable the `System.Data Compression Scheme` field in PCF Session Management service.

For more information to enable this feature and also the data compression in SM service, see PCF Session Management page in CNC Console.

The traffic profile containing the ADC rules can be created using the Traffic Profile page in the CNC Console. The ADC rules can also be configures using the Rest APIs. For more information, see "PCF Traffic Profile ADC Rule", "PCF Predefined ADC Rule", and "PCF Predefined ADC Rule Base" sections in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

HTTP and Diameter Result Codes Mapping

In CnPolicy converged deployment, both the HTTP and Diameter requests are handled by the application. The errors in Diameter Connector are handled by the result code AVP in Diameter messages, which are mapped to appropriate HTTP response code.

Diameter Gateway maps Diameter error codes to HTTP status codes. This table provides the mapping of Diameter result code to HTTP response code when the Diameter Connector sends response to SM service.

Table 4-45 Diameter Result Codes from TDF toward SM service

Diameter Result Code	HTTP Response Code	Diameter Connector Response Body
DIAMETER_SUCCESS	200	No response body

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-45 (Cont.) Diameter Result Codes from TDF toward SM service

Diameter Result Code	HTTP Response Code	Diameter Connector Response Body
DIAMETER_MISSING_AVP / DIAMETER_UNABLE_TO_COMPLY / DIAMETER_UNABLE_TO_DELIVER / DIAMETER_TOO_BUSY / DIAMETER_LOOP_DETECTED/ DIAMETER_APPLICATION_UNSUPPORTED	500	{ "type": null, "title": "INTERNAL_SERVER_ERROR", "status": 500, "detail": "Error Occurred", "instance": null, "cause": "<Mapping of Diameter Result Code with Cause is provided in below table>", "invalidParams": null }
DIAMETER_UNKNOWN_SESSION_ID	404	{ "type": null, "title": "NOT_FOUND", "status": 404, "detail": "Session Does not Exist", "instance": null, "cause": "A request is received with unknown session ID.", "invalidParams": null }

This table describes the Diameter Connector various error 'cause' that it can send in its response body to SM service.

Table 4-46 Error Cause Diameter Connector to SM service

Diameter Error Name	Diameter Result Code	Response Body 'Cause' from Diameter Connector to SM
DIAMETER_UNABLE_TO_COMPLY	5012	An internal failure occurred.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-46 (Cont.) Error Cause Diameter Connector to SM service

Diameter Error Name	Diameter Result Code	Response Body 'Cause' from Diameter Connector to SM
DIAMETER_UNKNOWN_SESSION_ID	5002	A request is received with unknown session ID.
DIAMETER_UNABLE_TO_DELIVER	3002	Request did not delivered to the destination.
DIAMETER_TOO_BUSY	3004	An upstream peer is either in congestion or too busy to handle a request.
DIAMETER_MISSING_AVP	5005	The request did not contain an AVP that is required by the Command Code definition.
DIAMETER_COMMAND_UNSUPPORTED	3001	The Request contained a Command-Code that the receiver did not recognize or support.
DIAMETER_LOOP_DETECTED	3005	An agent detected a loop while trying to get the message to the intended recipient.
DIAMETER_UNSUPPORTED_VERSION	5011	A request was received, whose version number is unsupported.
DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	5009	A message was received that included an AVP that appeared more often than permitted in the message definition.
DIAMETER_AVP_UNSUPPORTED	5001	The peer received a message that contained an AVP that is not recognized or supported and was marked with the Mandatory bit.
DIAMETER_INVALID_AVP_VALUE	5004	The request contained an AVP with an invalid value in its data portion.
DIAMETER_INVALID_AVP_LENGTH	5014	The request contained an AVP with an invalid length.
DIAMETER_INVALID_HDR_BITS	3008	A request was received whose bits in the Diameter header were either set to an invalid combination, or to a value that is inconsistent with the command code definition.
DIAMETER_INVALID_AVP_BITS	3009	A request was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the AVP definition.

When Diameter Connector times out while processing a request, then it will send and `503 Service Unavailable` response.

```
{
    "type": null,
    "title": "SERVICE_UNAVAILABLE",
    "status": 503,
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    "detail": "Service Unavailable",
    "instance": null,
    "cause": "Request processing timeout.",
    "invalidParams": null
}
```

Delay response by TDF: Diameter-gateway will send DIAMETER_UNABLE_TO_DELIVER to diameter-connector and diameter-connector will send 500 Internal Server Error to SM with response body.

```
{
    "type": null,
    "title": "INTERNAL_SERVER_ERROR",
    "status": 500,
    "detail": "Error Occurred",
    "instance": null,
    "cause": "Request did not delivered to the destination.",
    "invalidParams": null
}
```

Destination-Realm (Host-Realm) is null/empty in Sd TSR/RAR request from SM towards TDF: Diameter-gateway will response back with DIAMAETER_MISSING_AVP to diameter-connector. Diameter-connector will send 500 Internal Server Error to SM with response body.

```
{
    "type": null,
    "title": "INTERNAL_SERVER_ERROR",
    "status": 500,
    "detail": "Error Occurred",
    "instance": null,
    "cause": "The request did not contain an AVP that is required by the
Command Code definition.",
    "invalidParams": null
}
```

Destination-Identity (Host-Identity) is null/empty in Sd TSR/RAR request from SM towards TDF: Diameter-gateway will response back with DIAMETER_UNABLE_TO_DELIVER to diameter-connector. Diameter-connector will send 500 Internal Server Error to SM with response body.

```
{
    "type": null,
    "title": "INTERNAL_SERVER_ERROR",
    "status": 500,
    "detail": "Error Occurred",
    "instance": null,
    "cause": "Request did not delivered to the destination.",
    "invalidParams": null
}
```

Sd CCR-T/CCR-U response from SM towards TDF

Copyright © 2019, 2026, Oracle and/or its affiliates.

HTTP status codes are used to indicate the success or failure of an HTTP request, and can be mapped to Diameter errors. This table provides the mapping of HTTP response code to Diameter result code when SM service sends response to Diameter Connector.

Table 4-47 HTTP Result Codes from SM service toward TDF

HTTP Response Code	Diameter Result Code
204/200	DIAMETER_SUCCESS
500	DIAMETER_UNABLE_TO_COMPLY
503	DIAMETER_UNABLE_TO_COMPLY
400	DIAMETER_UNABLE_TO_COMPLY
404	DIAMETER_UNKNOWN_SESSION_ID

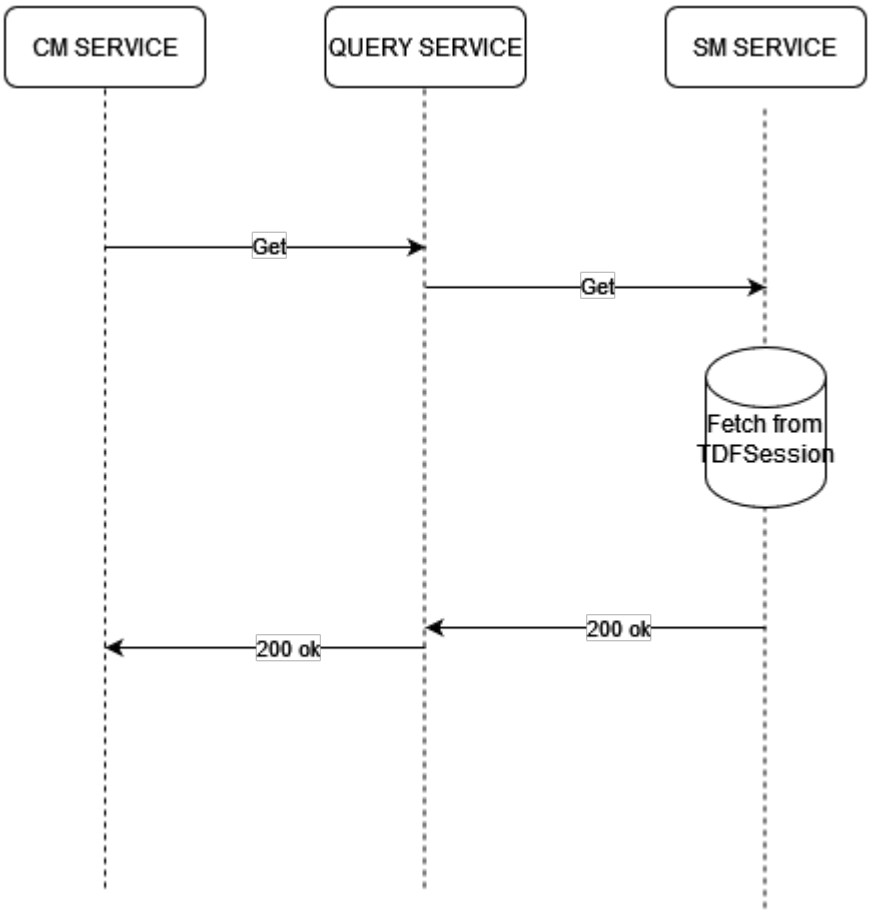
Support for TDF Session in Session Viewer

The session viewer supports `SM TDF session` in Session Viewer page of CNC Console.

TDF Session Viewer Call Flows

This section describes the different call flows for TDF session in Session view.

Figure 4-70 Fetch TDF Session



Copyright © 2019, 2026, Oracle and/or its affiliates.

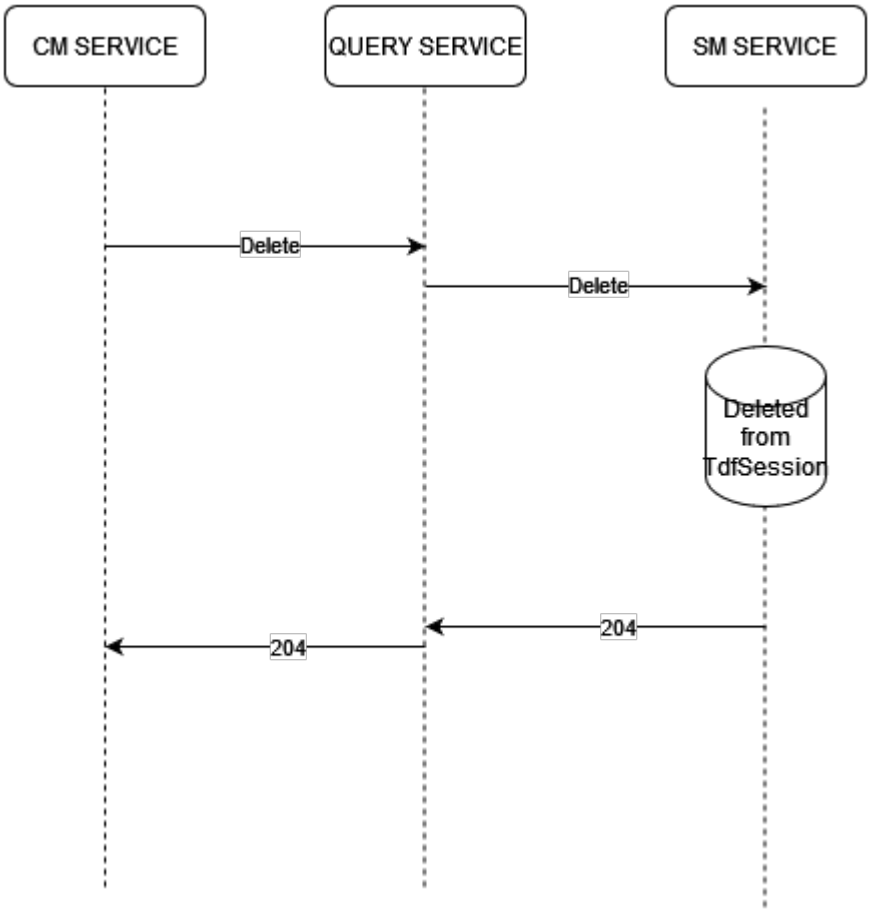
TDF Session can be fetched based on:

- SUPI
- GPSI
- IPV4
- IPv6
- TDF_SESSION_ID
- DIAMETER_SESSION_ID

TDF_SESSION_ID can be obtained using the given DIAMETER_SESSION_ID. TDF session can be fetched based on TDF_SESSION_ID.

Delete TDF Session

Figure 4-71 LOCAL DELETE TDF SESSION



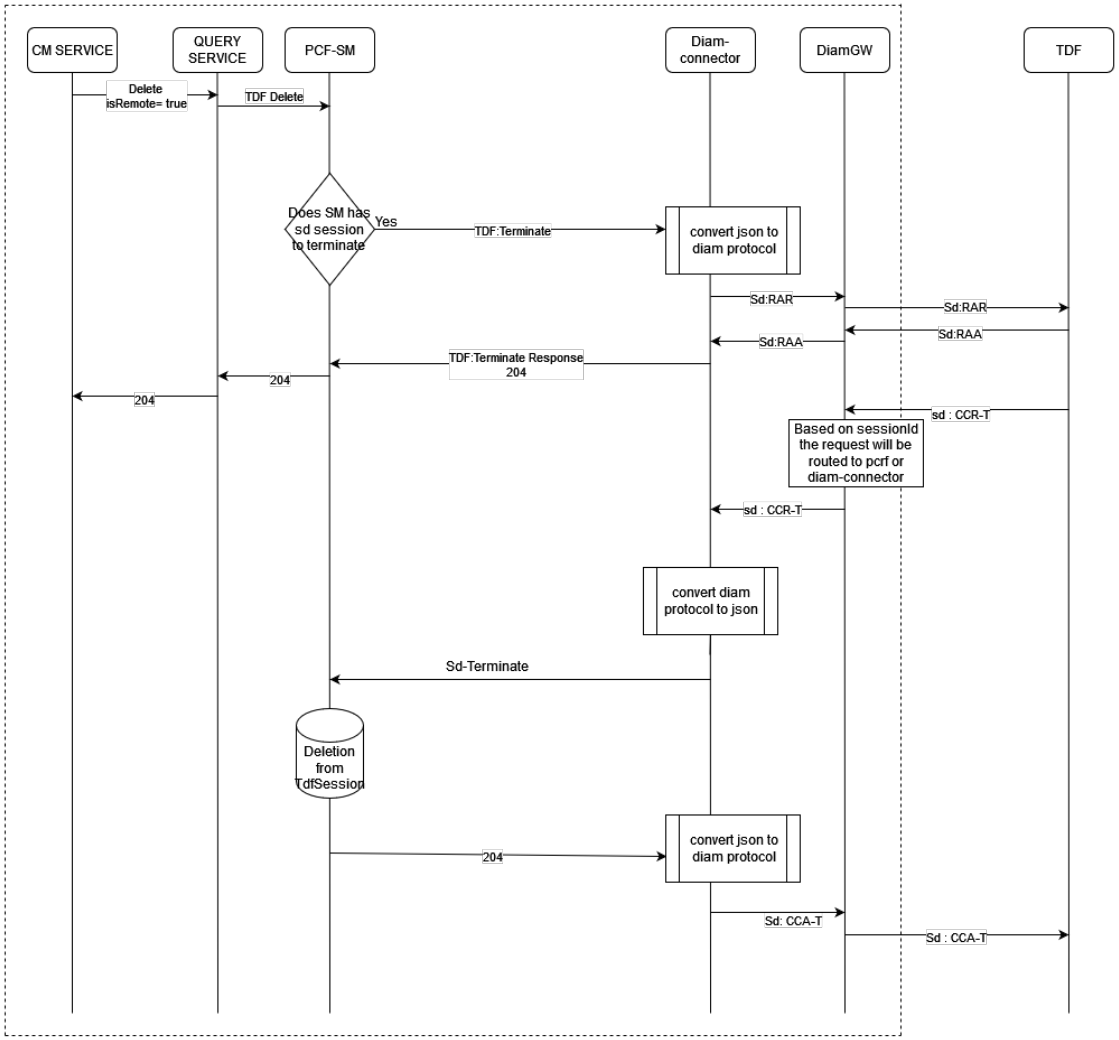
Query TDF SESSION ID from the **Session Viewer** under **Status and Query** on CNC Console. Click **Delete** to delete the individual session by checking **Initiate Remote Session Cleanup**.

1. CM Service sends ResoureDeleteRequest to Query Service.
2. Query Service sends ResoureDeleteRequest to SM service through TDFApi.
3. SM service deletes TDF session from `TDFSession` table in its database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

REMOTE DELETE TDF SESSION

Figure 4-72 REMOTE DELETE TDF SESSION



Query TDF SESSION ID from the **Session Viewer** under **Status and Query** on CNC Console. Click **Delete** to delete the individual session by checking **Initiate Remote Session Cleanup**.

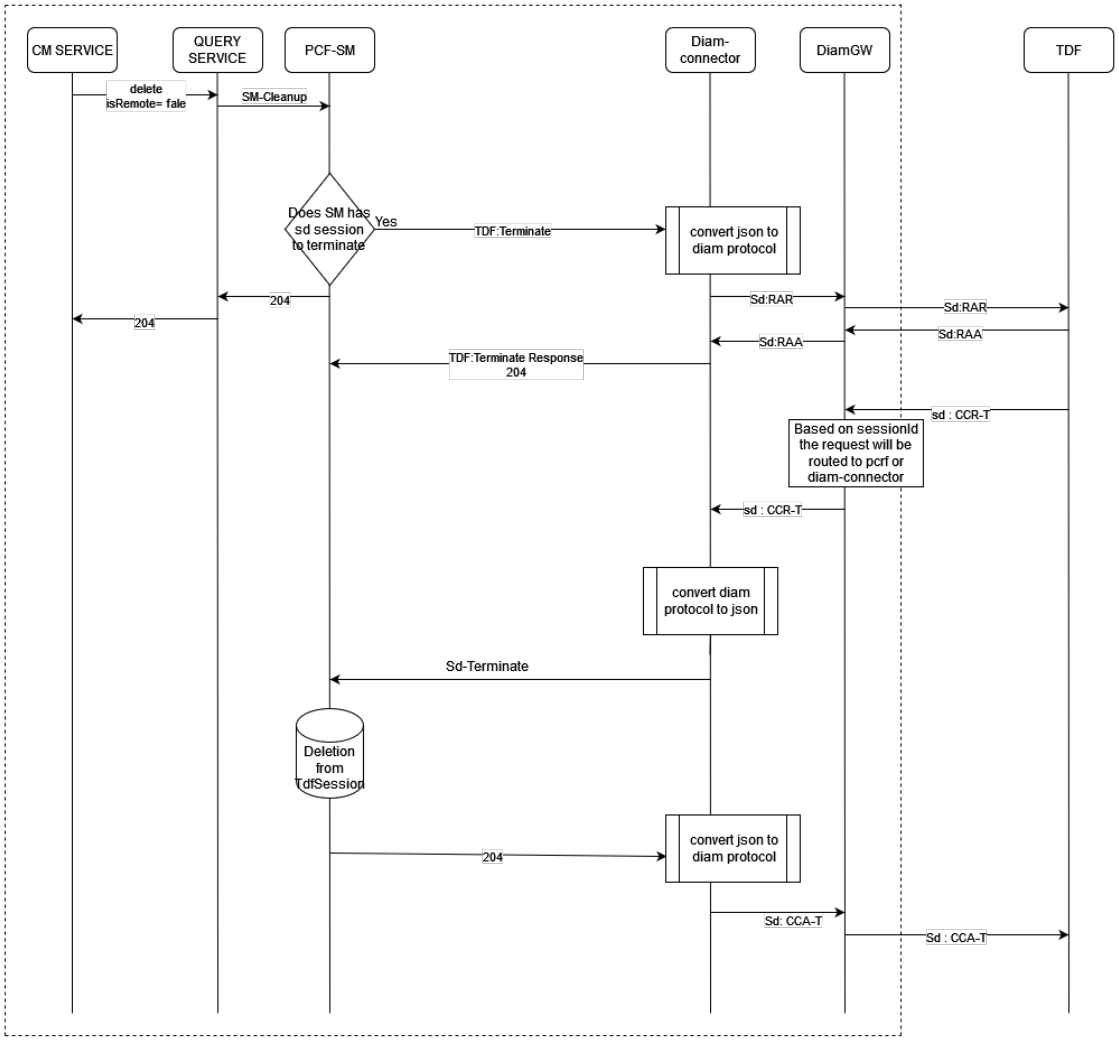
1. CM Service sends ResoureDeleteRequest to Query Service.
2. Query Service sends ResoureDeleteRequest to SM service through TDFAPI.
3. SM service sends RAR with `UNSPECIFIED_REASON` towards TDF through Diameter Connector and Diameter Gateway .
4. SM service receives RAA from TDS and responds to CM service.

> **Note**
>
> Actual TDF session is deleted either when CCR-T is received or when 404 response is received in RAA.

Copyright © 2019, 2026, Oracle and/or its affiliates.

LOCAL DELETE SM SESSION

Figure 4-73 LOCAL DELETE SM SESSION



Query TDF SESSION ID from the **Session Viewer** under **Status and Query** on CNC Console. Click **Delete** to delete the individual session by checking **Initiate Remote Session Cleanup**.

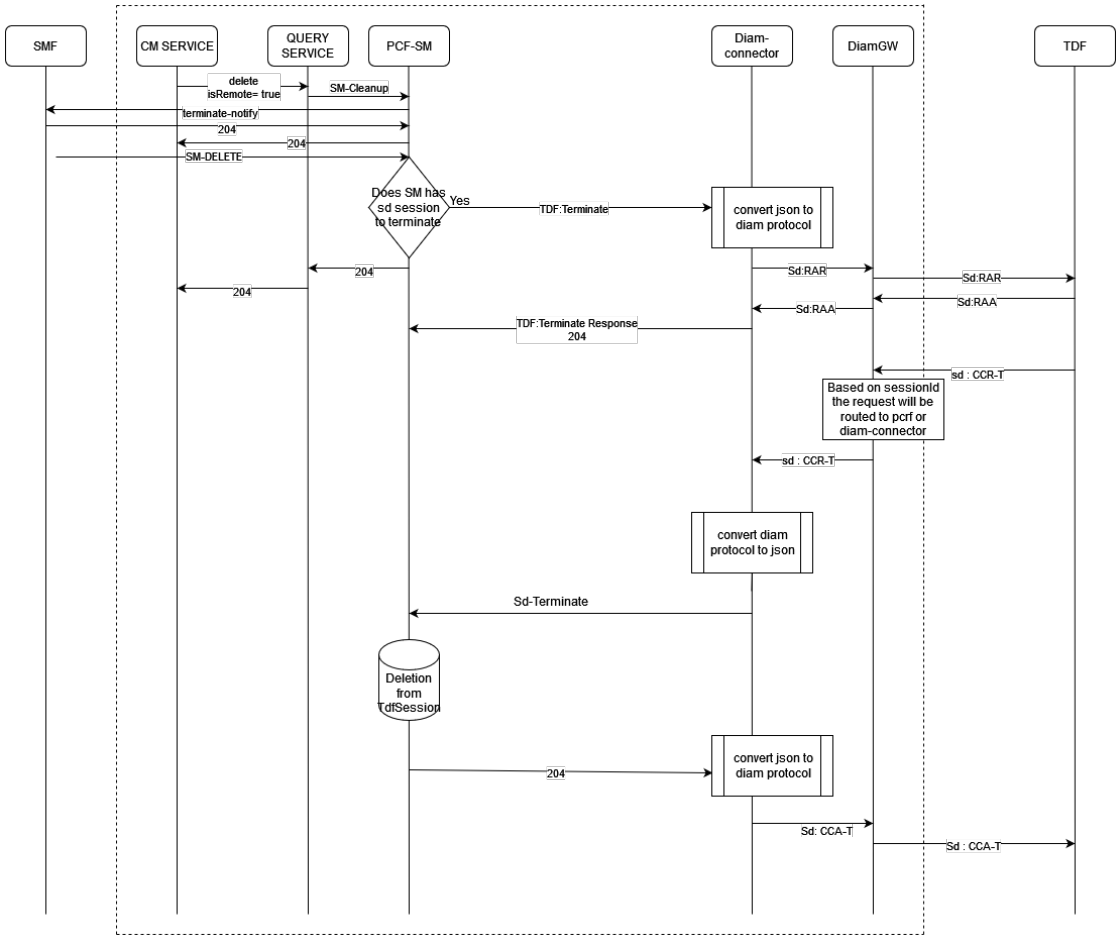
1. CM Service sends ResoureDeleteRequest to Query Service.
2. Query Service sends ResoureDeleteRequest to SM service.
3. SM service sends Terminate Notification towards SMF .
4. SM service receives a response from SMF and then sends the same to CM service.
5. SM service receives SM Delete from SMF.
6. If TDFSessionId is present in smpolicyAssociation, SM service sends RAR towards TDF.
7. Actual TDF session deletion happens when CCR-T is received from TDF or on receive of any error as RAA.

REMOTE DELETE SM SESSION

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> TDF session is deleted only when TDS feature is enabled.

Figure 4-74 REMOTE DELETE SM SESSION



Query TDF SESSION ID from the **Session Viewer** under **Status and Query** on CNC Console. Click **Delete** to delete the individual session by checking **Initiate Remote Session Cleanup**.

1. CM Service sends ResoureDeleteRequest to Query Service.
2. Query Service sends ResoureDeleteRequest to SM service.
3. SM service sends Terminate Notification towards SMF .
4. SM service receives a response from SMF and then sends the same to CM service.
5. SM service receives SM Delete from SMF.
6. If TDFSessionId is present in smpolicyAssociation, SM service sends RAR towards TDF.
7. Actual TDF session deletion happens when CCR-T is received from TDF or on receive of any error as RAA.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Manage Sd Interface Support for PCF

Enable

This feature is not enabled by default.

Configure Using CNC Console

Enable this feature by adding the `TDF.TDF_ENABLED` advanced settings key to PCF Session Management page in CNC Console.

To configure auditing of TDF stale sessions, see PCF Session Management page in CNC Console.

To view the `SM TDF Session` details, see Session Viewer page in CNC Console.

Policy Blockly

The following blockly's are added to the PCF SM category.

- `FQDN from notificationUri`
- `Remove ADC Type Rules`
- `Install ADC Rules`
- `Remove ADC Rules`
- `Establish traffic detection session with peer node name`
- `Establish traffic detection session with peer node set name`
- `Install ADCRules For TimePeriod`

For more details about this blockly, see "PCF-SM Category" section in *Oracle Communications Cloud Native Core, Policy Design Guide*.

Observability

Metrics

Following SM Service Metrics are used to provide information about this feature:

- `occnp_http_out_conn_request_total`
- `occnp_http_out_conn_response_total`
- `ocpm_egress_request_total`
- `ocpm_egress_response_total`
- `occnp_pcf_smservice_overall_processing_time_seconds_count`
- `occnp_pcf_smservice_overall_processing_time_seconds_sum`
- `occnp_pcf_smservice_overall_processing_time_seconds_max`
- `ocpm_egress_request_timeout_total`
- `session_oam_request_total`
- `session_oam_response_total`
- `occnp_http_sm_request_total`
- `occnp_http_sm_response_total`
- `audit_notifications_sent_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- audit_update_notify_session_not_found_total
- audit_update_notify_session_found_total
- audit_update_notify_response_error_total
- audit_update_timestamp_cnt_total
- audit_delete_records_count_total
- audit_delete_records_max_ttl_count_total
- ocpm_late_arrival_rejection_total
- occnp_late_processing_rejection_total

Following Diameter Gateway Metrics are used to provide information about this feature:

- occnp_diam_service_overall_processing_time_seconds
- occnp_diam_service_overall_processing_time_seconds_bucket
- occnp_diam_service_overall_processing_time_seconds_sum
- occnp_diam_service_overall_processing_time_seconds_max
- occnp_diam_request_network_total
- occnp_diam_response_network_total
- occnp_diam_response_latency_seconds_bucket
- occnp_diam_response_latency_seconds_sum
- occnp_diam_response_latency_seconds_count
- occnp_diam_response_latency_seconds_max

Following Diameter Connector Service Metrics are used to provide information about this feature:

- occnp_diam_connector_overall_processing_time_seconds_max
- occnp_diam_connector_overall_processing_time_seconds_count
- occnp_diam_connector_overall_processing_time_seconds_sum
- occnp_stale_diam_request_cleanup_total
- occnp_stale_http_request_cleanup_total

Alerts

The TDF_CONNECTION_DOWN alert is generated when there is a disconnection with configured TDF peer node.

4.28 Handling Collision Between AAR and STR Messages During Update Notify Timeout

Whenever PCF receives a Authorization Authentication Request (AAR-I/AAR-U) from Proxy-Call Session Control Function (P-CSCF), PCF asynchronously responds to P-CSCF with a Authorization Authentication Answer (AAA) and also sends an `UpdateNotify` message to SMF to install the pccRules.

If PCF does not receive any response from SMF and the wait time expires, it applies the session retry logic if configured. If PCF does not receive any response from SMF after all the

Copyright © 2019, 2026, Oracle and/or its affiliates.

retries and during this time if PCF also receives a Session Termination Request (STR) from P-CSCF, PCF sends a `UpdateNotify` message to SMF to remove the pccRules. Thereby, a collision or race condition arises as PCF first sends an `UpdateNotify`message to SMF to install the pccRule and before receiving any response from SMF, PCF also sends an `UpdateNotify` message to SMF to remove the pccRule.

PCF handles concurrency or collision between AAR-I or AAR-U triggered due to `UpdateNotify` to install pccRule and STR messages triggered due to `UpdateNotify` to remove the pccRule.

PCF sends `UpdateNotify` request for pccRule removal to SMF for STR after Timeouts and there is no response received for `UpdateNotify` request sent due to AAR-I/AAR-U.

PCF interacts with P-CSCF to enforce Quality of Service (QoS) parameters. PCF allocates the necessary network resources to ensure VoLTE calls have the lowest possible latency, ensuring call quality.

PCF receives AAR from P-CSCF through BSF to create the dedicated QoS flow for VoLTE session. AAR includes QoS information associated with the bearer. The request includes IP Multimedia Subsystem (IMS) Voice bearer and optionally Video or Real-time text (RTT) bearer.

PCF processes the AAR-I request and sends a `UpdateNotify` for pccRule install to SMF. If PCF does not receive any response from SMF, it retries the request as per session retry configuration.

While PCF is awaiting response for `UpdateNotify` for pccRule install from SMF, if it receives a STR to terminate the session:

- If the wait time to receive response from SMF expires and as per the session retry configuration, if the number of retries is also exhausted, pccRules are deleted from `SmPolicyAssociation` during timeout error handling.
- PCF sends the `UpdateNotify` to SMF due to STR to remove the pccRule depending on whether the pccRules are present in `SmPolicyAssociation` database or not.

Design and Architecture

PCF handles the race condition between multiple `UpdateNotify` messages triggered due to AAR-I or AAR-U and STR requests using `pendingConfirmationAction` advanced settings key.

To handle the race condition, Bulwark service must be enabled and configured to wait for processing the STR request until AAR-I or AAR-U request is complete. Also, the following advanced settings keys for SM service must be configured:

- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.PROCESS_ON_UPDATE`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPONSE_CODES`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS`

For more information on these advanced settings keys for SM service, see PCF Session Management.

When PCF receives AAR, PCF sends `UpdateNotify` to SMF to install the rules. The message to SMF also includes `pendingConfirmationAction` key.

The `pendingConfirmationAction` key indicates if the pccRule is installed in `SmPolicyAssociation` database or not during the timeout error.

If pccRules are installed as part of AAR-I or AAR-U and are saved in `SmPolicyAssociation` database, the `pendingConfirmationAction` key is updated accordingly.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The value of `pendingConfirmationAction` key can be:

- 0 (None)
- 1 (install)
- 2 (remove)

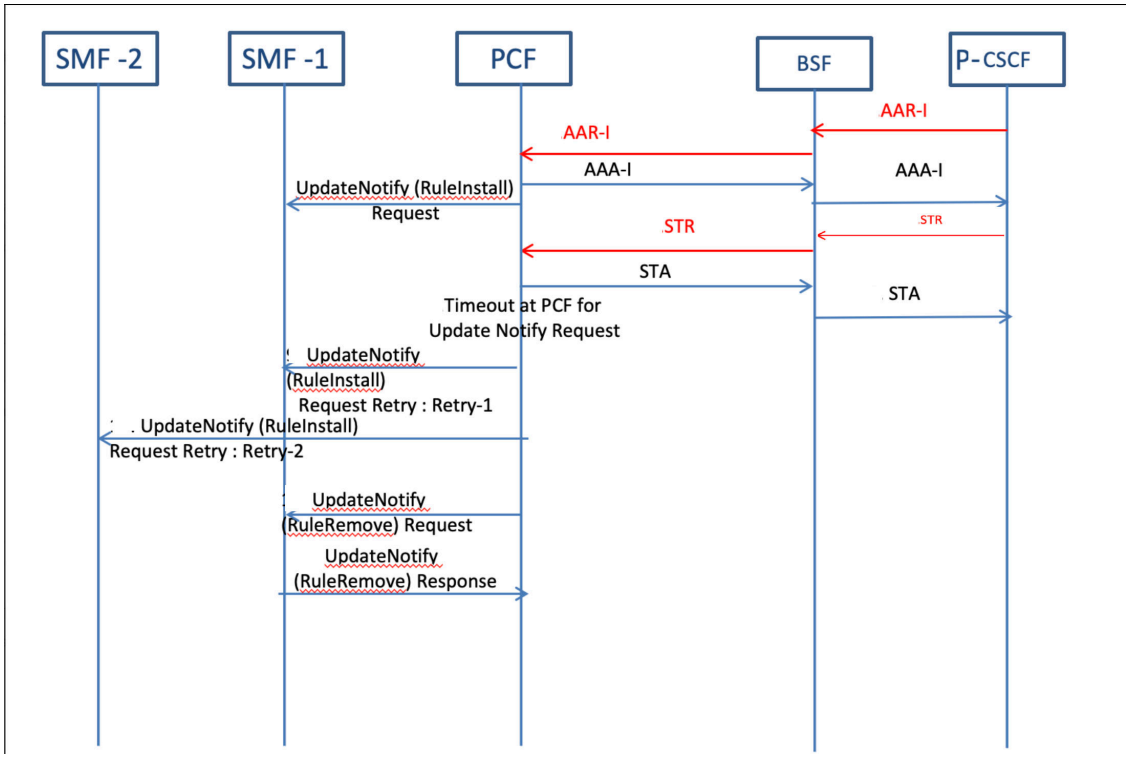
If PCF receives a successful response from SMF for the `UpdateNotify` message sent due to AAR-I or AAR-U, PCF removes the `pendingConfirmationAction` from `SmPolicyAssociation` database.

Otherwise, if PCF receives STR request before receiving any response from SMF, the pccRules are removed from `SmPolicyAssociation` database and `pendingConfirmationAction` key is updated accordingly.

PCF sends `pendingConfirmationAction` key in ASR to P-CSCF depending on `Supress_ASR` key. When `Supress_ASR` key is enabled, PCF does not send `pendingConfirmationAction` to P-CSCF.

Call Flow

Figure 4-75 Handling Collision Between AAR and STR Messages During UpdateNotify Timeout



1. PCF receives requests from P-CSCF to enforce Quality of Service (QoS) parameters. The PCF allocates the necessary network resources to ensure Voice over Long-Term Evolution (VoLTE) calls have the lowest possible latency and high call quality.

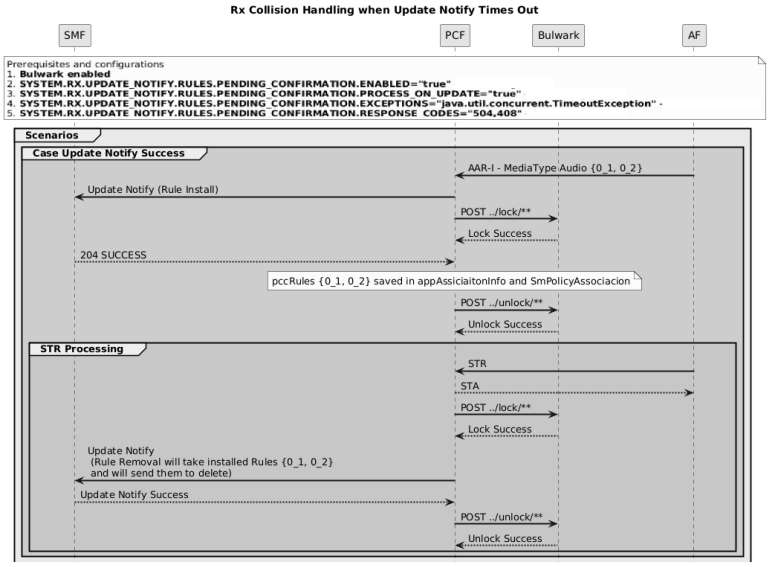
   P-CSCF sends AAR command to PCF through BSF to create the dedicated bearer for Voice over New Radio (VoNR) session. AAR includes QoS information associated with the bearer. The request includes IP Multimedia Subsystem (IMS) Voice bearer and optionally Video/Round-trip time (RTT) bearer.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. BSF sends the request to PCF.
3. PCF responds to P-CSCF with AAA through BSF.
4. BSF forwards the AAA from PCF to P-CSCF through Diameter Gateway.
5. PCF sends an `UpdateNotify` request to SMF triggered due to AAR-I.
6. After sending the `UpdateNotify` request for AAR-I to SMF, PCF waits for configured timeout period.
7. If there is no response for `UpdateNotify` from SMF triggered due to AAR-I, PCF applies the session retry for `SMUpdate` notification.
8. If there is no response from SMF beyond the configured time period and all the retries are over for `UpdateNotify` request sent to SMF due to AAR-I, PCF sends an `UpdateNotify` request to SMF for STR for pccRule removal.

Flow scenarios

Figure 4-76 Handling Collision Between AAR and STR Messages During Update Notify-Success Scenario



In this case, PCF receives an AAR-I message from AF/P-CSCF.

PCF sends the `UpdateNotify` (pccRule install) message to SMF. SMF responds with a 204 Success message.

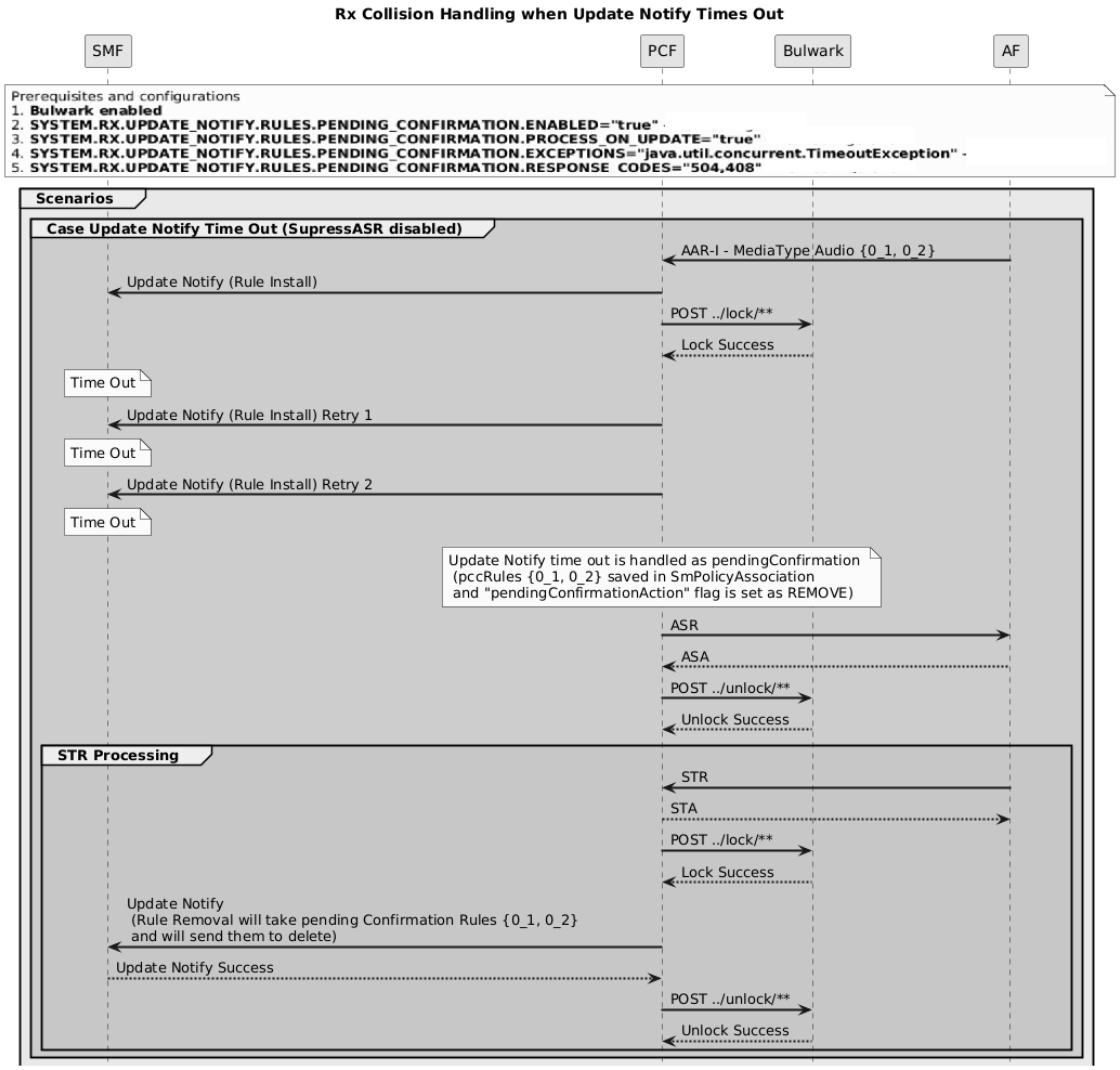
PCF saves the pccRules in the `SMPolicyAssociation` database.

When PCF receives an STR message to terminate the session, it sends an STR request to SMF for pccRule removal.

SMF responds with an `UpdateNotify` success message and PCF removes the pccRules from `SMPolicyAssociation` database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-77 Handling Collision Between AAR and STR Messages During UpdateNotify-Timeout Scenario



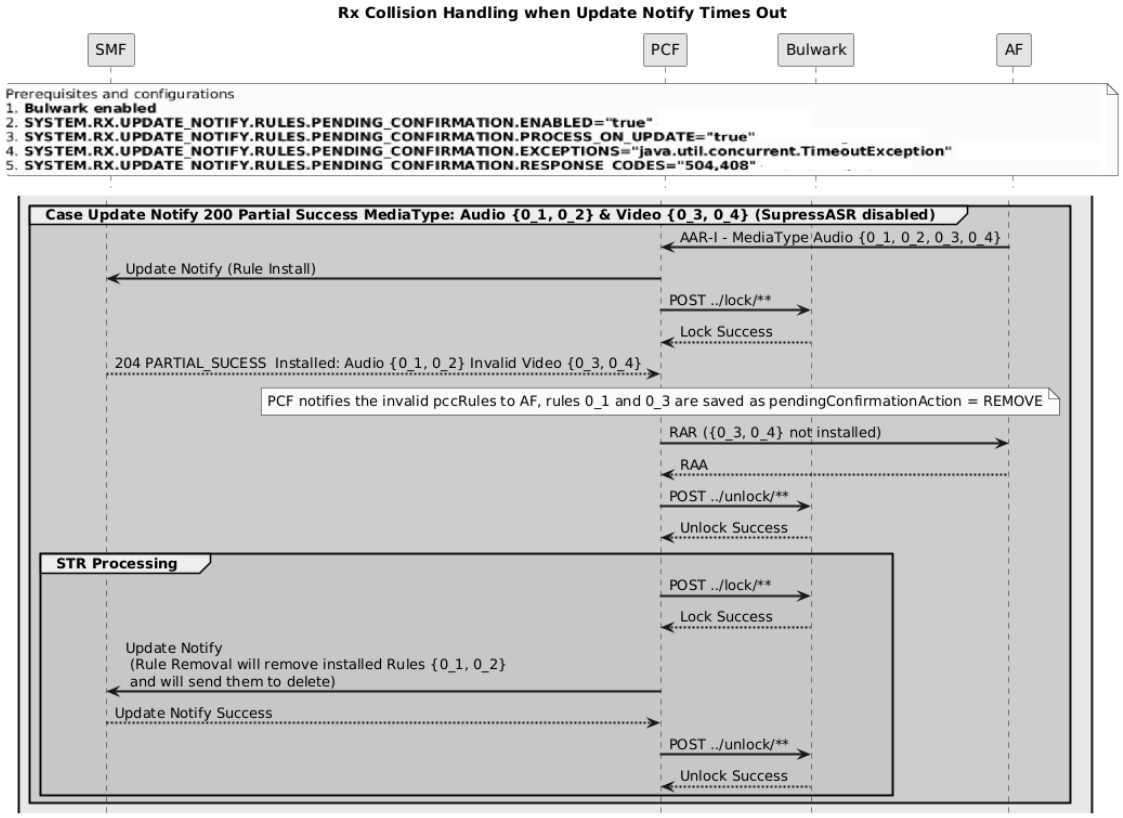
After PCF sends an `UpdateNotify` for pccRule install to SMF, if there is no response from SMF due to Timeout at SMF, PCF applies the session retry.

PCF handles the timeout scenario at SMF based on the following pending confirmation advanced settings keys configured for SM service in CNC Console. Accordingly, PCF saves the pccRules in the database if `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED` advanced settings key is set to `true`.

- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.PROCESS_ON_UPDATE`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPONSE_CODES`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-78 Handling Collision Between AAR and STR Messages During UpdateNotify-Partial Success Scenario

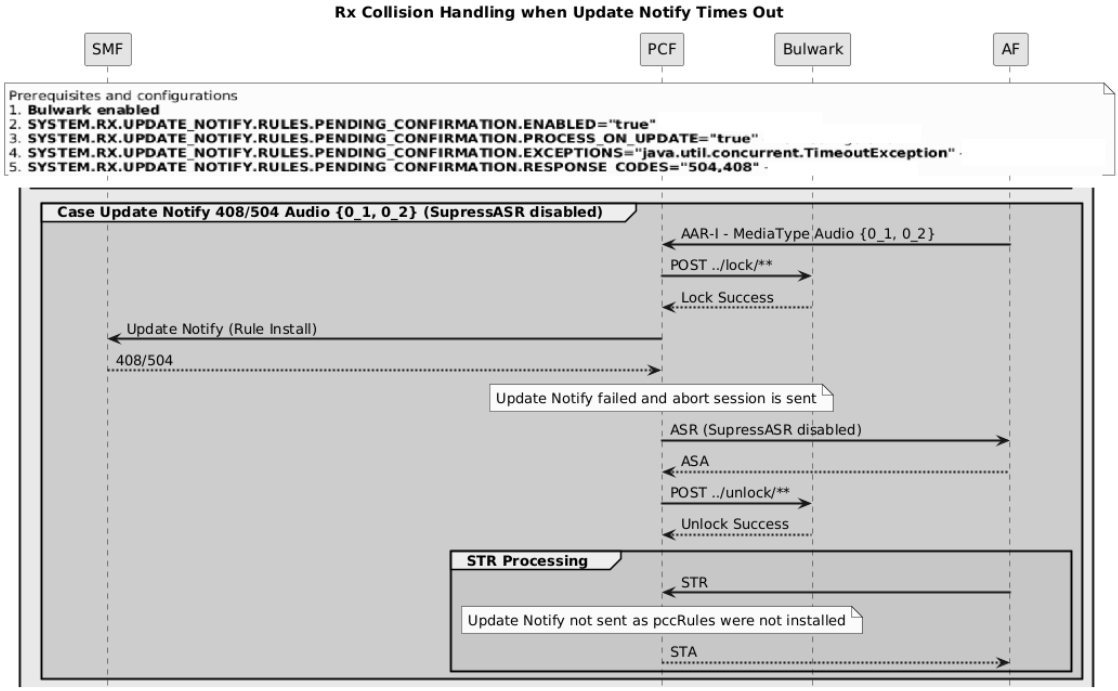


In case of partial success in pccRule installation by SMF, PCF handles the situation as `pending-Success-pendingFailure` (200 partial success response).

- The pccRules sent in `UpdateNotify` are saved in `SMPolicyAssociation` database with `pendingConfirmation` key if `handleUpdateNotifyForRxCollision` key is enabled.
- If PCF receives AAR-U, `smUpdateNotify` is sent with pccRules to create them if `sendPendingConfirmationRulesToInstallOnUpdate` key is enabled. If PCF receives a successful response from SMF, the `pendingConfirmation` key is removed for pccRules.
- If PCF receives AAR-U, `smUpdateNotify` is sent with pccRules to create them if `sendPendingConfirmationRulesToInstallOnUpdate` key is enabled. If PCF receives a successful response from SMF, the `pendingConfirmation` key is removed for pccRules.
- STR is sent with pccRules information to be removed if `sendPendingConfirmationToDeleteOnSTR` key is enabled.
- If PCR receives STR, it sends `SmfUpdateNotify` cleaning up pccRules.
- If PCF receives AAR-U, it sends the pccRules again to confirm if they are installed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

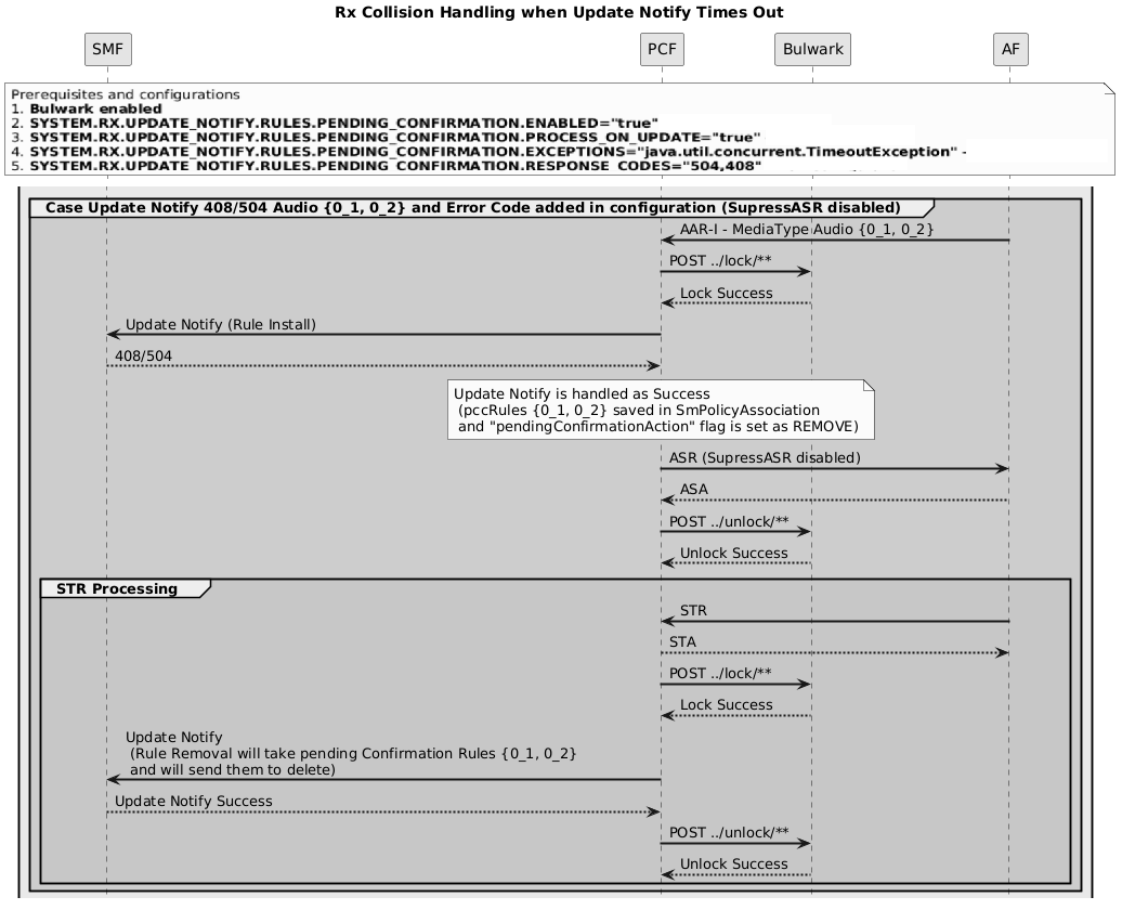
Figure 4-79 Handling Collision Between AAR and STR Messages During UpdateNotify-408 or 504 Errors from SMF



- If SMF responds with Timeout error, 408/504 `REQUEST_TIMEOUT` error code and if `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPONSE_CODES` key is enabled, and pccRules are saved in SMPolicyAssociation database.
- PCF sends a Abort Session Request (ASR) with `SuppressASR` key disabled to AF/P-CSCF.
- AF/P-CSCF responds with Abort Session Answer (ASA).
- PCF receives a STR from AF/P-CSCF. PCF does not send any `UpdateNotify` message to SMF as the pccRules were not installed.
- PCF responds to AF- PCSCF with STA.

Copyright © 2019, 2026, Oracle and/or its affiliates.

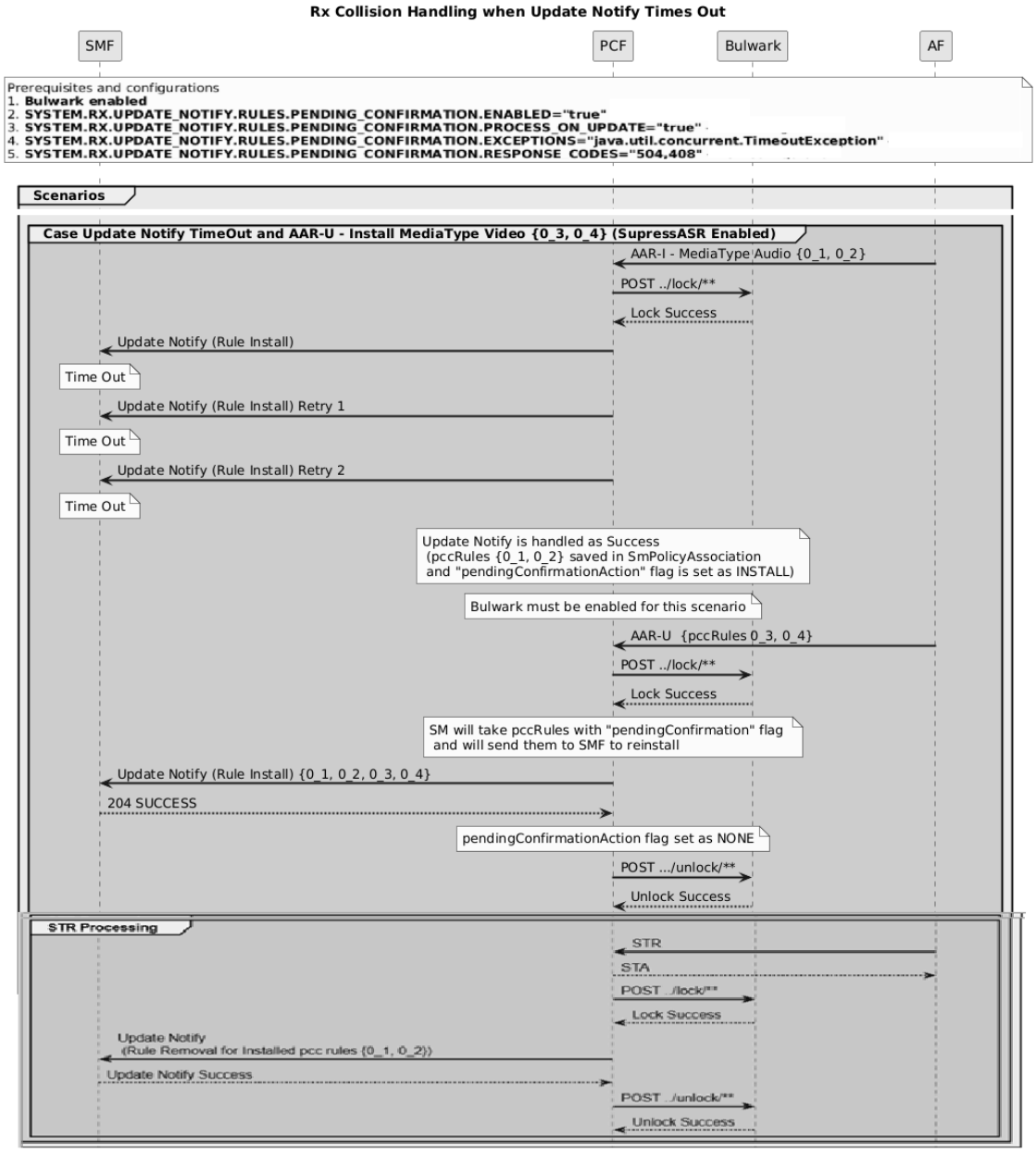
Figure 4-80 Handling Collision Between AAR and STR Messages During UpdateNotify-408 or 504 Errors from SMF When Error Codes are Configured



- If SMF responds with Timeout error, 408/504 `REQUEST_TIMEOUT` error.
- PCF treats the `UpdateNotify` message as `Success`. The pccRules are saved in `SMPolicyAssociation` database. The value of `pendingConfirmationAction` key is set to `REMOVE`.
- PCF sends a Abort Session Request (ASR) with `SuppressASR` disabled to AF/P-CSCF.
- AF/P-CSCF responds with Abort Session Answer (ASA).
- PCF receives a STR from AF/P-CSCF. PCF asynchronously responds with STA to AF/P-CSCF.
- PCF sends the `UpdateNotify` message to SMF for pccRule removal. SMF removes the pccRules and responds with a success message to PCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-81 Handling Collision Between AAR-I, AAR-U, and STR Messages During UpdateNotify-Timeout Scenario with SupressASR Enabled



1. PCF receives an AAR-I from AF/P-CSCF and sends an `UpdateNotify` to SMF to install the pccRule.
2. If PCF does not receive the response from SMF, PCF retries to send the `UpdateNotify` message.
3. PCF treats the response to `UpdateNotify` as `success`. PCF saves the pccRules in `SMPolicyAssociation` database with the value of `pendingConfirmationAction` key set to `INSTALL`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. While awaiting the response for the `UpdateNotify` due to AAR-I from SMF, if PCF receives an AAR-U from AF/P-CSCF, PCF sends an `UpdateNotify` due to AAR-U to SMF.
5. PCF saves the pccRules in `SMPolicyAssociation` database with the value of `pendingConfirmationAction` key set to `REINSTALL`.
6. If SMF responds with a `204 SUCCESS` message, PCF saves the pccRules in `SMPolicyAssociation` database and removes the `PendingConfirmation` key.
7. When PCF receives an STR message from AF/P-CSCF, PCF sends an `UpdateNotify` message to SMF to remove the pccRules.
8. If SMF responds to `UpdateNotify` with a `204 Success` message, PCF removes the pccRules from `SMPolicyAssociation` database.

Managing Collision Between AAR and STR Messages During Update Notify Timeout

Enable

This feature can be enabled by configuring `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED` Advanced Settings Key under **PCF Session Management** page for **Service Configurations** in CNC Console. For more information, see PCF Session Management.

Configure

This feature can be configured using the following Advanced Settings Keys under **PCF Session Management** page for **Service Configurations** in CNC Console.

- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.PROCESS_ON_UPDATE`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPONSE_CODES`
- `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS`

For more information, see PCF Session Management.

Observability

Metrics

This feature uses the following metrics:

- `ocpm_handle_update_notify_timeout_as_pending_confirmation_total`
- `ocpm_handle_update_notify_error_response_as_pending_confirmation_total`
- `ocpm_process_pending_confirmation_rules_on_pa_update_total`
- `ocpm_process_pending_configuration_rules_on_pa_delete_total`
- `ocpm_rx_update_notify_request_total`

For more information, see SM Service Metrics.

Alerts

This feature uses the following alerts:

- `RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL_THRESHOLD`
- `RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_THRESHOLD`
- `RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_THRESHOLD`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHOLD
- RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD
- RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

For more information, see Common Alerts.

Logging

Policy logs collisions that occur when pccRule Removal is sent to SMF during UpdateNotify after timeouts occur for UpdateNotify for AAR messages.

Examples:

AAR-I/AAR-U update notify:


```
{
   "instant":{
      "epochSecond":1737588500,
      "nanoOfSecond":256798000
   },
   "thread":"boundedElastic-7",
   "level":"INFO",
   "loggerName":"ocpm.pcf.service.sm.serviceconnector.SmfConnector",
   "message":"Ready to send Update Notification to SMF: {\n
\"smPolicyDecision\" : {\n    \"pccRules\" : {\n      \"0_3\" : {\n
\"flowInfos\" : [ {\n          \"flowDescription\" : \"permit in 17 from
10.10.10.10 to 10.17.18.19 8001\",\n          \"flowDirection\" :
\"UPLINK\"\n        }, {\n          \"flowDescription\" : \"permit out 17
from 10.17.18.19 to 10.10.10.10 8001\",\n          \"flowDirection\" :
\"DOWNLINK\"\n        } ],\n        \"pccRuleId\" : \"0_3\",\n
\"precedence\" : 401,\n        \"refQosData\" : [ \"qosdata_2\" ],\n
\"refTcData\" : [ \"tcdata_1\" ]\n      },\n      \"0_2\" : {\n
\"flowInfos\" : [ {\n          \"flowDescription\" : \"permit in 17 from
10.10.10.10 to 10.17.18.19 8000\",\n          \"flowDirection\" :
\"UPLINK\"\n        }, {\n          \"flowDescription\" : \"permit out 17
from 10.17.18.19 to 10.10.10.10 8000\",\n          \"flowDirection\" :
\"DOWNLINK\"\n        } ],\n        \"pccRuleId\" : \"0_2\",\n
\"precedence\" : 400,\n        \"refQosData\" : [ \"qosdata_1\" ],\n
\"refTcData\" : [ \"tcdata_0\" ]\n      }\n    },\n    \"qosDecs\" : {\n
\"qosdata_1\" : {\n        \"5qi\" : 1,\n        \"qosId\" :
\"qosdata_1\",\n        \"maxbrUl\" : \"12.0 Kbps\",\n        \"maxbrDl\" :
\"12.0 Kbps\",\n        \"gbrUl\" : \"12.0 Kbps\",\n        \"gbrDl\" :
\"12.0 Kbps\",\n        \"arp\" : {\n          \"priorityLevel\" :
15,\n          \"preemptCap\" : \"NOT_PREEMPT\",\n          \"preemptVuln\" :
\"PREEMPTABLE\"\n        }\n      },\n      \"qosdata_2\" : {\n
\"5qi\" : 1,\n        \"qosId\" : \"qosdata_2\",\n        \"maxbrUl\" :
\"600.0 bps\",\n        \"maxbrDl\" : \"600.0 bps\",\n        \"gbrUl\" :
\"600.0 bps\",\n        \"gbrDl\" : \"600.0 bps\",\n        \"arp\" :
{\n          \"priorityLevel\" : 15,\n          \"preemptCap\" :
\"NOT_PREEMPT\",\n          \"preemptVuln\" : \"PREEMPTABLE\"\n        }
\n      }\n    },\n    \"traffContDecs\" : {\n      \"tcdata_0\" : {\n
\"tcId\" : \"tcdata_0\",\n        \"flowStatus\" :
\"ENABLED\"\n      },\n      \"tcdata_1\" : {\n        \"tcId\" :
\"tcdata_1\",\n        \"flowStatus\" : \"ENABLED\"\n      }\n    },\n
\"policyCtrlReqTriggers\" : [ \"PLMN_CH\", \"UE_IP_CH\", \"DEF_QOS_CH\",
\"AC_TY_CH\", \"SUCC_RES_ALLO\" ],\n    \"lastReqRuleData\" : [ {\n
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
\"refPccRuleIds\" : [ \"0_2\", \"0_3\" ],\n      \"reqData\" :
[ \"SUCC_RES_ALLO\" ]\n    } ]\n  },\n  \"resourceUri\" : \"https://
pcf_smservice.pcf:5805/npcf-smpolicycontrol/v1/sm-policies/1eb1b1bc-9e51-4ac0-
ae38-13f21af05318_0_U1VQSTppbXNpLTQ1MDA4MTAwMDAwODAwMTs=\"\n}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":293,
   "threadPriority":5,
   "messageTimestamp":"2025-01-22T17:28:20.256-0600",
   "ocLogId":"${ctx:ocLogId}"
}"TimeOut Exception
Time Out"{
   "instant":{
      "epochSecond":1737588500,
      "nanoOfSecond":257747000
   },
   "thread":"boundedElastic-7",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.user.UserManager",
   "message":"process user service request",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":293,
   "threadPriority":5,
   "messageTimestamp":"2025-01-22T17:28:20.257-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1737588500,
      "nanoOfSecond":257766000
   },
   "thread":"boundedElastic-7",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.user.UserManager",
   "message":"Processing Async policyCounterActions.",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":293,
   "threadPriority":5,
   "messageTimestamp":"2025-01-22T17:28:20.257-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1737588503,
      "nanoOfSecond":261970000
   },
   "thread":"boundedElastic-7",
   "level":"WARN",
   "loggerName":"ocpm.pcf.util.StackTraceUtil",
   "message":"Failed to call SMF",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":293,
   "threadPriority":5,
   "messageTimestamp":"2025-01-22T17:28:23.261-0600",
   "triggerClass":"ocpm.pcf.service.sm.serviceconnector.SmfConnector",
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   "errorName":"java.util.concurrent.TimeoutException",
   "errorMessage":"Did not observe any item or terminal signal within 3000ms
in 'source(MonoDeferContextual)' (and no fallback has been configured)",

"errorStack":"[reactor.core.publisher.FluxTimeout$TimeoutMainSubscriber.handle
Timeout(FluxTimeout.java:295),
reactor.core.publisher.FluxTimeout$TimeoutMainSubscriber.doTimeout(FluxTimeout
.java:280),
reactor.core.publisher.FluxTimeout$TimeoutTimeoutSubscriber.onNext(FluxTimeout
.java:419),
reactor.core.publisher.FluxOnErrorReturn$ReturnSubscriber.onNext(FluxOnErrorRe
turn.java:162),
reactor.core.publisher.MonoDelay$MonoDelayRunnable.propagateDelay(MonoDelay.ja
va:271),
reactor.core.publisher.MonoDelay$MonoDelayRunnable.run(MonoDelay.java:286),
reactor.core.scheduler.SchedulerTask.call(SchedulerTask.java:68),
reactor.core.scheduler.SchedulerTask.call(SchedulerTask.java:28),
io.micrometer.core.instrument.composite.CompositeTimer.recordCallable(Composit
eTimer.java:129),
io.micrometer.core.instrument.Timer.lambda$wrap$1(Timer.java:206), java.base/
java.util.concurrent.FutureTask.run(FutureTask.java:264), java.base/
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Sched
uledThreadPoolExecutor.java:304), java.base/
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136
), java.base/
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635
), java.base/java.lang.Thread.run(Thread.java:840)]"
}"Handling time out for Rx Collision
Handle as Success"{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":965052000
   },
   "thread":"boundedElastic-2",
   "level":"INFO",

"loggerName":"ocpm.pcf.service.sm.domain.component.rule.PendingConfirmationRul
eHelper",
   "message":"PccRules in Update Notify failure will be set as
pendingConfirmation",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.965-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":965553000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",

"loggerName":"ocpm.pcf.service.sm.domain.component.rule.PendingConfirmationRul
eHelper",
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   "message":"PccRule 0_3 set as pendingConfirmation",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.965-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":965600000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",

"loggerName":"ocpm.pcf.service.sm.domain.component.rule.PendingConfirmationRul
eHelper",
   "message":"PccRule 0_2 set as pendingConfirmation",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.965-0600",
   "ocLogId":"${ctx:ocLogId}"
}"Metric Pegged
Metric"{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":959692000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.metrics.SmMetrics",
   "message":"Pegging Handle Update Notify timeout as Pending Confirmation
metric, Operation Type: update_notify, Cause: Update Notify Time Out handled
as PendingConfirmation",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.959-0600",
   "ocLogId":"${ctx:ocLogId}"
}"STR Update Notify (Rule Remove)
STR Update Notify"{
   "instant":{
      "epochSecond":1746472392,
      "nanoOfSecond":580363000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.metrics.SmMetrics",
   "message":"Pegging Sent pending confirmation rules to remove metric,
Operation Type: update_notify",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:12.580-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472392,
      "nanoOfSecond":580524000
   },
   "thread":"boundedElastic-2",
   "level":"INFO",
   "loggerName":"ocpm.pcf.service.sm.serviceconnector.SmfConnector",
   "message":"Ready to send Update Notification to SMF: {\n
\"smPolicyDecision\" : {\n    \"pccRules\" : {\n      \"0_2\" : null,\n
\"0_3\" : null\n    },\n    \"qosDecs\" : {\n      \"qosdata_1\" :
null,\n      \"qosdata_2\" : null\n    },\n    \"traffContDecs\" : {\n
\"tcdata_0\" : null,\n      \"tcdata_1\" : null\n    }\n  },\n
\"resourceUri\" : \"https://pcf_smservice.pcf:5805/npcf-smpolicycontrol/v1/sm-
policies/00ec301a-77eb-4536-
aea1-394a6f33ea00_0_U1VQSTppbXNpLTQ1MDA4MTAwMDAwODAwMTs=\"\n}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:12.580-0600",
   "ocLogId":"${ctx:ocLogId}"
}"ASR
ASR"{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":978063000
   },
   "thread":"boundedElastic-2",
   "level":"INFO",
   "loggerName":"ocpm.pcf.service.pa.serviceconnector.AfConnector",
   "message":"Sent Termination Notification to AF: http://localhost:1080/
smservicenotify/terminate, \n class TerminationInfo {\n    termCause:
ALL_SDF_DEACTIVATION\n    resUri: https://pcf_smservice.pcf:5805/npcf-
policyauthorization/v1/app-sessions/6f3f0561-3365-4516-886b-831833b6ac74\n}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.978-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":978165000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",

"loggerName":"ocpm.pcf.service.sm.domain.component.pcrt.PolicyTriggerManager",
   "message":"Details for appSession are:
AppSessionImpl{appSessionContext=class AppSessionContext {\n    ascReqData:
class AppSessionContextReqData {\n        afAppId: urn:urn-7:3gpp-
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
service.ims.icsi.mmtel\n        afRoutReq: Optional.empty\n        aspId:
null\n        bdtRefId: null\n        dnn: null\n        evSubsc:
Optional[class EventsSubscReqData {\n            events: [class
AfEventSubscription {\n                event:
FAILED_RESOURCES_ALLOCATION\n                notifMethod:
EVENT_DETECTION\n            }]\n            notifUri: http://localhost:1080/
smservicenotify/\n            usgThres: null\n            reqAnis:
null\n        }]\n        medComponents: null\n        ipDomain:
null\n        mpsId: null\n        notifUri: http://localhost:1080/
smservicenotify/\n        sliceInfo: null\n        sponId: null\n
sponStatus: null\n        supi: null\n        suppFeat: 10\n        ueIpv4:
192.168.10.10\n        ueIpv6: null\n        ueMac: null\n        serviceUrn:
null\n        servInfStatus: null\n        liIndicatorEncrypted:
null\n        authorizationLifetime: null\n    }\n    ascRespData: class
AppSessionContextRespData {\n        servAuthInfo: null\n        suppFeat:
10\n    }\n    evsNotif: null\n}, smPolicyAssociationId='00ec301a-77eb-4536-
aea1-394a6f33ea00_0_U1VQSTppbXNpLTQ1MDA4MTAwMDAwODAwMTs=',
emergencyServiceUrn=false,
flowMetadatas={1.1=ocpm.pcf.service.pa.domain.model.FlowMetadata@442b970,
1.2=ocpm.pcf.service.pa.domain.model.FlowMetadata@3baab8ae},
AssociationImpl{associationId='6f3f0561-3365-4516-886b-831833b6ac74',
supportedFeatures='10', supportedFeatureBits={4}, variables=null,
routingContexts=null, sbiBinding={}, prodNfInstId=null,
nfInstanceId=fe7d992b-0541-4c7d-ab84-c6d70b1b0123,
sbiCorrelationInfoHeader=null}}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.978-0600",
   "ocLogId":"${ctx:ocLogId}"
}"Policy Decision  after AAR-I
SmPolicy Association After AAR-I Collapse source""sessRules":{
   "0_1":{
      "authSessAmbr":{
         "uplink":"500.0 Kbps",
         "downlink":"1.0 Mbps"
      },
      "authDefQos":{
         "5qi":5,
         "arp":{
            "priorityLevel":1,
            "preemptCap":"NOT_PREEMPT",
            "preemptVuln":"NOT_PREEMPTABLE"
         },
         "priorityLevel":2
      },
      "sessRuleId":"0_1"
   }
},
"pccRules":{
   "0_0":{
      "flowInfos":[
         {
            "flowDescription":"permit in ip from any to any",
            "flowDirection":"UPLINK"
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
            },
            {
               "flowDescription":"permit out ip from any to any",
               "flowDirection":"DOWNLINK"
            }
         ],
         "pccRuleId":"0_0",
         "precedence":3000,
         "refQosData":[
            "qosdata_0"
         ],
         "pendingConfirmationAction":0
      },
      "0_2":{
         "flowInfos":[
            {
               "flowDescription":"permit in 17 from 10.10.10.10 to 10.17.18.19
8000",
               "flowDirection":"UPLINK"
            },
            {
               "flowDescription":"permit out 17 from 10.17.18.19 to 10.10.10.10
8000",
               "flowDirection":"DOWNLINK"
            }
         ],
         "pccRuleId":"0_2",
         "precedence":400,
         "refQosData":[
            "qosdata_1"
         ],
         "refTcData":[
            "tcdata_0"
         ],
         "pendingConfirmationAction":2
      },
      "0_3":{
         "flowInfos":[
            {
               "flowDescription":"permit in 17 from 10.10.10.10 to 10.17.18.19
8001",
               "flowDirection":"UPLINK"
            },
            {
               "flowDescription":"permit out 17 from 10.17.18.19 to 10.10.10.10
8001",
               "flowDirection":"DOWNLINK"
            }
         ],
         "pccRuleId":"0_3",
         "precedence":401,
         "refQosData":[
            "qosdata_2"
         ],
         "refTcData":[
            "tcdata_1"
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
      ],
      "pendingConfirmationAction":2
   }
},
"qosDecs":{
   "qosdata_0":{
      "5qi":5,
      "qosId":"qosdata_0",
      "arp":{
         "priorityLevel":1,
         "preemptCap":"NOT_PREEMPT",
         "preemptVuln":"NOT_PREEMPTABLE"
      },
      "priorityLevel":2
   },
   "qosdata_1":{
      "5qi":1,
      "qosId":"qosdata_1",
      "maxbrUl":"12.0 Kbps",
      "maxbrDl":"12.0 Kbps",
      "gbrUl":"12.0 Kbps",
      "gbrDl":"12.0 Kbps",
      "arp":{
         "priorityLevel":15,
         "preemptCap":"NOT_PREEMPT",
         "preemptVuln":"PREEMPTABLE"
      }
   },
   "qosdata_2":{
      "5qi":1,
      "qosId":"qosdata_2",
      "maxbrUl":"600.0 bps",
      "maxbrDl":"600.0 bps",
      "gbrUl":"600.0 bps",
      "gbrDl":"600.0 bps",
      "arp":{
         "priorityLevel":15,
         "preemptCap":"NOT_PREEMPT",
         "preemptVuln":"PREEMPTABLE"
      }
   }
},
"chgDecs":{

},
"traffContDecs":{
   "tcdata_0":{
      "tcId":"tcdata_0",
      "flowStatus":"ENABLED"
   },
   "tcdata_1":{
      "tcId":"tcdata_1",
      "flowStatus":"ENABLED"
   }
},
"conds":{
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
},
"policyCtrlReqTriggers":[
   "PLMN_CH",
   "UE_IP_CH",
   "DEF_QOS_CH",
   "AC_TY_CH"
]
}
```


Timeout exception:


```
{
   "instant":{
      "epochSecond":1737588500,
      "nanoOfSecond":257747000
   },
   "thread":"boundedElastic-7",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.user.UserManager",
   "message":"process user service request",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":293,
   "threadPriority":5,
   "messageTimestamp":"2025-01-22T17:28:20.257-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1737588500,
      "nanoOfSecond":257766000
   },
   "thread":"boundedElastic-7",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.user.UserManager",
   "message":"Processing Async policyCounterActions.",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":293,
   "threadPriority":5,
   "messageTimestamp":"2025-01-22T17:28:20.257-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1737588503,
      "nanoOfSecond":261970000
   },
   "thread":"boundedElastic-7",
   "level":"WARN",
   "loggerName":"ocpm.pcf.util.StackTraceUtil",
   "message":"Failed to call SMF",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":293,
   "threadPriority":5,
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   "messageTimestamp":"2025-01-22T17:28:23.261-0600",
   "triggerClass":"ocpm.pcf.service.sm.serviceconnector.SmfConnector",
   "errorName":"java.util.concurrent.TimeoutException",
   "errorMessage":"Did not observe any item or terminal signal within 3000ms
in 'source(MonoDeferContextual)' (and no fallback has been configured)",

"errorStack":"[reactor.core.publisher.FluxTimeout$TimeoutMainSubscriber.handle
Timeout(FluxTimeout.java:295),
reactor.core.publisher.FluxTimeout$TimeoutMainSubscriber.doTimeout(FluxTimeout
.java:280),
reactor.core.publisher.FluxTimeout$TimeoutTimeoutSubscriber.onNext(FluxTimeout
.java:419),
reactor.core.publisher.FluxOnErrorReturn$ReturnSubscriber.onNext(FluxOnErrorRe
turn.java:162),
reactor.core.publisher.MonoDelay$MonoDelayRunnable.propagateDelay(MonoDelay.ja
va:271),
reactor.core.publisher.MonoDelay$MonoDelayRunnable.run(MonoDelay.java:286),
reactor.core.scheduler.SchedulerTask.call(SchedulerTask.java:68),
reactor.core.scheduler.SchedulerTask.call(SchedulerTask.java:28),
io.micrometer.core.instrument.composite.CompositeTimer.recordCallable(Composit
eTimer.java:129),
io.micrometer.core.instrument.Timer.lambda$wrap$1(Timer.java:206), java.base/
java.util.concurrent.FutureTask.run(FutureTask.java:264), java.base/
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Sched
uledThreadPoolExecutor.java:304), java.base/
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136
), java.base/
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635
), java.base/java.lang.Thread.run(Thread.java:840)]"
}
```


Handling timeout for Rx collision:


```
{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":965052000
   },
   "thread":"boundedElastic-2",
   "level":"INFO",

"loggerName":"ocpm.pcf.service.sm.domain.component.rule.PendingConfirmationRul
eHelper",
   "message":"PccRules in Update Notify failure will be set as
pendingConfirmation",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.965-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":965553000
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",

"loggerName":"ocpm.pcf.service.sm.domain.component.rule.PendingConfirmationRul
eHelper",
   "message":"PccRule 0_3 set as pendingConfirmation",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.965-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":965600000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",

"loggerName":"ocpm.pcf.service.sm.domain.component.rule.PendingConfirmationRul
eHelper",
   "message":"PccRule 0_2 set as pendingConfirmation",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.965-0600",
   "ocLogId":"${ctx:ocLogId}"
}


{"instant":
{"epochSecond":1738790542,"nanoOfSecond":924361000},"thread":"boundedElastic-4
","level":"DEBUG","loggerName":"ocpm.pcf.service.sm.serviceconnector.SmfConnec
tor","message":"PccRules [0_2, 0_3] added to be removed by STR as TimeOut
happened","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":106,"threadPriority":5,"messageTimestamp":"2025-02-05T15:22:22.9
24-0600","ocLogId":"${ctx:ocLogId}"}
```


Metric pegged:


```
{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":959692000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.metrics.SmMetrics",
   "message":"Pegging Handle Update Notify timeout as Pending Confirmation
metric, Operation Type: update_notify, Cause: Update Notify Time Out handled
as PendingConfirmation",
   "endOfBatch":false,
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.959-0600",
   "ocLogId":"${ctx:ocLogId}"
}
```


STR update notify:


```
{
   "instant":{
      "epochSecond":1746472392,
      "nanoOfSecond":580363000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",
   "loggerName":"ocpm.pcf.service.sm.domain.component.metrics.SmMetrics",
   "message":"Pegging Sent pending confirmation rules to remove metric,
Operation Type: update_notify",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:12.580-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472392,
      "nanoOfSecond":580524000
   },
   "thread":"boundedElastic-2",
   "level":"INFO",
   "loggerName":"ocpm.pcf.service.sm.serviceconnector.SmfConnector",
   "message":"Ready to send Update Notification to SMF: {\n
\"smPolicyDecision\" : {\n    \"pccRules\" : {\n      \"0_2\" : null,\n
\"0_3\" : null\n    },\n    \"qosDecs\" : {\n      \"qosdata_1\" :
null,\n      \"qosdata_2\" : null\n    },\n    \"traffContDecs\" : {\n
\"tcdata_0\" : null,\n      \"tcdata_1\" : null\n    }\n  },\n
\"resourceUri\" : \"https://pcf_smservice.pcf:5805/npcf-smpolicycontrol/v1/sm-
policies/00ec301a-77eb-4536-
aea1-394a6f33ea00_0_U1VQSTppbXNpLTQ1MDA4MTAwMDAwODAwMTs=\"\n}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:12.580-0600",
   "ocLogId":"${ctx:ocLogId}"
}
```


ASR


```
{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":978063000
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   },
   "thread":"boundedElastic-2",
   "level":"INFO",
   "loggerName":"ocpm.pcf.service.pa.serviceconnector.AfConnector",
   "message":"Sent Termination Notification to AF: http://localhost:1080/
smservicenotify/terminate, \n class TerminationInfo {\n    termCause:
ALL_SDF_DEACTIVATION\n    resUri: https://pcf_smservice.pcf:5805/npcf-
policyauthorization/v1/app-sessions/6f3f0561-3365-4516-886b-831833b6ac74\n}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.978-0600",
   "ocLogId":"${ctx:ocLogId}"
}{
   "instant":{
      "epochSecond":1746472387,
      "nanoOfSecond":978165000
   },
   "thread":"boundedElastic-2",
   "level":"DEBUG",

"loggerName":"ocpm.pcf.service.sm.domain.component.pcrt.PolicyTriggerManager",
   "message":"Details for appSession are:
AppSessionImpl{appSessionContext=class AppSessionContext {\n    ascReqData:
class AppSessionContextReqData {\n        afAppId: urn:urn-7:3gpp-
service.ims.icsi.mmtel\n        afRoutReq: Optional.empty\n        aspId:
null\n        bdtRefId: null\n        dnn: null\n        evSubsc:
Optional[class EventsSubscReqData {\n            events: [class
AfEventSubscription {\n                event:
FAILED_RESOURCES_ALLOCATION\n                notifMethod:
EVENT_DETECTION\n            }]\n            notifUri: http://localhost:1080/
smservicenotify/\n            usgThres: null\n            reqAnis:
null\n        }]\n        medComponents: null\n        ipDomain:
null\n        mpsId: null\n        notifUri: http://localhost:1080/
smservicenotify/\n        sliceInfo: null\n        sponId: null\n
sponStatus: null\n        supi: null\n        suppFeat: 10\n        ueIpv4:
192.168.10.10\n        ueIpv6: null\n        ueMac: null\n        serviceUrn:
null\n        servInfStatus: null\n        liIndicatorEncrypted:
null\n        authorizationLifetime: null\n    }\n    ascRespData: class
AppSessionContextRespData {\n        servAuthInfo: null\n        suppFeat:
10\n    }\n    evsNotif: null\n}, smPolicyAssociationId='00ec301a-77eb-4536-
aea1-394a6f33ea00_0_U1VQSTppbXNpLTQ1MDA4MTAwMDAwODAwMTs=',
emergencyServiceUrn=false,
flowMetadatas={1.1=ocpm.pcf.service.pa.domain.model.FlowMetadata@442b970,
1.2=ocpm.pcf.service.pa.domain.model.FlowMetadata@3baab8ae},
AssociationImpl{associationId='6f3f0561-3365-4516-886b-831833b6ac74',
supportedFeatures='10', supportedFeatureBits={4}, variables=null,
routingContexts=null, sbiBinding={}, prodNfInstId=null,
nfInstanceId=fe7d992b-0541-4c7d-ab84-c6d70b1b0123,
sbiCorrelationInfoHeader=null}}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
   "threadId":95,
   "threadPriority":5,
   "messageTimestamp":"2025-05-05T13:13:07.978-0600",
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
   "ocLogId":"${ctx:ocLogId}"
}
```

SMPolicyAssociation after AAR-I:

```
"sessRules": {
    "0_1": {
      "authSessAmbr": {
        "uplink": "500.0 Kbps",
        "downlink": "1.0 Mbps"
      },
      "authDefQos": {
        "5qi": 5,
        "arp": {
          "priorityLevel": 1,
          "preemptCap": "NOT_PREEMPT",
          "preemptVuln": "NOT_PREEMPTABLE"
        },
        "priorityLevel": 2
      },
      "sessRuleId": "0_1"
    }
  },
  "pccRules": {
    "0_0": {
      "flowInfos": [
        {
          "flowDescription": "permit in ip from any to any",
          "flowDirection": "UPLINK"
        },
        {
          "flowDescription": "permit out ip from any to any",
          "flowDirection": "DOWNLINK"
        }
      ],
      "pccRuleId": "0_0",
      "precedence": 3000,
      "refQosData": [
        "qosdata_0"
      ],
      "pendingConfirmationAction": 0
    },
    "0_2": {
      "flowInfos": [
        {
          "flowDescription": "permit in 17 from 10.10.10.10 to 10.17.18.19
8000",
          "flowDirection": "UPLINK"
        },
        {
          "flowDescription": "permit out 17 from 10.17.18.19 to 10.10.10.10
8000",
          "flowDirection": "DOWNLINK"
        }
      ],
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
      "pccRuleId": "0_2",
      "precedence": 400,
      "refQosData": [
        "qosdata_1"
      ],
      "refTcData": [
        "tcdata_0"
      ],
      "pendingConfirmationAction": 2
    },
    "0_3": {
      "flowInfos": [
        {
          "flowDescription": "permit in 17 from 10.10.10.10 to 10.17.18.19
8001",
          "flowDirection": "UPLINK"
        },
        {
          "flowDescription": "permit out 17 from 10.17.18.19 to 10.10.10.10
8001",
          "flowDirection": "DOWNLINK"
        }
      ],
      "pccRuleId": "0_3",
      "precedence": 401,
      "refQosData": [
        "qosdata_2"
      ],
      "refTcData": [
        "tcdata_1"
      ],
      "pendingConfirmationAction": 2
    }
  },
  "qosDecs": {
    "qosdata_0": {
      "5qi": 5,
      "qosId": "qosdata_0",
      "arp": {
        "priorityLevel": 1,
        "preemptCap": "NOT_PREEMPT",
        "preemptVuln": "NOT_PREEMPTABLE"
      },
      "priorityLevel": 2
    },
    "qosdata_1": {
      "5qi": 1,
      "qosId": "qosdata_1",
      "maxbrUl": "12.0 Kbps",
      "maxbrDl": "12.0 Kbps",
      "gbrUl": "12.0 Kbps",
      "gbrDl": "12.0 Kbps",
      "arp": {
        "priorityLevel": 15,
        "preemptCap": "NOT_PREEMPT",
        "preemptVuln": "PREEMPTABLE"
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
      }
    },
    "qosdata_2": {
      "5qi": 1,
      "qosId": "qosdata_2",
      "maxbrUl": "600.0 bps",
      "maxbrDl": "600.0 bps",
      "gbrUl": "600.0 bps",
      "gbrDl": "600.0 bps",
      "arp": {
        "priorityLevel": 15,
        "preemptCap": "NOT_PREEMPT",
        "preemptVuln": "PREEMPTABLE"
      }
    }
  },
  "chgDecs": {
  },
  "traffContDecs": {
    "tcdata_0": {
      "tcId": "tcdata_0",
      "flowStatus": "ENABLED"
    },
    "tcdata_1": {
      "tcId": "tcdata_1",
      "flowStatus": "ENABLED"
    }
  },
  "conds": {
  },
  "policyCtrlReqTriggers": [
    "PLMN_CH",
    "UE_IP_CH",
    "DEF_QOS_CH",
    "AC_TY_CH"
  ]
}
```

SmPolicy Association after STR

```
{
  "httpRequest" : {
    "method" : "POST",
    "path" : "/smf/notify/update",
    "body" : {
      "smPolicyDecision" : {
        "pccRules" : {
          "0_2" : null
        },
        "qosDecs" : {
          "qosdata_1" : null
        },
        "traffContDecs" : {
          "tcdata_0" : null
        }
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
      }
    }
  },
  "httpResponse" : {
    "statusCode" : 204
  },
  "id" : "smfRequest",
  "priority" : 1,
  "timeToLive" : {
    "unlimited" : true
  },
  "times" : {
    "unlimited" : true
  }
} ]
13:13:12.522 [main] INFO  c.intuit.karate.core.FeatureRuntime -
classpath:ocpm/contract/test/core/contract.feature - call by tag at line
3563: name=deleteAppSession
13:13:12.525 [main] DEBUG com.intuit.karate - request:
1 > POST http://localhost:8080/npcf-policyauthorization/v1/app-sessions/
6f3f0561-3365-4516-886b-831833b6ac74/delete
1 > Content-Type: application/json; charset=UTF-8
1 > Content-Length: 102
1 > Host: localhost:8080
1 > Connection: Keep-Alive
1 > User-Agent: Apache-HttpClient/4.5.13 (Java/17.0.12)
1 > Accept-Encoding: gzip,deflate
{"events":null,"notifUri":"http:\/\/localhost:1080\/
smservicenotify\/","usgThres":null,"reqAnis":null}

13:13:12.580 [main] DEBUG com.intuit.karate - response time in milliseconds:
54
1 < 204
1 < Date: Mon, 05 May 2025 19:13:12 GMT

13:13:12.581 [main] INFO  contract.test.util.common.JavaUtil - Delay: 3sec
13:13:15.612 [main] INFO  contract.test.util.common.HttpUtils - VerifyMetric
occnp_http_out_conn_response_total with params
operationType="update_notify",responseCode="204": 1.0 - 0.0 == 1.0
13:13:15.613 [main] INFO  contract.test.util.common.HttpUtils - VerifyMetric
ocpm_egress_request_total with params operation_type="update_notify": 2.0 -
1.0 == 1.0
13:13:15.613 [main] DEBUG c.intuit.karate.core.ScenarioEngine - over-writing
existing variable 'SmSession' with new value:
JSON.parse(util.db.readValue("select v from SmPolicyAssociation where k='" +
smPolicyId + "'"))
13:13:15.632 [main] INFO  com.intuit.karate - [print] {
  "sessRules": {
    "0_1": {
      "authSessAmbr": {
        "uplink": "500.0 Kbps",
        "downlink": "1.0 Mbps"
      },
      "authDefQos": {
        "5qi": 5,
        "arp": {
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
            "priorityLevel": 1,
            "preemptCap": "NOT_PREEMPT",
            "preemptVuln": "NOT_PREEMPTABLE"
          },
          "priorityLevel": 2
        },
        "sessRuleId": "0_1"
      }
    },
    "pccRules": {
      "0_0": {
        "flowInfos": [
          {
            "flowDescription": "permit in ip from any to any",
            "flowDirection": "UPLINK"
          },
          {
            "flowDescription": "permit out ip from any to any",
            "flowDirection": "DOWNLINK"
          }
        ],
        "pccRuleId": "0_0",
        "precedence": 3000,
        "refQosData": [
          "qosdata_0"
        ],
        "pendingConfirmationAction": 0
      }
    },
    "qosDecs": {
      "qosdata_0": {
        "5qi": 5,
        "qosId": "qosdata_0",
        "arp": {
          "priorityLevel": 1,
          "preemptCap": "NOT_PREEMPT",
          "preemptVuln": "NOT_PREEMPTABLE"
        },
        "priorityLevel": 2
      }
    },
    "chgDecs": {
    },
    "traffContDecs": {
    },
    "conds": {
    },
    "policyCtrlReqTriggers": [
      "PLMN_CH",
      "UE_IP_CH",
      "DEF_QOS_CH",
      "AC_TY_CH"
    ]
  }
```


SMPolicyAssociation after STR:

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.29 Supports Reattempt after Back-off during N1N2 Communication

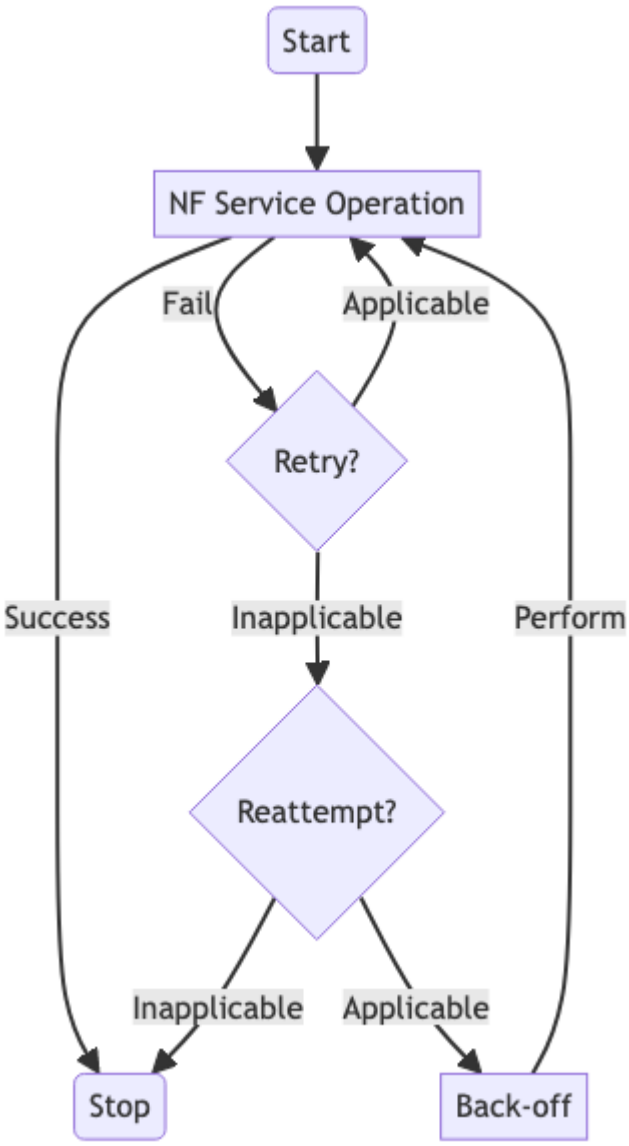
The **UE Policy Association** procedure involves the AMF establishing a relationship with the PCF to deliver UE specific policies. PCF evaluates the relevant policies to determine the URSP rules that need to be sent to the UE. Before sending the URSP rules, PCF subscribes to the AMF by invoking N1N2Communication request. This step ensures that PCF can communicate with the appropriate AMF. To find the correct AMF, PCF uses the Nnrf_NFdiscovery service, which identifies the available AMF instances in the network. Following the successful AMF discovery and subscription, PCF sends the URSP rules to the UE through the N1N2MessageTransfer request. If any part of the procedure, such as the AMF discovery, subscription process or URSP transfer fails, then the overall URSP transfer will not be successful. This shows the importance of each of these procedures, as they are integral to successful N1N2Communication.

PCF supports multiple N1N2 Communication attempts that would help in successful delivery of URSP rules to UE. Since this procedure also has AMF Discovery, N1N2Subscription, and N1N2Transfer requests the reattempt is applied to them too.

The following flowchart illustrates the sequence of retry and reattempt mechanism as applied to a NF service operation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-82 Reattempt Flow Chart



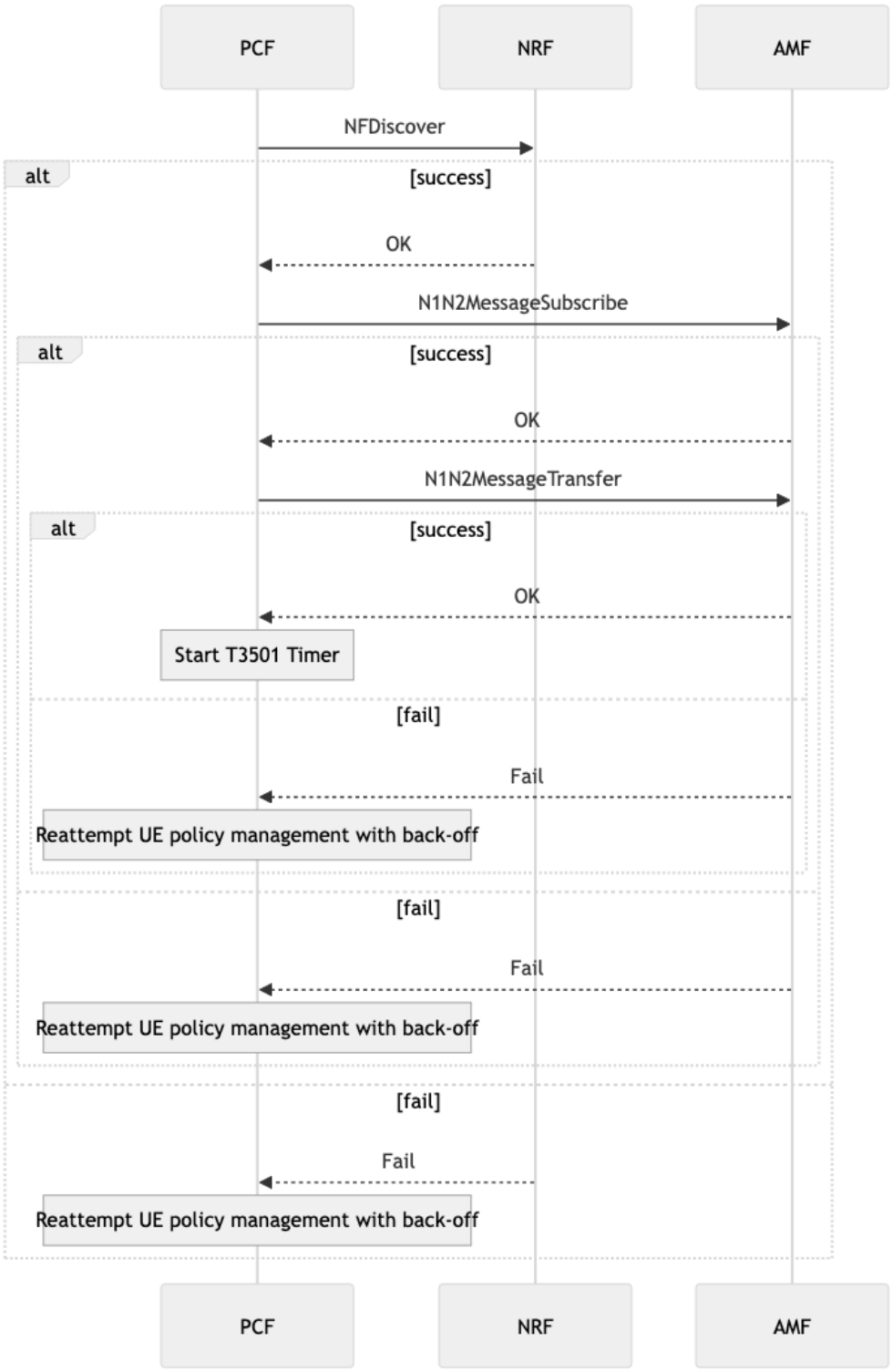
On external trigger, a UE Policy management procedure is initiated and a procedure is attempted, and if that procedure fails retry mechanism kicks in. If the retry is applicable the failed procedure is retried. If this still fails and all the retries are exhausted, then reattempt is considered. So if the reattempt is applicable according to the reattempt profile, UE service will schedule a timer with audit service.

The PCF starts a back-off timer. The length of this timer exponentially increases based on the number of failed attempts. After the timer elapses, the PCF attempts to re-send the request. If successful, the process ends. If it fails again, the back-off timer is reset, and the retries continue until a maximum number of attempts is reached.

UE service uses reattempt mechanism on `NFDiscover`, `N1N2MessageSubscribe`, and `N1N2MessageTransfer` in UE policy management procedure. The following call flow illustrates the reattempt of UE policy management with back-off feature getting triggered during N1N2 message failures.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-83 Reattempt and backoff Call flow



- PCF sends `NFDiscover` request to NRF.
- On success the procedure continues. On failure, PCF reattempts the UE policy management with back-off.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- PCF sends `N1N2MessageSubscribe` request to AMF.
- On success the procedure continues. On failure, PCF reattempts the UE policy management with back-off.
- PCF sends `N1N2MessageTransfer` request to AMF.
- On success the procedure continues. On failure, PCF reattempts the UE policy management with back-off.

Reattempts for NFDiscover, N1N2MessageSubscribe and N1N2MessageTransfer

Back-off is a rate limiting strategy that allows for dynamic rate limits, where the delay increases with each retry. When a request is rejected due to the rate limit, the back-off timer waits before attempting to retry the request.

The PCF uses a configured backoff timer with an added randomization value in the order of milliseconds. The max randomization millisecond value is specified in configuration. This helps to resolve the "thundering herd" problem, which occurs when many clients attempt to reconnect at same time. The PCF throttles all reattempts after the configured threshold limit level, this typically involves rate limiting which sets a maximum number attempts allowed within a specific time frame. The configured threshold limit applies globally, restricting the total number of requests across PCF rather than just applying on individual services like UE. Hence, in reattempt profile, the threshold limit level is confined to max 360K for each NF Service Operation.

The Reattempt are configurable for AMF and NRF interfaces and is defined using existing Reattempt profile. The existing Reattempts Profile is enhanced to create reattempt profiles to AMF interface for `N1N2 Subscribe`, `N1N2 Transfer`, `N1N2 Failure Notification` operations. The reattempt profile can also be created to NRF interface for `AMF Discovery` operation. For each NF operations, user can configure maximum number of retry attempts and backoff timer for each retry. Retrying can also be enabled for internal failures, such as timeout exceptions or no response from the AMF, and just not for the service timeouts.

An Internal Failure indicates that the UE service was unable to complete the N1/N2 transfer operation due to a failure in request preparation, communication with AMF, AMF error handling, or response processing.

Common causes include:

- AMF is unreachable, unavailable, or does not return a usable response.
- The request fails due to network, DNS, TLS, socket, timeout, or HTTP client issues.
- AMF returns an error response and the UE service cannot recover through retry or alternate routing.
- The response from AMF is malformed (including unsupported or invalid HTTP Error Codes such as 419, 427, and so on), unreadable, incomplete, or cannot be converted into the expected N1/N2 transfer response format.
- The UE service encounters an internal error while building the request, adding headers, preparing the payload, logging metrics, or sending the request.

> **Note**
>
> In reattempt profile threshold limit level is confined to max 360K combined for all NF operations.

The reattempt profile can be configured to retry for specific error codes and its causes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following fields are added or modified in Reattempts Profile in CNC Console that allows you to create new, and manage existing reattempt profiles for AMF and NRF interfaces and this get listed in the **NF Communication Profiles** page in CNC Console.

Table 4-48 Reattempts Profile

Field Name	Value
Interface Type	This field is modified to support **AMF** and **NRF** interface types.
Re-attempt Settings: Maximum Number of Attempts	This field is modified to configure maximum number of reattempts that are allowed for AMF or NRF service operation.
Re-attempt Settings: Back-off timer configurations	This field is added to provide specific configurations for back-off timer such as **Index**, **Back-Off Timer (Seconds)**, and **Max Random Number (Millisecond)**.
Re-attempt Settings: Threshold Limit Level	This field is modified to configure the threshold limit for timers that can be backed off for reattempt in case of either AMF or NRF operations. **Note** The threshold limit level is confined to max 360K combined for all NF operations.
Re-attempt Error Code Settings: Enable Reattempt On Internal Failure	This field is added to determines whether to perform reattempt in occurrence of internal failures for either AMF or NRF operations.
Re-attempt Error Code Settings: Re-attempt for Following Error Codes	This field is added to configure the list of combination of HTTP **Error Code** and **Error Cause** for reattempt after back off.
Rate Limiting Settings: Rate Limit (per second)	This field is added to configure the rate limit threshold per second for NF service operation(s).

Note

The **Rate Limit (per second)** field can be set to numerical value ranging from 0 - 700. But it is recommended to keep this value above or equal to 100 requests per second. The timer expiry notification rate should be more than the allowed timer creation time so as to prevent the creation of backlogs which will cause a delay in timer expiry notification reaching the UE service.

The NF Communication profile **Re-attempt Settings** section allows to enable the reattempts and select from the created reattempt profiles for specific NF operations. The following fields are added to support reattempts for AMF and NRF interfaces in NF Communication Profiles page in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-49 NF Communication Profiles

Field Name	Value
Re-attempt Settings	Provide Re-attempt Settings details:
Enable NF Service Operation Re-attempt	false
NF Service Operation Profiles	NAS operations: • AMF Discovery • N1N2 Message Subscribe • N1N2 Message Transfer • N1N2 Transfer Failure Notification

The created NF communication profile comprising of reattempt profile gets listed in the PCF UE Policy Service configurations page in CNC Console.

With rate limiting mechanism the UE slows down the rate of requests toward AMF after getting a server error. If PCF receives a "Retry-After IE" from AMF, its value is compared with the configured backoff timer, and which ever is the greater, it is used to set the timer.

> **Note**
>
> The PCF does not consider "Retry-After" header from AMF or SCP or NRF.

Timer Service

The PCF Audit service is enhanced to provide Timer service providing a one-shot timer for one time use. It manages the life cycle of a scheduled timer. The consuming service has to schedule a new timer once the timer is notifier or canceled. Timer service uses a pre-defined database table for managing the timers as defined by the audit service.

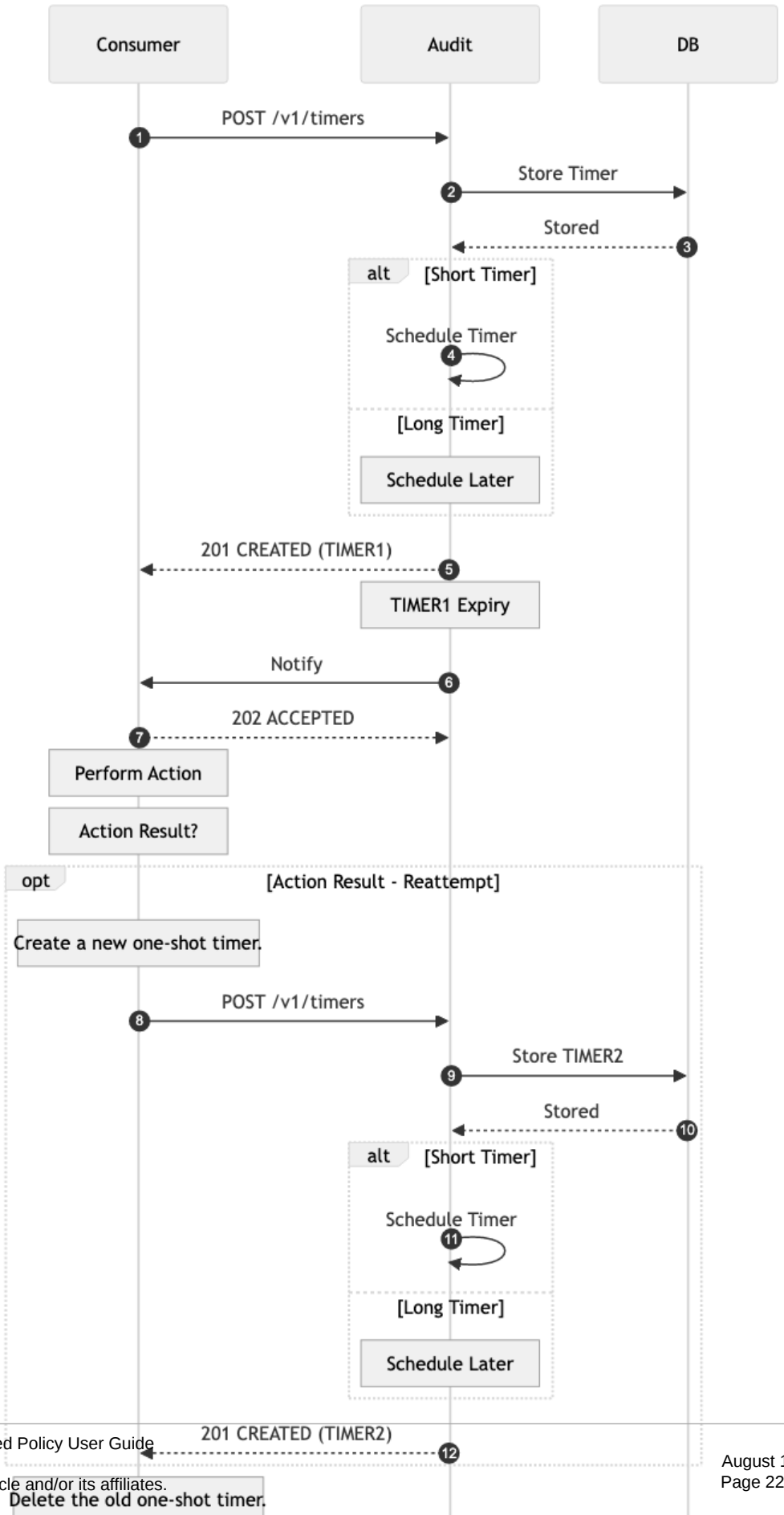
Timer service provides scheduling of Short timer and Long timer. Short timer are timers that expires within five minutes of their creation. The five minutes being default value and configurable. Any timer which is not a Short timer is a Long timer. The Short timers are scheduled at the creation timer, whereas the Long timer are scheduled during the scan time when they are close to expiring.

By default, the timer service is disabled. The timer service can be enabled or disabled at Timer Service page in CNC Console.

The below diagram provides an overview of the Timer service:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-84 Timer Service Overview



Copyright © 2019, 2026, Oracle and/or its affiliates.

Rate Limiting: The notification requests sent on timer expiry are rate limited. To perform rate limiting of timer notification, the rate limiting configuration is split across pods. For example, if there are 2 pods and rate limit is set to 1000 requests per second, then each pod performs rate limiting of 500 requests per second. This ensures that the rate limit state is shared across pods during runtime.

> **Note**
>
> It is assumed that the consumer has load balanced the timer requests across Audit pods.

The Timer service uses the `REPLICA_COUNT` environment variable to determine the number of timer pods deployed. This value is mapped to the `minReplicas` key in the `values.yaml` file of the audit Helm chart. Although the audit service is deployed with a Kubernetes HorizontalPodAutoscaler (HPA), please note that dynamic scaling based on CPU load is not supported by the audit/timer services.

> **Note**
>
> It is recommended not to scale the audit pods using the `kubectl` scale command to increase the number of pods, instead modify the `minReplicas` value in the `values.yaml` file and perform a Helm upgrade.

Rate Limiting the Timer Creation API: The `Timer Creation` API in the Audit service is rate limited using the token bucket algorithm. The default limit is 25 requests per pod to prevent traffic storms. For example, if there are 2 audit pods and requests are load balanced equally across the audit pods, the service can support 50 create timer requests.

> **Note**
>
> Rate limiting is not guaranteed request rate; existing limitations from the token bucket algorithm still apply. Temporary spikes of 30-50% above 50 requests are acceptable, as the audit service can handle these bursts.

The timer `occnp_timer_capacity` metrics and capacity alerts are determined by the total number of timers created on the site and will not consider the fostered timers from pods of other sites as the logic for denying timer creation is based only on total timers created on the site, without regard for fostered timers.

The timer capacity alerts may deviate by 30 seconds, as the gauge metric is updated each time the timer scan run at default interval of 30 seconds.

Timer Count Synchronization Activity

The Timer Service API utilizes the 'timer_count' column in the Timer Registration record to monitor the number of active timers for a specific timer name. This mechanism allows the Timer API to determine whether to accept or reject timer creation requests based on the configured timer capacity threshold.

Upon successful timer creation, the Timer Service increments the 'timer_count' in the Timer Registration record. Conversely, after a timer deletion, the service decrements the count. However, database-related issues may lead to discrepancies between the actual number of

Copyright © 2019, 2026, Oracle and/or its affiliates.

timers and the value in the registration record, potentially causing incorrect acceptance or rejection of timer creation requests.

To address this, a new activity introduced in release 25.2.100 synchronizes the 'timer_count' field in each Timer Registration record with the actual count of timers in the Timer table for a given timer name and site. If a discrepancy is detected, the registration record is updated with the correct count. Given the database-intensive nature of this activity, it is designed to run infrequently, with a default execution interval of every 12 hours

Bulwark Concurrency

Bulwark needs to be enabled for the UE operations namely, UE create, update, UDR or CHF notification, T3501 Timer Expiry, N1Notify, and Timer Expiry Notification. The following table provides details about the newly added Bulwark configurations for Timer notifications.

Table 4-50 Newly added Advanced Settings for Bulwark Configurations for Timer

Key	Value	Description
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_COUNT	2	The number of retries when the lock acquisition fails from Bulwark due to lock request failing.
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_BACKOFF	1000	This is the duration for which UE service will wait once it receives ALREADY_LOCKED response from Bulwark.
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_LEASE_DURATION	2000	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically.
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_WAIT_DURATION	3000	The duration by which the UE service waits for the response to get a lock.
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.ENABLED	false	If Bulwark lock is enabled for processing Reattempt timer expiry Notification.

Table 4-51 AMF Discovery and Subscription

Key	Value	Description
AMF.OPTIMIZED.DISCOVERY.AND.SUBS.ENABLED	true	True: Discovery and subscription to AMF occur only when an N1MessageTransfer is required False: In-Advance AMF Discovery and Subscription are performed, N1Message Transfer may or may not be initiated, depending on the UE policy action

Support for GeoRedundency

A Policy Site is single deployment (NF instance) of Policy solution. Policy mated region refers to collection of two or more Policy Sites that share the same data. The Mated region is equivalent to an NF Set.

Copyright © 2019, 2026, Oracle and/or its affiliates.

In a georedundant deployment, a mated region allows a service to be provided by any instance within the region, and providing access to the same context data. You can create mated region by configuring the Policy Mated Region page in under General Configurations in CNC Console.

An alternate site (NF Instance) from the Policy mated region can be configured for UE Policy Management Procedures. This common site takeover data is monitored and used by Audit service to check for remote orphan and perform site takeover. The site take over configurations can be performed at Site Fallback page under General Configurations in CNC Console.

Scanning `timer_service` database

The Audit service scans the `timer_service` database to schedule timers, which are about to expire and to handle abnormal behavior of pod restarts and stale or stuck timers. Scans are performed at NF-level activities followed by pod-level activities. By default, the scans are run every 30 seconds.

The following pod-level activities are performed by each pod during the scan:

- Checking for stale and stuck state of timers created or adopted.
- Scheduling timers which are about to expire, that includes:
  - Scheduling of adopted timers
  - Scheduling of long timers

The following NF-level activities are performed by a single pod at a site or NF:

- Orphan timers adoption at local site to check for the dead pods at the local site. The frequency to run the orphan local scan activity can be configured using `TIMER_SCAN_ORPHAN_LOCAL_ACTIVITY_FREQUENCY` Advanced Settings key. By default, `TIMER_SCAN_ORPHAN_LOCAL_ACTIVITY_FREQUENCY` is set to 2 cycles.
- Orphan timers adoption at alternate site to check for the dead pods at the alternate site and adopt them if necessary. The frequency to run the orphan remote scan activity can be configured using `TIMER_SCAN_ORPHAN_REMOTE_ACTIVITY_FREQUENCY` Advanced Settings key. By default, `TIMER_SCAN_ORPHAN_REMOTE_ACTIVITY_FREQUENCY` is set to 4 cycles.

For more details on `TIMER_SCAN_ORPHAN_LOCAL_ACTIVITY_FREQUENCY` and `TIMER_SCAN_ORPHAN_REMOTE_ACTIVITY_FREQUENCY` Advanced Settings keys, see Timer Service.

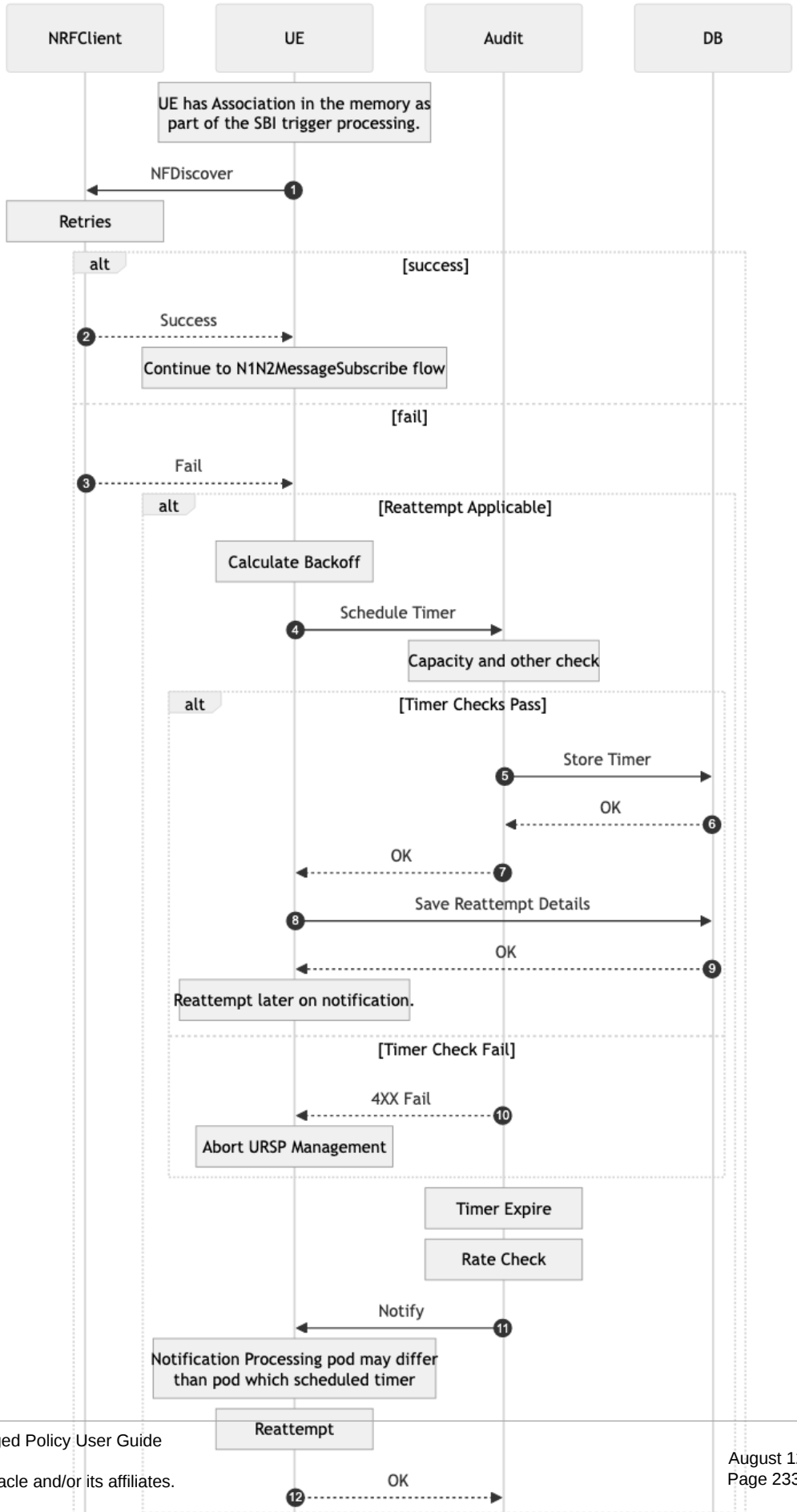
Call Flows

Reattempt NFDiscover Call Flow

The following figure illustrates the PCF UE Service call flow, handling the reattempts on a NFDiscover failure.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-85 NFDiscover Call Flow



Copyright © 2019, 2026, Oracle and/or its affiliates.

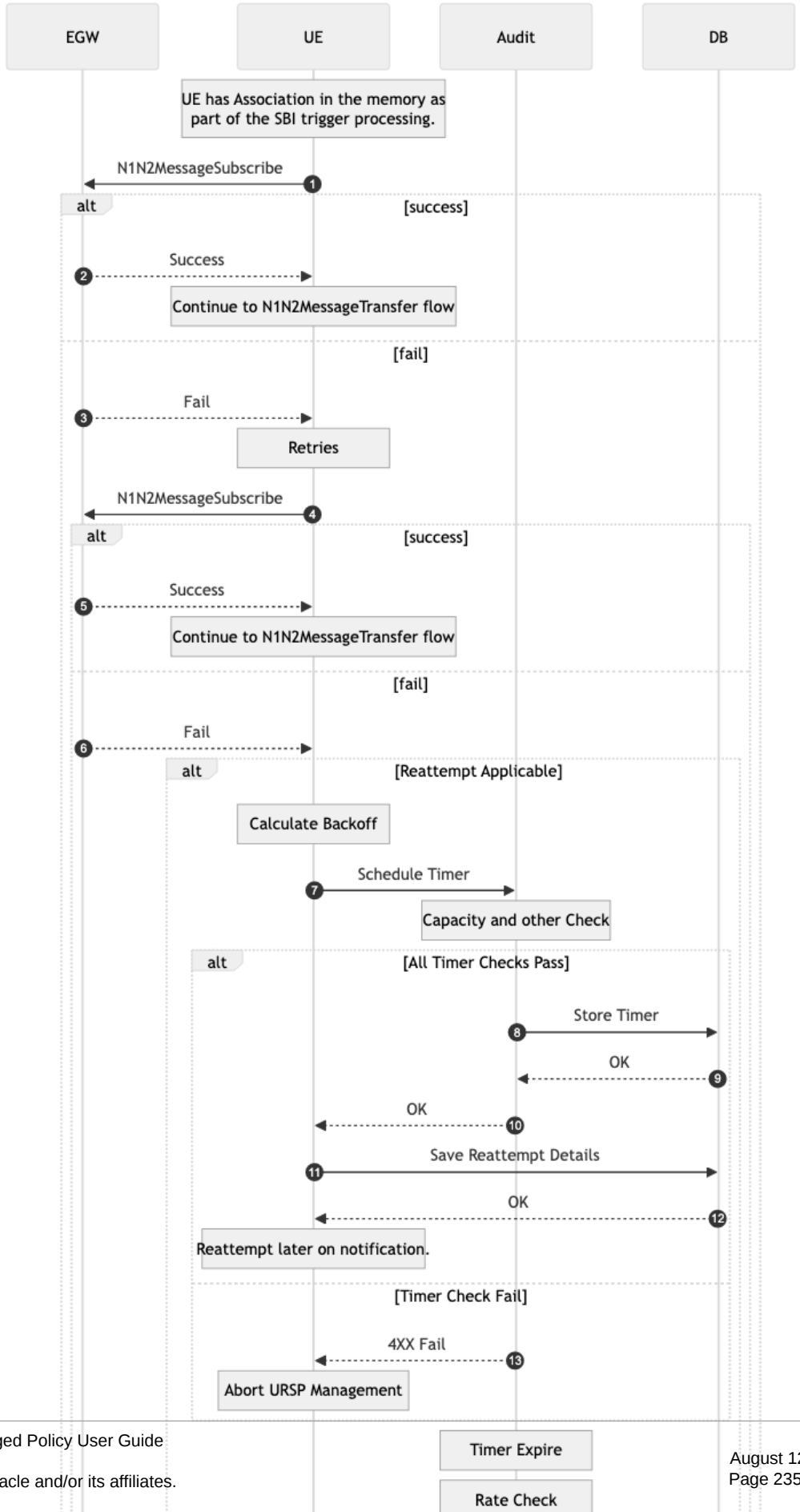
1. UE service initiates a `NFDiscover` request toward NRF Client.
2. On success from NRF Client, the UE Policy management procedure for `N1N2MessageSubscribe` continues with the next step.
3. On failure from NRF Client, PCF checks for reattempt applicability.
4. If the reattempt is applicable, then calculates the backoff based on the configured reattempt profile and schedules timer.
5. On Timer check passes for the capacity and other parameters, the timer information is stored in the database.
6. The database returns success 'OK'.
7. The scheduled timer success 'OK' is sent by Audit service to UE.
8. The reattempts details are stored in the database.
9. The database returns success 'OK'.
10. Alternate to Step 5. Failed check shall return failure to UE micro service which should abort the procedure.
11. Timer expiry shall notify the UE micro service after performing a rate limit check.
12. UE micro service performs a reattempt and returns OK.
13. Alternate to Step 4. Reattempt is not applicable and UE Policy Management Procedure shall be aborted.

N1N2MessageSubscribe Call Flow

The following figure illustrates the PCF UE Service call flow, handling the reattempts on a N1N2MessageSubscribe failure.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-86 N1N2MessageSubscribe Call Flow



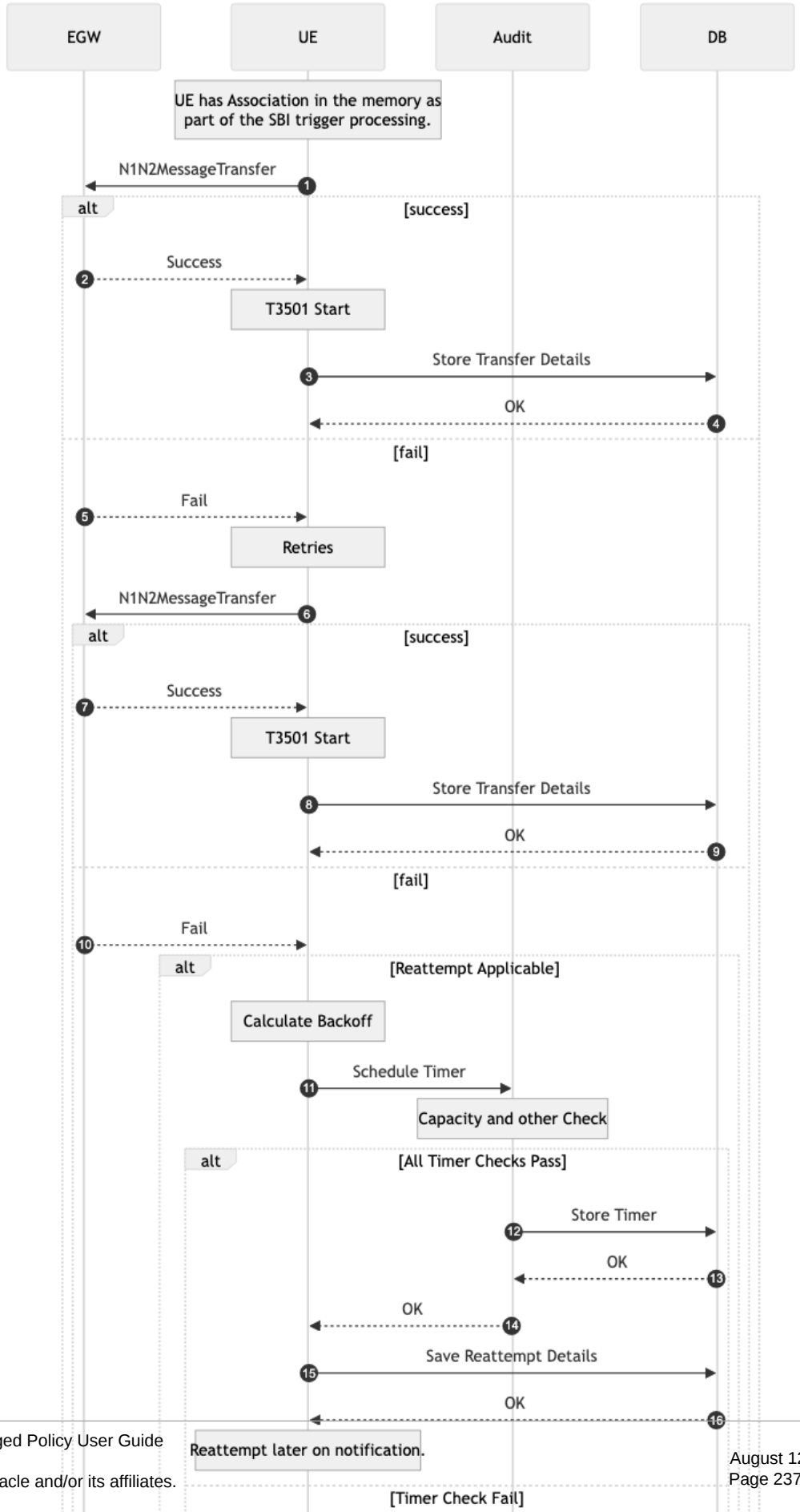
Copyright © 2019, 2026, Oracle and/or its affiliates.

N1N2MessageTransfer Call Flow

The following figure illustrates the PCF UE Service call flow, handling the reattempts on a N1N2MessageTransfer failure.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-87 N1N2MessageTransfer Call Flow



Copyright © 2019, 2026, Oracle and/or its affiliates.

Manage Support for Backoff during N1N2Communication in UE

Feature Assumptions and Limitations

- For this feature to work as expected , we need to provision the respective Bulwark configuration for Timer service.
- Maximum capacity threshold for reattempt per site is 360K. Default is 180K.
- Maximum rate for the re-attempt is assumed to be 700 per second.
- Maximum rate of re-attempt timer scheduling is assumed to be 25 per second.
- During rate limiting, the NF Service Operation is not throttled. The UE Policy Management Procedure is to be executed later i.e. not aborted.
- Bulwark needs to be enabled for the feature as reattempt increases the chances of collisions for procedures related to the same UE.
- Reattempts are calculated per UE unless stated otherwise.
  - This means that same NF Service Producer can be retried as part of back-off for a different UE other than that for which the back-off timer is in progress.
- For `ProblemDetails` processing, final `ProblemDetails` returned is considered.
  - E.g. If both AMF1 and AMF2 returned `ProblemDetails` and AMF2 returned the last response, `ProblemDetails` from AMF2 shall be considered for back-off calculation.
- Rate limit is specific to reattempts and not to the initial requests for `NFDiscover`, `N1N2MessageSubscribe`, `N1N2MessageTransfer` service operations.
- Rate limits are global i.e. all the `NFDiscover` irrespective of the target NRF are considered, all `N1N2MessageSubscribe` irrespective of target AMF are considered.
- The retryAfter IE shall be used from last response received if multiple AMFs are tried and both return the retryAfter IE.
- Capacity threshold defining the number of NF Service Operation to be queued for reattempt with back off are assumed to be local to a site i.e. if capacity threshold is set to 200K in the reattempt profile, it means that 100K of pending NF Service Operation for this site. If the network has three sites, there can be 3 x 200 K pending NF Service Operation for the network.
- Whenever we receive the `Retry-AfterIE` from AMF, we compare its value with the `backOffTimer` and use the greater of the two to set the timer. However, the requirement for PCF to honor the `Retry-AfterIE` by delaying the `Discovery/N1N2Subscribe/N1N2Transfer` request to AMF with updated URSP Rules/UPSIs until the timer expires is currently out of scope and not implemented at this stage.

Enable

By default, this feature is disabled. User can enable it either using either CNC Console or REST API.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> As a pre-requisite to enable *Supports Reattempt after Back-off during N1N2 Communication* feature, configure the value of `timerServiceEnable` Helm parameter to `true` during Policy installation or while upgrading Policy to a later version. For more information on configuring `timerServiceEnable` Helm parameter, see *Enabling/ Disabling Services Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Configure Using CNC Console

To enable this feature, set `Enable NF Service Operation Re-attempt` flag to `true` in NF Communication Profiles page in CNC Console. Create reattempt profiles for either AMF or NRF operations, see Reattempts Profile page in CNC Console.

Configure Using REST API

To enable this feature, use `Policy NF Communication Profiles APIs` configured for `reattemptSettings` request body parameter.

For more information, see "NF Communication Profiles" and "Recreate Attempts" API sections in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide* .

Observability

Metrics

The following changes are made to UE Service Metrics section:

- Following dimensions were added to `occnp_http_out_conn_request_total` and `occnp_http_out_conn_request_total` metrics:
  - `isReattempt`
  - `isRetryAttempt`
  - `reattemptType`
- The `reattempt_timer_expiry_notification` dimension is added to `ue_n1_policy_consolidation` metric.
- The `isReattempt` dimension is added to `ue_n1_policy_sequencing` metric.
- Following new metrics are added:
  - `occnp_ue_timer_registration_total`
  - `occnp_ue_timer_create_success_total`
  - `occnp_ue_timer_create_failure_total`
  - `occnp_ue_timer_delete_success_total`
  - `occnp_ue_timer_delete_failure_total`
  - `occnp_ue_nf_discovery_reattempt_request_total`
  - `occnp_ue_nf_discovery_reattempt_response_total`
  - `ue_n1_policy_backed_off_collation_total`

For more information about the dimensions, see CNC Policy Metrics section.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Following Audit Service Metrics are used to provide audit information for Timer service:

- occnp_timer_count_total
- occnp_timer_capacity
- occnp_timer_scan_total
- occnp_timer_registration_total
- occnp_timer_create_failure_total
- occnp_timer_notify_retry_total
- occnp_timer_state

Alerts

The following alerts are generated for this feature:

- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD
- AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD
- UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
- UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
- UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
- UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
- UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Copyright © 2019, 2026, Oracle and/or its affiliates.

- UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
- UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
- UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
- UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

4.30 Pod Congestion Control in Policy Services

The Pod Congestion Control feature in Policy application is a crucial mechanism to ensure consistent service availability and performance, especially in scenarios with high traffic and resource utilization. It is designed to identify congestion conditions and apply load shedding rules to maintain optimal service levels. The following Policy services implements the Pod Congestion Control mechanism:

- AM Service Pod Congestion Control
- Notifier Service Pod Congestion Control
- User Service Pod Congestion Control
- Diameter Connector Pod Congestion Control
- UE Service Pod Congestion Control
- SM Service Pod Congestion Control
- PDS Pod Congestion Control
- Usage Monitoring Pod Congestion Control
- PCRF Core Pod Congestion Control
- Binding Service Pod Congestion Control
- Bulwark Pod Congestion Control
- Diameter Pod Congestion Control

4.30.1 AM Service Pod Congestion Control

The Access and Mobility Management (AM) service, a key component in Policy services is responsible for managing user equipment (UE) registration, authentication, and mobility across the network. At times, an excessive traffic from consumer services toward AM service can be observed in the network, which can result in a high CPU utilization, high memory utilization. The AM service gets congested and can cause performance degradation in its service response time and eventually reach a state of service unavailability. To handle this, the AM service implements congestion control mechanism. and ensures that its service is protected from congestion and, also its service is consistently available to the consumer services.

The Pod Congestion Control feature in AM service is a crucial mechanism to ensure consistent service availability and performance, especially in scenarios with high traffic and resource utilization. It is designed to identify congestion conditions and apply load shedding rules to maintain optimal service levels.

The AM service receives every incoming requests, the congestion control mechanism decides to either accept or reject the request based on pods congestion state defined request priority. It

Copyright © 2019, 2026, Oracle and/or its affiliates.

invokes the load shedding rules when congestion state persist in the AM pods. The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In congestion control mechanism different congestion levels are defined, each level indicates how congested the pod is, and which requests can be served when pod is on certain congestion level. The congestion control works at following five congestion levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

Each AM service pod monitors its congestion state. The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, cpuacct.usage, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This REST API parameter can be configured to specify after how many continuous intervals, the pod state can be changed. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This REST API parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. This interval is configured in milliseconds and can range from 50 to 2147483647.

For more information about these congestion control configurations, see Congestion Control Settings section in CNC Console.

The pod's state changes when its resources, namely the CPU and Queue buffer usage exceeds the predefined congestion threshold, checked at regular intervals. An active CPU and Queue default threshold profile can be viewed using CNC Console at *Policy → Overload and Congestion Control → Congestion Control → Thresholds* section. The user can create new threshold profile and make it active. The AM service pod's different congestion states and their default congestion parameters, CPU, and Queue pending counts are provided in the following table:

Table 4-52 AM Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC	75	688

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-52 (Cont.) AM Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
CONGESTION_L1	80	1032
CONGESTION_L2	85	1376
CONGESTED	90	1720

For more information about these CPU and Queue count thresholds configurations, see Congestion Control Thresholds section in CNC Console.

Triggering Pod Congestion Control

With Congestion Control feature enabled for AM service, every time a message is fetched for processing, the system checks the current congestion state of the pod. If the current state is either in `DOC`, `CONGESTION_L1`, `CONGESTION_L2`, or `Congested` state, then the congestion control mechanism is triggered. After verifying that the message type is a request, a request priority is assigned to it. If the request priority is greater than or equal to the discard priority, then the message is rejected, otherwise it is accepted.

Congestion Control Load Shedding using Discard and Request Priority

The AM service pods performs load shedding by considering the load rule configured for the current congestion state. The load shedding rule is based on message priority configuration. A default load shedding rule is active and the messages are discarded based on it. You can configure these load rules using the Overload and Congestion Control menu in CNC Console. The priority value ranges between 0 to 31, with 0 being the highest, and 31 being the lowest priority. The default discard priority for load shedding rules used in AM service:

Table 4-53 AM Service Default Discard Priorities:

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	28
CONGESTION_L1	25
CONGESTION_L2	20
CONGESTED	17

For more information about discard priority configurations, see Congestion Control Load Shedding Rules section in CNC Console.

Computing the Congestion Control Resource Usage

The Exponential Moving Average (EMA) algorithm calculates the congestion resource usage by considering the resource consumption data over time, giving more weight to recent usage data, which provides a more accurate picture of current resource utilization compared to a simple average across all data points. This resource usage data is used for pod state change thus enabling smooth transition of congestion states during traffic spikes. For AM pod to use EMA algorithm for computing its CPU and Queue resources, add the following advanced key value while editing the Congestion Control Settings for AM service in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-54 Congestion Control EMA Configurations for AM Service

Key	Value	Description
CPU_CONGESTION_RESOURCE_CALC_ALGORITHM	EMA	This enables the congestion control CPU resource calculation to use the algorithm configured.
CPU_CONGESTION_RESOURCE_CALC_INTERVAL_MS	50	This configuration sets the time interval in milliseconds for CPU congestion resource to be calculated by the configured algorithm.
QUEUE_CONGESTION_RESOURCE_CALC_ALGORITHM	EMA	This enables the congestion control Queue resource calculation to use the algorithm provided.
QUEUE_CONGESTION_RESOURCE_CALC_INTERVAL_MS	50	This configuration sets the time interval in milliseconds for Queue congestion resource to be calculated by the configured algorithm.
EMA_CPU_CONGESTION_RESOURCE_CALC_RATIO	70:30	This configuration will be used to set the EMA ratio in which congestion CPU resource(s) calculated using EMA algorithm to be considered for calculation.
EMA_QUEUE_CONGESTION_RESOURCE_CALC_RATIO	70:30	This configuration will be used to set the EMA ratio in which congestion Queue resource(s) calculated using EMA algorithm to be considered for calculation.

For more information about the EMA algorithm, see Congestion Control Resource Usage Calculation Using EMA Algorithm feature.

You can configure the message priority for different rest endpoints for AM Service using using CNC Console at *Policy → Service Configurations → PCF Access and Mobility → Advanced Settings* section. The message priority value ranges between 0 to 31, with 0 being the highest, and 31 being the lowest priority. If an invalid value is provided, then the default priority shall be considered. You can add the following keys to configure the message priority for different rest endpoints at AM service:

Table 4-55 AM Service Request Default Priorities

Advanced Settings Key	Default Priority
AM_GET_SUBSCRIBER_SESSIONS_REQUEST_PRIORITY	28
AM_CREATE_REQUEST_PRIORITY	24
AM_UPDATE_REQUEST_PRIORITY	18
AM_NOTIFICATION_REQUEST_PRIORITY	18
AM_UPDATE_PDSLOCATIONINFO_REQUEST_PRIORITY	18
AM_DELETE_REQUEST_PRIORITY	16
AM_AUDIT_NOTIFY_REQUEST_PRIORITY	30

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following points needs to be known while assigning request or message priority to an request API:

- For requests coming from Diameter Gateway, the requests priority number is retrieved from *oc-message-priority* parameter in the http request header. But if this request header parameter is not present or its value is not set, then the message priority shall be based on the configured values from Advanced Settings or Default priority values.
- For requests coming from Ingress Gateway, the priority is based on *3gpp-sbi-message-priority* parameter in http request header. But if this request header parameter is not present or its value is not set, then the priority shall be based on configured values from Advanced Settings or on the default priority values.
- The request priority value ranges between 0 to 31, with 0 being the highest, and 31 being the lowest priority. If an invalid value is provided, then the default priority shall be considered.

Thus the precedence order for assigning message priority shall be from `oc-message-priority → 3gpp-sbi-message-priority → Advanced Settings Priority → Default Priority`.

When AM service is in congestion state, its response can be configured using PCF Access and Mobility service advanced settings in CNC Console, using the key `CONGESTION_RESPONSE_CODE`. You can configure the result codes for the rejected requests when configuring the load rules. The response code configured should be either `1xx`, or `3xx`, or `4xx`, or `5xx` status code. By default, AM service sends 503 as response code with error cause as '**NF_CONGESTION**'.

In the response body, an error header is sent to the consumer service, providing the congestion error details as understood by the error-handler framework. A sample JSON error response:

```
{
    "status": 503
    "cause" : "NF_CONGESTION",
    "detail" : "Pod <pod-name> is in CONGESTION_L1"
}
```

Managing AM service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for AM service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations** for AM Service.

To configure AM service pod congestion control feature in CNC Console, see Congestion Control section.

To configure AM service pod congestion control discard messages in CNC Console, see the Advanced Settings section in PCF Access and Mobility.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observability

Metrics:

The following common service metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_congestion_http_pending_request_active_counter`
- `occnp_http_congestion_message_reject_total`

For information about the metrics, see Pod Congestion Metrics section.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

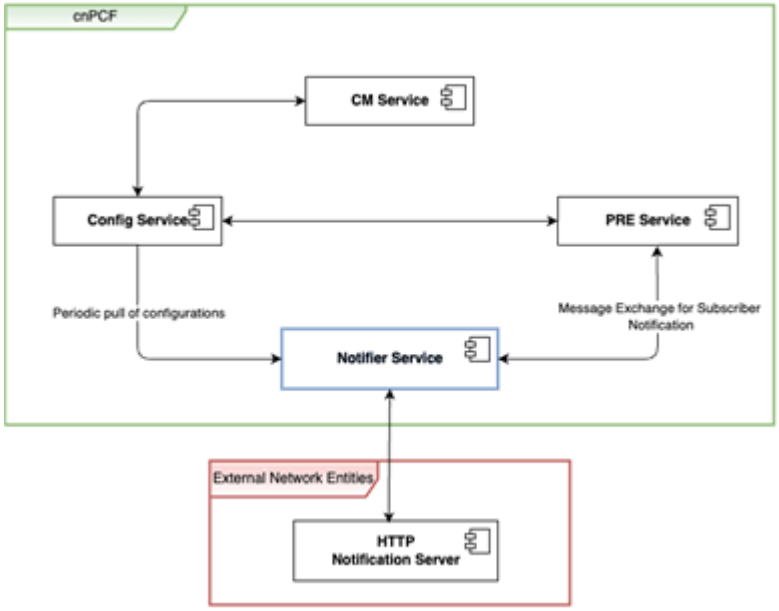
For more information about alerts, see Common Alerts.

4.30.2 Notifier Service Pod Congestion Control

The Notifier service is provided by the Policy Control Function (PCF). It is a notification framework used to send notifications such as events or messages to external notification servers such as HTTP server, SMS Gateway, Short Message Service Center (SMSC), and Mail Transfer Agent (MTA).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-88 Notifier Service interactions with other Services



At times, an excessive traffic from consumer services toward Notifier service can be observed in the network, which can result in a high CPU utilization, high memory utilization. The Notifier service gets congested and can cause performance degradation in its service response time and eventually reach a state of service unavailability. To handle this, the Notifier service implements congestion control mechanism. and ensures that its service is protected from congestion and, also its service is consistently available to the consumer services.

The Pod Congestion Control feature in Notifier service is a crucial mechanism to ensure consistent service availability and performance, especially in scenarios with high traffic and resource utilization. It is designed to identify congestion conditions and apply load shedding rules to maintain optimal service levels.

The Notifier service receives every incoming requests, the congestion control mechanism decides to either accept or reject the request based on pods congestion state defined request priority. It invokes the load shedding rules when congestion state persist in the Notifier pods. The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In congestion control mechanism different congestion levels are defined, each level indicates how congested the pod is, and which requests can be served when pod is on certain congestion level. The congestion control works at following five congestion levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

Copyright © 2019, 2026, Oracle and/or its affiliates.

Each Notifier service pod monitors its congestion state. The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, cpuacct.usage, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This parameter can be configured to specify after how many continuous intervals, the pod state can be changed. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. This interval is configured in milliseconds and can range from 50 to 2147483647.

For more information about these congestion control configurations, see Congestion Control Settings section in CNC Console.

The pod's state changes when its resources, namely the CPU and Queue buffer usage exceeds the predefined congestion threshold, checked at regular intervals. An active CPU and Queue default threshold profile can be viewed using CNC Console at *Policy → Overload and Congestion Control → Congestion Control → Thresholds* section. The user can create new threshold profile and make it active. The Notifier service pod's different congestion states and their default congestion parameters, CPU, and Queue pending counts are provided in the following table:

Table 4-56 Notifier Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC	77	140
CONGESTION_L1	78	160
CONGESTION_L2	79	180
CONGESTED	80	200

For more information about these CPU and Queue count thresholds configurations, see Congestion Control Thresholds section in CNC Console.

Triggering Pod Congestion Control

With Congestion Control feature enabled for Notifier service, every time a message is fetched for processing, the system checks the current congestion state of the pod. If the current state is either in `DOC`, `CONGESTION_L1`, `CONGESTION_L2`, or `Congested` state, then the congestion control mechanism is triggered. After verifying that the message type is a request, a request priority is assigned to it. If the request priority is greater than or equal to the discard priority, then the message is rejected, otherwise it is accepted.

Congestion Control Load Shedding using Discard and Request Priority

Copyright © 2019, 2026, Oracle and/or its affiliates.

The Notifier service pods performs load shedding by considering the load rule configured for the current congestion state. The load shedding rule is based on message priority configuration. A default load shedding rule is active and the messages are discarded based on it. You can configure these load rules using the Overload and Congestion Control menu in CNC Console. The priority value ranges between 0 to 31, with 0 being the highest, and 31 being the lowest priority. The default discard priority for load shedding rules used in Notifier service:

Table 4-57 Notifier Service Default Discard Priorities:

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	27
CONGESTION_L1	19
CONGESTION_L2	17
CONGESTED	15

For more information about discard priority configurations, see Congestion Control Load Shedding Rules section in CNC Console.

Computing the Congestion Control Resource Usage

The Exponential Moving Average (EMA) algorithm calculates the congestion resource usage by considering the resource consumption data over time, giving more weight to recent usage data, which provides a more accurate picture of current resource utilization compared to a simple average across all data points. This resource usage data is used for pod state change thus enabling smooth transition of congestion states during traffic spikes. For Notifier pod to use EMA algorithm for computing its CPU and Queue resources, add the following advanced key value while editing the Congestion Control Settings for Notifier service in CNC Console.

Table 4-58 Congestion Control EMA Configurations for Notifier Service

Key	Value	Description
CPU_CONGESTION_RESOURCE_CALC_ALGORITHM	EMA	This enables the congestion control CPU resource calculation to use the algorithm configured.
CPU_CONGESTION_RESOURCE_CALC_INTERVAL_MS	50	This configuration sets the time interval in milliseconds for CPU congestion resource to be calculated by the configured algorithm.
QUEUE_CONGESTION_RESOURCE_CALC_ALGORITHM	EMA	This enables the congestion control Queue resource calculation to use the algorithm provided.
QUEUE_CONGESTION_RESOURCE_CALC_INTERVAL_MS	50	This configuration sets the time interval in milliseconds for Queue congestion resource to be calculated by the configured algorithm.
EMA_CPU_CONGESTION_RESOURCE_CALC_RATIO	70:30	This configuration will be used to set the EMA ratio in which congestion CPU resource(s) calculated using EMA algorithm to be considered for calculation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-58 (Cont.) Congestion Control EMA Configurations for Notifier Service

Key	Value	Description
EMA_QUEUE_CONGESTION_RESOURCE_CALC_RATIO	70:30	This configuration will be used to set the EMA ratio in which congestion Queue resource(s) calculated using EMA algorithm to be considered for calculation.

For more information about the EMA algorithm, seeCongestion Control Resource Usage Calculation Using EMA Algorithm feature.

You can configure the message priority for different rest endpoints for Notifier Service using using CNC Console at *Policy → Service Configurations → Notifier Service → Advanced Settings* section. The message priority value ranges between 0 to 31, with 0 being the highest, and 31 being the lowest priority. If an invalid value is provided, then the default priority shall be considered. You can add the following keys to configure the message priority for different rest endpoints at Notifier service:

Table 4-59 Notifier Service Request Default Priorities

Message Type	Advanced Settings Key	Default Priority
Update Subscriber Notification	NOTIFIER.NOTIFY.PRIORITY	20

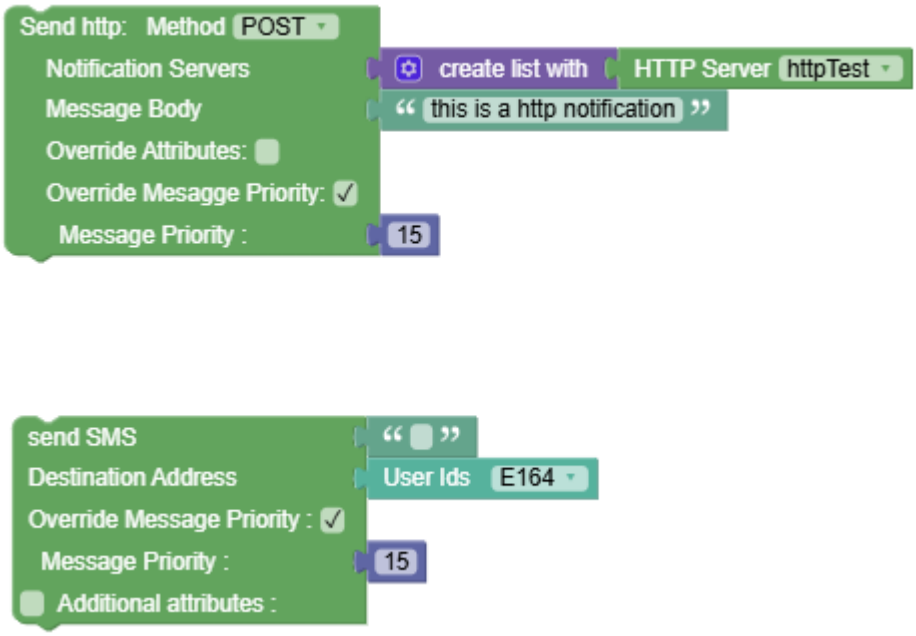
For more information about the Notifier service advanced settings, see Notifier Configurations section.

To override the message priority value received from the core service to PRE when we need to send a different value to the notifier we can use the new option of the currents blocklys. This depends on the type of notification being sent (SMPP or HTTP), as there is a constraint of having only one endpoint for both types of notifications.

The existing Blockly for HTTP and SMPP notifications now has a new option to override the `oc-message-priority` parameter. This helps in providing more control over the header value sent to the notifier for each notification request, especially when the policy uses more than one Blockly.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-89 Block to Override Message Priority



For more information about the different blocklys, see *Oracle Communications Cloud Native Core, Policy Design Guide*.

The following points needs to be known while assigning request or message priority to an request API:

- For requests coming from Diameter Gateway, the requests priority number is retrieved from *oc-message-priority* parameter in the http request header. But if this request header parameter is not present or its value is not set, then the message priority shall be based on the configured values from Advanced Settings or Default priority values.
- For requests coming from Ingress Gateway, the priority is based on *3gpp-sbi-message-priority* parameter in http request header. But if this request header parameter is not present or its value is not set, then the priority shall be based on configured values from Advanced Settings or on the default priority values.
- The request priority value ranges between 0 to 31, with 0 being the highest, and 31 being the lowest priority. If an invalid value is provided, then the default priority shall be considered.

Thus the precedence order for assigning message priority shall be from `oc-message-priority → 3gpp-sbi-message-priority → Advanced Settings Priority → Default Priority`.

When Notifier service is in congestion state, its response can be configured using Notifier service advanced settings in CNC Console, using the key CONGESTION_RESPONSE_CODE. You configure the result codes for the rejected requests when configuring the load rules. The response code configured should be **5xx** error status only. By default, Notifier service sends 503 as response code.

Managing Notifier service Pod Congestion Control

Enable

Copyright © 2019, 2026, Oracle and/or its affiliates.

By default, the Pod Congestion Control is disabled for Notifier service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations** for Notifier Service.

To configure Notifier service pod congestion control feature in CNC Console, see Congestion Control section.

To configure Notifier service pod congestion control discard messages in CNC Console, see the Advanced Settings section in Notifier Configurations.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The following common service metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_congestion_http_pending_request_active_counter`
- `occnp_http_congestion_message_reject_total`

For information about the metrics, see Pod Congestion Metrics section.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

Copyright © 2019, 2026, Oracle and/or its affiliates.

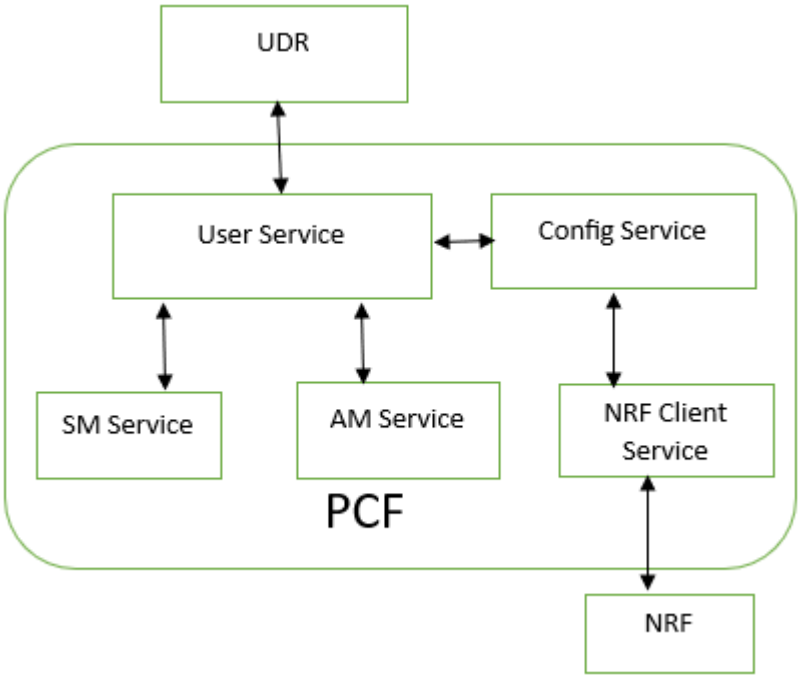
For more information about alerts, see Common Alerts.

4.30.3 User Service Pod Congestion Control

Policy User service is a connector service comprising of UDR and CHF connectors. UDR Connector interacts with UDR network function to fetch the latest subscriber information. CHF Connector interacts with CHF network function to fetch the latest charging information.

- **UDR Connector**- UDR Connector is a protocol specific layer which converts the PDS requests to nUDR specific request format and forwards it to UDR network function for subscription information. It also provides an ability to subscribe for notification in case of subscriber profile changes at UDR.
- **CHF Connector** – CHF Connector is a protocol specific layer which converts the PDS requests to nCHF specific request format and forwards it to CHF network function for fetching policy counter information. As per the 3gpp standards, it automatically subscribes for any profile changes at CHF.

Figure 4-90 PCF User Service interactions with other services



The Policy User service provides these subscriber and policy counter information to the core services such as SM, AM and UE services. It handles data requests from various policy services such as SM, AM, UE, NRF Client and PDS services. At times, an excessive traffic from these consumer services toward User service can be observed in the network, which can result in a high CPU utilization, high memory utilization. This can cause performance degradation in User service responses and eventually reach a state of service unavailability. Congestion control helps to identify such conditions and invoke load shedding rules to address these situations when these load conditions persist. With User service supporting the congestion control mechanism feature, it helps to protects its pods from congestion and ensures consistent service availability to its consumer.

The pod congestion control mechanism involves:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In the pod congestion control mechanism, each User service pod monitors its congestion state. The congestion control works at 5 levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, `cpuacct.usage`, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This REST API parameter can be configured to specify after how many continuous intervals, the pod state can be changed. The default value is 5. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This REST API parameter can be configured to specify the time duration or interval, after which the pod resource will be re-calculated. The default value is 200ms. This interval is configured in milliseconds and can range from 50 to 2147483647.

A pod's state changes when its resources, namely the CPU and Queue buffer usage exceeds the predefined congestion threshold, checked at regular intervals. An active CPU and Queue default threshold profile can be viewed using CNC Console at *Policy → Overload and Congestion Control → Congestion Control → Thresholds* section. The user can create new threshold profile and make it active. The UDR and CHF connector service pod's congestion states and their default congestion parameters, CPU, and Queue counts are provided in the following table:

Table 4-60 UDR Connector Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC)	50	2100
CONGESTION_L1	55	2400
CONGESTION_L2	60	2700
CONGESTED	65	3000

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-61 CHF Connector Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC)	60	3000
CONGESTION_L1	65	3400
CONGESTION_L2	70	3800
CONGESTED	75	4200

For more information about congestion control threshold profiles, see Thresholds section in CNC Console.

Triggering Pod Congestion Control

Every time User service receives requests from other services, it checks for the current congestion state of the pod. The Congestion Control mechanism is triggered if the pod's congestion state is in Danger of Congestion (DOC) or CONGESTION_L1 or CONGESTION_L2, or Congested. After verifying that the message request type, a priority is assigned to it. If the assigned priority is less than discard priority, the message is accepted and if the assigned priority is greater than or equal to discard priority then, the message is rejected.

Congestion Control Load Shedding

Based on the pod's current congestion state, a load shedding rule is applied to perform priority-based load shedding. The load shedding rule is based on message priority. For example, when the User service pod state is CONGESTED and the priority of discard messages is 30, then it determines if the message with the assigned priority is less than discard priority, the message is accepted and if the assigned priority is greater than or equal to discard priority than the message is rejected.

The User service pods performs load shedding by considering the load rule configured for current congestion state. You can configure these load rules using the Overload and Congestion Control menu in CNC Console. The User service drops the requests based on discard priority.

Priority-Based Load Shedding

You can configure load shedding rule for User service by providing the discard priority for each of the congestion state. If not, a default load shedding rule is active, and messages are discarded based on it. The default load shedding rules for UDR and CHF Connector service:

Table 4-62 UDR Connector Load Shedding Rules

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	29
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-63 CHF Connector Load Shedding Rules

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	29
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

You can add the following keys to configure the message priority for different rest endpoints using User service advanced settings in CNC Console. If any invalid or incorrect values are provided then the default priority values shall be considered.

Table 4-64 Configuring Message Priority

Key	Value	Description
UDR_GET_USER_DATA_REQUEST_PRIORITY	24	0-31
UDR_DELETE_USER_DATA_REQUEST_PRIORITY	16	0-31
UDR_PATCH_USER_DATA_REQUEST_PRIORITY	18	0-31
UDR_SUBS_TO_NOTIFY_REQUEST_PRIORITY	22	0-31
UDR_NOTIFY_REQUEST_PRIORITY	18	0-31
UDR_UM_NOTIFY_REQUEST_PRIORITY	18	0-31
CHF_GET_SPENDING_LIMIT_REQUEST_PRIORITY	24	0-31
CHF_DELETE_SPENDING_LIMIT_REQUEST_PRIORITY	16	0-31
CHF_TERMINATE_NOTIFY_REQUEST_PRIORITY	17	0-31
CHF_NOTIFY_REQUEST_PRIORITY	18	0-31

The user can configure the result codes for the rejected requests when configuring the load rules. The default response code is `503 Service Unavailable` for HTTP messages. You can configure with any valid non-2xx response codes only. The response can be configured using User service advanced settings in CNC Console, using the following keys:

- `UDR_CONGESTION_RESPONSE_CODE`
- `CHF_CONGESTION_RESPONSE_CODE`

In the response body, an error header is sent to the consumer service, providing the congestion error details as understood by the error-handler framework. A sample JSON error header:

```
{
  "errorDetails":{
  "status":"503",
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
  "cause":"NF_CONGESTION",
  "message":"Pod <pod-name> is in CONGESTION_L1",
  "targetService":"UDR_C"
  }
}
```

Propagation of Message Priority as Header Attribute

For internal requests toward User service, the priority is based on `oc-message-priority` header attribute. And for notification requests from Ingress Gateway, the priority is based on `3gpp-sbi-message-priority` header attribute. But if the priority values are not provided in the respective requests headers, then the message priority shall be based on the configured values in Advanced Settings or Default message priority values. Thus, the precedence order for assigning message priority shall be `oc-message-priority → 3gpp-sbi-message-priority → Advanced Settings Priority → Default Priority`.

The User service sends the `oc-message-priority` header attribute to upstream services and the value of this header depends on the priority precedence order. You can decide to include the priority information in `3gpp-sbi-message-priority` header toward Egress Gateway and NRF Client by adding the following keys in the User service advanced settings in CNC Console:

- UDR_ADD_3GPP_SBI_MSG_PRIORITY
- CHF_ADD_3GPP_SBI_MSG_PRIORITY

Again, the value of `3gpp-sbi-message-priority` is based on the above mentioned precedence order. The default value of these keys are false. The `oc-message-priority` header shall always propagate from User service to Egress Gateway and NRF Client.

It is recommended that Egress Gateway should not propagate `oc-message-priority` headers to external NFs. And by default behavior, `oc-message-priority` header will be dropped by Egress Gateway. But in case if you want to send these headers to external NFs, then remove these headers name under `globalRemoveRequestHeader` parameter in `custom_values.yaml` file.

Sample of customizable yaml file:

```
egress-gateway:
  globalRemoveRequestHeader:
    - name: ocLogId #DO NOT REMOVE OR EDIT THIS. This header holds the value
of TraceId and need to be removed from outgoing traffic.
    - name: oc-message-priority # Do not remove this. This is an internal
header that holds the message priority value.
  #  - name: 3gpp-Sbi-Origination-Timestamp
  #  - name: 3gpp-Sbi-Max-Rsp-Time
  #  - name: 3gpp-Sbi-Sender-Timestamp
```

For more information about Egress Gateway Helm parameters, see "Basic Configurations in Egress Gateway" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Call flow diagram for User Service Congestion Control

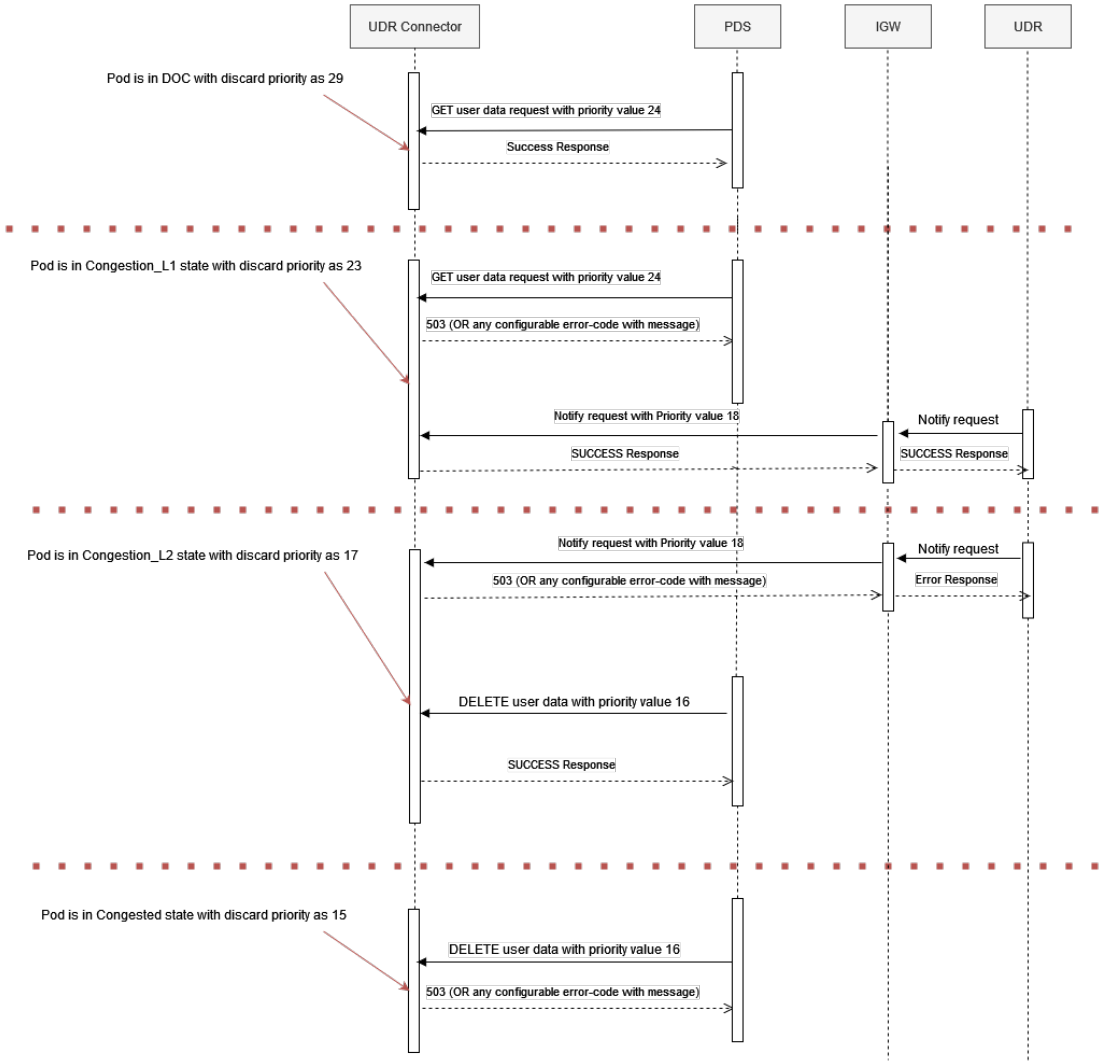
For this call flow, assume the load shedding rule for UDR Connector is set as:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-65 Example: UDR Connector Load Shedding Rule

Congestion States	Discard Priority
DANGER_OF_CONGESTION	29
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

Figure 4-91 Call flow diagram for UDR Connector Congestion Control



UDR Connector pod is in DOC state and the discard priority is configured as 29:

- PDS service sends a GET user request with message priority value set to 24 toward UDR Connector service.
- UDR Connector service responds with a success status.

UDR Connector pod is in Congestion_L1 state and the discard priority is configured as 23:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- PDS sends a GET user request with message priority value set to 24 toward UDR Connector.
- UDR Connector responds with a reject 503 status or with any configured error code and message.
- UDR sends notify request to Ingress Gateway.
- Ingress Gateway sends a notification request with message priority value set to 18 toward UDR Connector.
- UDR Connector responds with a success status to Ingress Gateway.
- Ingress Gateway service responds with a success status to UDR.

UDR Connector pod is in Congestion_L2 state and the discard priority is configured as 17:

- UDR sends notify request to Ingress Gateway.
- Ingress Gateway sends a notification request with message priority value set to 18 toward UDR Connector.
- UDR Connector responds with a reject 503 status or with any configured error code and message to Ingress Gateway.
- Ingress Gateway forwards the error response to the UDR.
- PDS sends DELETE user data request with priority value set to 16 toward UDR Connector.
- UDR Connector responds with a success status to PDS.

UDR Connector pod is in Congested state and the discard priority is configured as 15:

- PDS sends DELETE user data request with priority value set to 16 toward UDR Connector.
- UDR Connector responds with a reject 503 status or with any configured error code and message to PDS.

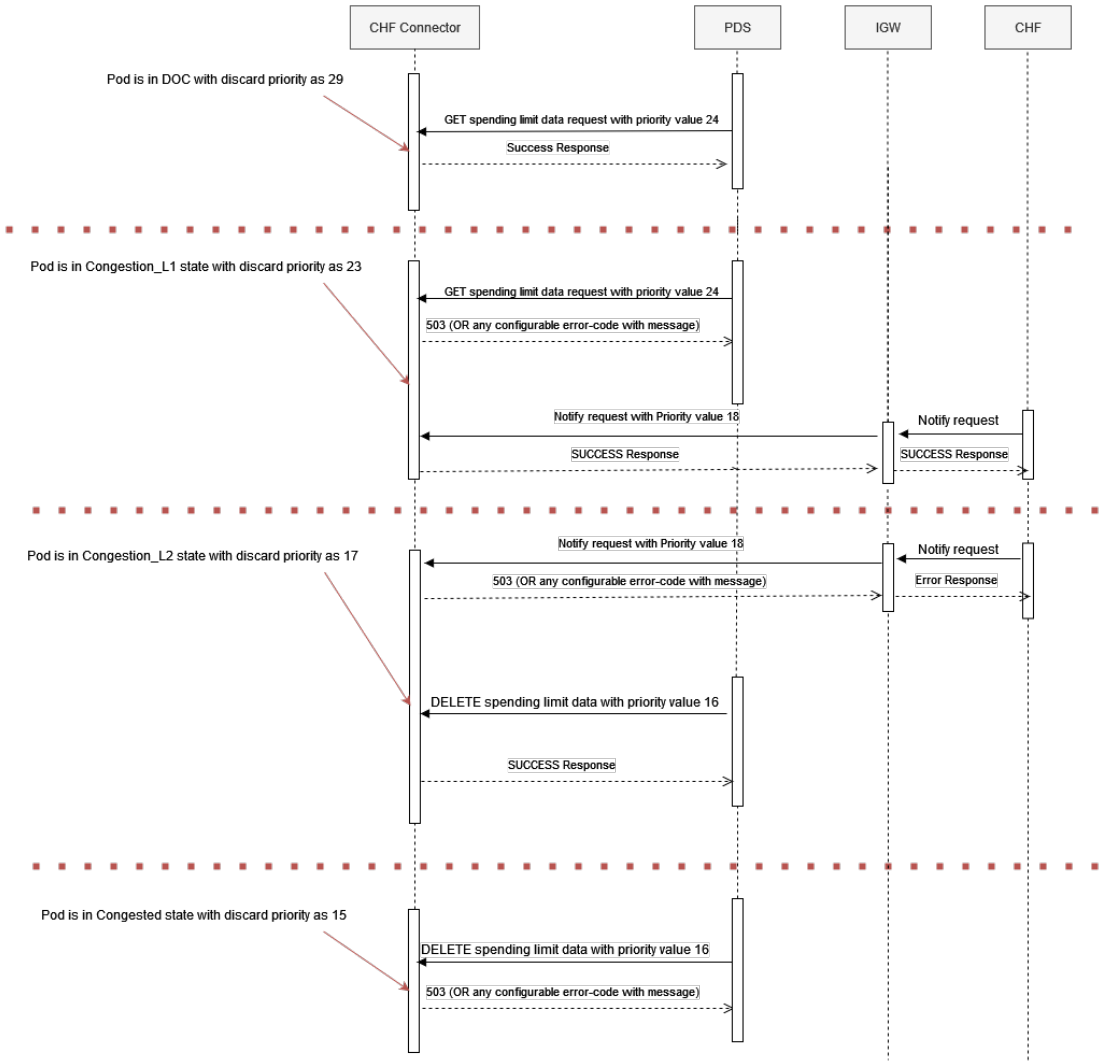
For this call flow, assume the load shedding rule for CHF Connector is set as:

Table 4-66 Example: CHF Connector Load Shedding Rule

Congestion States	Discard Priority
DANGER_OF_CONGESTION	29
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-92 Call flow diagram for CHF Connector Congestion Control



CHF Connector pod is in DOC state and the message priority is configured as 29:

- PDS service sends a GET user request with message priority value set to 24 toward CHF Connector service.
- CHF Connector service responds with a success status.

CHF Connector pod is in Congestion_L1 state and the discard priority is configured as 23:

- PDS sends a GET user request with message priority value set to 24 toward CHF Connector.
- CHF Connector responds with a reject 503 status or with any configured error code and message.
- CHF sends notify request to Ingress Gateway.
- Ingress Gateway sends a notification request with message priority value set to 18 toward CHF Connector.
- CHF Connector responds with a success status to Ingress Gateway.
- Ingress Gateway service responds with a success status to UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

CHF Connector pod is in Congestion_L2 state and the discard priority is configured as 17:

- CHF sends notify request to Ingress Gateway.
- Ingress Gateway sends a notification request with message priority value set to 18 toward CHF Connector.
- CHF Connector responds with a reject 503 status or with any configured error code and message to Ingress Gateway.
- Ingress Gateway forwards the error response to the CHF.
- PDS sends DELETE user data request with priority value set to 16 toward CHF Connector.
- CHF Connector responds with a success status to PDS.

CHF Connector pod is in Congested state and the discard priority is configured as 15:

- PDS sends DELETE user data request with priority value set to 16 toward CHF Connector.
- CHF Connector responds with a reject 503 status or with any configured error code and message to PDS.

Managing User service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for User service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations** for User Service.

To configure User service pod congestion control feature in CNC Console, see Congestion Control section.

To configure User service pod congestion control discard messages in CNC Console, see the Advanced Settings section in PCF User Connector.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The following common service metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_congestion_http_pending_request_active_counter`
- `occnp_http_congestion_message_reject_total`

For information about the metrics, see Pod Congestion Metrics section.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Maintain

Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support.

4.30.4 Diameter Connector Pod Congestion Control

Diameter Gateway acts as a gateway for all diameter traffic to the Policy solution. And, the Diameter Connector accepts diameter messages from Diameter Gateway and converts them to Http messages, and sends them to the other PCF components

At times, an excessive traffic from the consumer services toward Diameter Connector service can be observed in the network, which can result in a high CPU utilization, high memory utilization. This can cause performance degradation in Diameter Connector service responses and eventually reach a state of service unavailability. Congestion control helps to identify such conditions and invoke load shedding rules to address these situations when these load conditions persist. With Diameter Connector service supporting the congestion control mechanism feature, it helps to protects its pods from congestion and ensures consistent service availability to its consumer.

The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Copyright © 2019, 2026, Oracle and/or its affiliates.

Determining Pod Congestion State

In the pod congestion control mechanism, each Diameter Connector service pod monitors its congestion state. The congestion control works at 5 levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, `cpuacct.usage`, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

To avoid switching between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This REST API parameter can be configured to specify after how many continuous intervals, the pod state can be changed. The default value is 5. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This REST API parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. The default value is 200ms. This interval is configured in milliseconds and can range from 50 to 2147483647.

A pod's state changes when its resources, namely the CPU and Queue buffer usage exceeds the predefined congestion threshold, checked at regular intervals. An active CPU and Queue default threshold profile can be viewed using CNC Console at *Policy → Overload and Congestion Control → Congestion Control → Thresholds* section. The user can create new threshold profile and make it active. The Diameter Connector service pod's congestion states and their default congestion parameters, CPU, and Queue counts are provided in the following table:

Table 4-67 Diameter Connector Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC)	97	99997
CONGESTION_L1	98	99997
CONGESTION_L2	99	99997
CONGESTED	100	10000

For more information about congestion control threshold profiles, see Thresholds section in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Triggering Pod Congestion Control

Every time Diameter Connector service receives requests from other services, it checks for the current congestion state of the pod. The Congestion Control mechanism is triggered if the pod's congestion state is in Danger of Congestion (DOC) or CONGESTION_L1 or CONGESTION_L2, or Congested. After verifying that the message request type, a priority is assigned to it. If the assigned priority is greater than or equal to discard priority, the message is rejected.

Congestion Control Load Shedding

Based on the pod's current congestion state, a load shedding rule is applied to perform priority-based load shedding. The load shedding rule is based on message priority. For example, when the Diameter Connector service pod state is CONGESTED and the priority of discard messages is 30, then it determines if the message with the assigned priority should be rejected or accepted.

The Diameter Connector pods performs load shedding by considering the load rule configured for current congestion state. You can configure these load rules using the Overload and Congestion Control menu in CNC Console. The Diameter Connector drops the requests based on discard priority.

Priority-Based Load Shedding

You can configure the load shedding rule for Diameter Connector service by providing the discard priority for each of the congestion state. If not, a default load shedding rule is active, and messages are discarded based on it. The default load shedding rules for Diameter Connector service:

Table 4-68 Diameter Connector Load Shedding Rules

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	28
CONGESTION_L1	25
CONGESTION_L2	20
CONGESTED	17

Table 4-69 Messages Default Priorities

Advanced Settings Key	Default Priority	Message Type
SM.NOTIFY.REQUEST.PRIORITY	25	Re Authorization notification (RAR)
SM.NOTIFY.TERMINATE.REQUEST.PRIORITY	20	Terminate notify (ASR)
PDS.FETCH.REQUEST.PRIORITY	25	PDS Fetch SLR
PDS.NOTIFY.TERMINATE.REQUEST.PRIORITY	20	PDS Notify terminate (STR)

Table 4-70 Diameter Messages Default Priorities

Advanced Settings Key	Default Priority	Diameter Message Type
RX.AAR.REQUEST.PRIORITY	30	Rx AAR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-70 (Cont.) Diameter Messages Default Priorities

Advanced Settings Key	Default Priority	Diameter Message Type
RX.STR.REQUEST.PRIORITY	20	Rx STR
SY.SNR.DEFAULT.PRIORITY	25	Sy SNR

You can add the following keys to configure the message priority for different rest endpoints using Diameter Connector advanced settings in CNC Console. If any invalid or incorrect values are provided then the default priority values shall be considered.

Table 4-71 Configuring Response Code

Key	Value	Description
CONGESTION.USE.EXPERIMENTAL.RESULT.CODE	false	To set if user wants to use experimental result code when rejecting diameter messages. Allowed values are true or false. By default it will be false.
CONGESTION.VENDOR.ID	0	This is to configure the diameter vendor id for the congestion control discards and data type of value will be numerical. If value is non-zero, then the *CONGESTION_DIAMETER_RESPONSE_CODE* considered as the experimental result code. If value is zero / not configured, then *CONGESTION_DIAMETER_RESPONSE_CODE*considered as the normal result code. **Examples**: CONGESTION_DIAMETER_VENDOR_ID=10415 CONGESTION_DIAMETER_VENDOR_ID=21274

You can also configure the result codes for the rejected requests when configuring the load rules. For diameter requests, the Diameter Connector rejects request with default `DIAMETER_TOO_BUSY (3004)` result code.

Table 4-72 Response Code

Key	Value	Description
CONGESTION.DIAMETER.RESPONSE.CODE	3004	To set response code when rejecting diameter messages. Only valid 3xxx, 4xxx, 5xxx response codes are allowed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-72 (Cont.) Response Code

Key	Value	Description
CONGESTION.HTTP.RESPONSE.CODE	503	Configure the response code of any rejected requests by Diameter Connector Core service due to congestion state. By default, the service sends 503 as response code. If configured then it shall be 1xx, 3xx, 4xx or 5xx response code.

In the response body, an error header is sent to the consumer service, providing the congestion error details as understood by the error-handler framework. A sample JSON error response:

```
{
  "errorDetails":{
  "status":"503",
  "cause":"NF_CONGESTION",
  "message":"Pod <pod-name> is in CONGESTION_L1",
  "targetService":"DIAMETER_CONNECTOR"
  }
}
```

Propagation of Message Priority as Header Attribute

For internal requests toward Diameter Connector service, the priority is based on `oc-message-priority` AVP. But if the priority values are not provided in the requests headers, then the message priority shall be based on the configured values in Advanced Settings or Default message priority values. Thus, the precedence order for assigning message priority shall be `oc-message-priority → Advanced Settings Priority → Default Priority`.

Managing User service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for Diameter Connector service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations** for Diameter Connector Service.

To configure Diameter Connector service pod congestion control feature in CNC Console, see Congestion Control section.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observability

Metrics:

The following common service metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_http_congestion_message_reject_total`
- `occnp_congestion_http_pending_request_active_counter`

For information about the metrics, see Pod Congestion Metrics section.

The following common service metrics are used to provide information about this feature:

- `occnp_diam_congestion_message_reject_total`
- `occnp_http_pending_requests`
- `occnp_diam_pending_requests`
- `occnp_congestion_diam_pending_request_active_counter`
- `occnp_congestion_http_pending_request_active_counter`
- `occnp_congestion_diam_pending_request_end_to_end_id_map_size`
- `occnp_congestion_DiamMsgBuffer_queue_msg_count`

For information about the metrics, see Diameter Connector Service Metrics section.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.30.5 UE Service Pod Congestion Control

The UE Policy Control service is provided by the Policy Control Function (PCF). This service is used as part of the provisioning of UE policies determined by the PCF to the UE via the AMF. At times, an excessive traffic from consumer services toward UE service can be observed in the network, which can result in a high CPU utilization, high memory utilization. The UE service gets congested and can cause performance degradation in its service response time and eventually reach a state of service unavailability. By implementing Congestion Control mechanism in UE service ensures that its service is protected from congestion and also its service is consistently available to the consumer services.

Congestion control mechanism identifies congestion conditions and invokes load shedding rules when such load conditions persist in UE service. The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In the pod congestion control mechanism, each UE service pod monitors its congestion state. The congestion control works at 5 levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

Each state indicates how congested the Pod is, and which requests can be served when the Pod is in certain congestion state.

The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, cpuacct.usage, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

The UE service pod's congestion states and their default congestion parameters, CPU, and Queue counts are provided in the following table:

Table 4-73 UE Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC)	65	1400
CONGESTION_L1	70	2100
CONGESTION_L2	75	2800
CONGESTED	80	3500

Copyright © 2019, 2026, Oracle and/or its affiliates.

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This REST API parameter can be configured to specify after how many continuous intervals, the pod state can be changed. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This REST API parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. This interval is configured in milliseconds and can range from 50 to 2147483647.

Triggering Pod Congestion Control

Every time UE service receives requests from other services, it checks for the current congestion state of the pod. The Congestion Control mechanism is triggered if the pod's congestion state is in DOC or CONGESTION_L1 or CONGESTION_L2 or Congested.

The requests to the UE service might have priority included as `oc-message-priority` attribute in the request header. The priority value ranges between 0 to 31 with 0 being the highest and 31 being the lowest priority.

Priority-Based Load Shedding

Based on the pod's current congestion state, a load shedding rule is applied to perform priority-based load shedding. The load shedding rule is based on message priority. For example, when the UE service pod state is CONGESTED and the priority of discard messages is 30, then it determines if the message with the assigned priority should be rejected or accepted.

The user can configure load shedding rule for UE service by providing the discard priority for each of the congestion state. If not, a default load shedding rule is active, and messages are discarded based on it. The user can configure the result codes for the rejected requests when configuring the load rules. The default result code is `503 Service Unavailable` for HTTP messages.

The default load shedding rules for UE service:

```
- state: DANGER_OF_CONGESTION
      discardPriority: 28
- state: CONGESTION_L1
      discardPriority: 25
- state: CONGESTION_L2
      discardPriority: 20
- state: CONGESTED
      discardPriority: 17
```

When UE service is in congestion state, its response can be configured using UE service advanced settings in CNC Console, using the key CONGESTION.HTTP.RESPONSE.CODE. This key is used to configure the response code of the messages that are rejected by the UE service due to pod's congestion state. By default, UE Service responds with a response code of 503. The response code configured should be 5xx error status only. Following is the list of configurable keys that can be added to set the message priority:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-74 Configuring Message Priority

Key	Default Value	Allowed Values
UE.GET.SUBSCRIBER.SESSIONS.PRIORITY	28	0-31
UE.GET.POLICY.ASSOCIATION.PRIORITY	18	0-31
UE.CREATE.PRIORITY	24	0-31
UE.UPDATE.PRIORITY	18	0-31
UE.UPDATE.NOTIFICATION.PRIORITY	18	0-31
UE.DELETE.PRIORITY	16	0-31
UE.AUDIT.NOTIFY.PRIORITY	30	0-31
UE.N1.NOTIFICATION.MESSAGE.PRIORITY	18	0-31
UE.N1.FAILURE.NOTIFICATION.MESSAGE.PRIORITY	18	0-31
CONGESTION.HTTP.RESPONSE.CODE	503	1xx, 3xx, 4xx, or 5xx

Managing UE service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for UE service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations**.

To configure UE service pod congestion control feature in CNC Console, see Congestion Control section.

To configure UE service pod congestion control discard messages in CNC Console, see the Advanced Settings section in PCF UE Policy Service.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The following common service metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

For information about the metrics, see Pod Congestion Metrics section.

The metric `occnp_http_congestion_message_reject_total` was added to the UE service for this feature. For information about the metrics, see UE Service Metrics section.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Maintain

Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

To resolve any alerts at the system or application level, see Alerts section. In case the alerts still persist, perform the following:

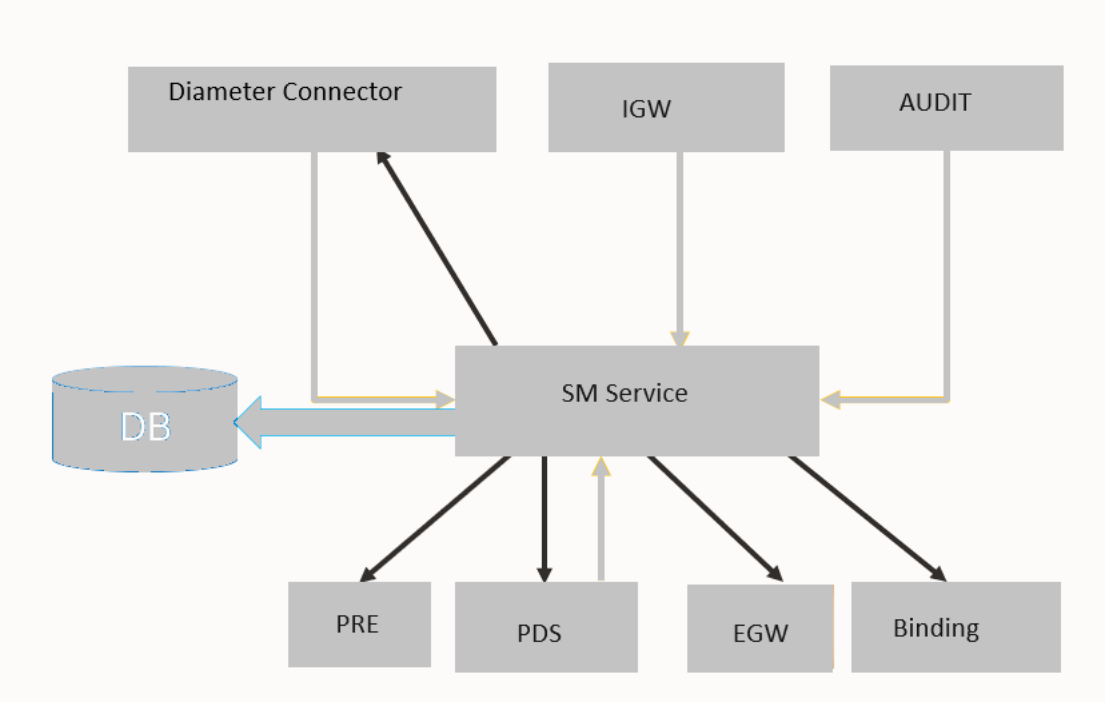
- **Collect the logs**: For more information on how to collect logs, see *Oracle Communications Clout Native Core, Converged Policy Troubleshooting Guide*.
- **Raise a service request**: See My Oracle Support.

4.30.6 SM Service Pod Congestion Control

The Session Management (SM) service performs provisioning, update and removal of session related policies and PCC rules by PCF to Session Management Function (SMF). SM service interacts with other PCF services, as shown in the following diagram:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-93 Policy Services and SM service interaction



- SMF interacts with SM service to Create/Update/Delete Policy associations.
- AF interacts with SM service to Create/Update/Delete App Sessions.
- PDS interacts with SM service to notify user data change and UDR subscription failures.
- Audit service interacts with SM service to process stale data.

At times, an excessive traffic from these services toward SM service can be observed in the network, which can result in a high CPU utilization, high memory utilization. This can cause performance degradation in SM service responses and eventually reach a state of service unavailability. Congestion control helps to identify such conditions and invoke load shedding rules to address these situations when these load conditions persist.

The SM service pod congestion control mechanism ensures consistent service availability to its consumer.

The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In the pod congestion control mechanism, each SM service pod monitors its congestion state. The congestion control works at 5 levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2

Copyright © 2019, 2026, Oracle and/or its affiliates.

- CONGESTED

The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, `cpuacct.usage`, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

The SM service pod's congestion states and their default congestion parameters, CPU, and Queue counts are provided in the following table:

Table 4-75 SM Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC)	75	720
CONGESTION_L1	80	1080
CONGESTION_L2	85	1440
CONGESTED	90	1800

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This REST API parameter can be configured to specify after how many continuous intervals, the pod state can be changed. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This REST API parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. This interval is configured in milliseconds and can range from 50 to 2147483647.

Triggering Pod Congestion Control

Every time SM service receives requests from other services, it checks for the current congestion state of the pod. The Congestion Control mechanism is triggered if the pod's congestion state is in DOC or CONGESTION_L1 or CONGESTION_L2 or Congested.

The requests to the SM service might have priority included as `oc-message-priority` attribute in the request header. The priority value ranges between 0 to 100 with 0 being the highest and 100 being the lowest priority.

Priority-Based Load Shedding

Based on the pod's current congestion state, a load shedding rule is applied to perform priority-based load shedding. The load shedding rule is based on message priority. For example, when the SM service pod state is CONGESTED and the priority of discard messages is 30, then it determines if the message with the assigned priority should be rejected or accepted.

The user can configure load shedding rule for SM service by providing the discard priority for each of the congestion state. If not, a default load shedding rule is active, and messages are discarded based on it. The user can configure the result codes for the rejected requests when configuring the load rules. The default result code is `503 Service Unavailable` for HTTP messages.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The default load shedding rules for SM service:

```
- state: DANGER_OF_CONGESTION
      discardPriority: 27
- state: CONGESTION_L1
      discardPriority: 19
- state: CONGESTION_L2
      discardPriority: 17
- state: CONGESTED
      discardPriority: 15
```

When SM service is in congestion state, its response can be configured using SM service advanced settings in CNC Console, using the key CONGESTION_RESPONSE_CODE. This key is used to configure the response code of the messages that are rejected by the SM service due to pod's congestion state. By default, SM Service responds with a response code of 503. The response code configured should be 5xx error status only. Following is the list of configurable keys that can be added to set the message priority:

Table 4-76 Configuring Message Priority

Key	Default Value	Allowed Values
SM.TDF.SESSION.DELETE.PRIORITY	16	0-31
SM.TDF.SESSION.UPDATE.PRIORITY	18	0-31
SM.UPDATE.EVENT.SUBS.PRIORITY	18	0-31
SM.CREATE.PRIORITY	24	0-31
SM.SUB.FAIL.NOTIFY.PRIORITY	26	0-31
SM.USER.SERVICE.NOTIFY.PRIORITY	18	0-31
SM.UPDATE_PRIORITY	18	0-31
SM.REAUTH_PRIORITY	20	0-31
SM.DELETE.PRIORITY	16	0-31
SM.POLICY.CLEANUP.PRIORITY	20	0-31
SM.APP.SESSION.CREATE.PRIORITY	24	0-31
SM.APP.SESSION.DELETE.PRIORITY	16	0-31
SM.APP.SESSION.CLEANUP.PRIORITY	20	0-31
SM.AUDIT.NOTIFY.PRIORITY	30	0-31
SM.GET.APP.SESSION.PRIORITY	28	0-31
SM.GET.ASSOC.PRIORITY	28	0-31
SM.GET.SUBSCRIBER.SESSIONS.PRIORITY	28	0-31
SM.GET.ASSOC.QUERY.PRIORITY	28	0-31

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-76 (Cont.) Configuring Message Priority

Key	Default Value	Allowed Values
SM.PDS.LOCATION.INFO.NOTIFY.PRIORITY	30	0-31
CONGESTION_RESPONSE_CODE	503	5xx

> **Note**
>
> Emergency session during SM pod congestion should be handled with a message profile configuration to assign the highest message priority to avoid emergency session rejection during congestion.

Managing SM service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for SM service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations**.

To configure SM service pod congestion control feature in CNC Console, see Congestion Control section.

To configure SM service pod congestion control discard messages in CNC Console, see the Advanced Settings section in PCF Session Management section.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The following metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_http_congestion_message_reject_total`

For information about the metrics, see Pod Congestion Metrics.

Alerts

The following alerts are generated for this feature:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Maintain

Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support.

4.30.7 PDS Pod Congestion Control

The Policy Data Source (PDS) stores the User or Subscriber State Variable (SSV) information. PDS interacts with other Policy services, such as:

- The core services such as AM/UE/SM and PCRF Core services send requests to PDS. It would be a request to either fetch, update, or delete the SSV data.
- User service, SOAP Connector, and Diameter Connector send notification requests to PDS.
- Query service sends request to PDS to either get or delete SSV data. It also gets the default workflow details from the PDS.
- Audit service sends audit notification request to PDS.

At times, an excessive traffic from these services toward PDS service can be observed in the network, which can result in a high CPU utilization, high memory utilization. This can cause performance degradation in PDS service responses and eventually reach a state of service unavailability. Congestion control helps to identify such conditions and invoke load shedding rules to address these situations when these load conditions persist.

The PDS pod congestion control mechanism ensures consistent service availability to its consumer.

The pod congestion control mechanism involves:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In the pod congestion control mechanism, each PDS service pod monitors its congestion state. The congestion control works at 5 levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, `cpuacct.usage`, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

The PDS service pod's congestion states and their default congestion parameters, CPU, and Queue counts are provided in the following table:

Table 4-77 PDS Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC)	65	50
CONGESTION_L1	70	100
CONGESTION_L2	75	150
CONGESTED	80	200

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This REST API parameter can be configured to specify after how many continuous intervals, the pod state can be changed. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This REST API parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. This interval is configured in milliseconds and can range from 50 to 2147483647.

Triggering Pod Congestion Control

Every time PDS service receives requests from other services, it checks for the current congestion state of the pod. The Congestion Control mechanism is triggered if the pod's congestion state is in DOC or CONGESTION_L1 or CONGESTION_L2 or Congested.

Assigning Message Priority:

Copyright © 2019, 2026, Oracle and/or its affiliates.

The requests to the PDS service might have priority included as `oc-message-priority` attribute in the request header. The priority value ranges between 0 to 100 with 0 being the highest and 100 being the lowest priority. If the priority header is not provided in the requests, then the message priority shall be decided based on the configured or default values set for PDS service. Thus message priority precedence order shall be `oc-message-priority → priority set in PDS Advanced Settings → Default Priority`.

Currently Policy services such as SM, PCRF Core, UDR Connector, and CHF Connector services propagates `oc-message-priority` header to PDS service. The other Policy services shall also support this header propagation to PDS service in future releases.

Priority-Based Load Shedding

Based on the pod's current congestion state, a load shedding rule is applied to perform priority-based load shedding. The load shedding rule is based on message priority. For example, when the PDS service pod state is CONGESTED and the priority of discard messages is 30, then it determines if the message with the assigned priority should be rejected or accepted.

The user can configure load shedding rule for PDS service by providing the discard priority for each of the congestion state. If not, a default load shedding rule is active, and messages are discarded based on it. The user can configure the result codes for the rejected requests when configuring the load rules. The default result code is `503 Service Unavailable` for HTTP messages.

The default load shedding rules for PDS service:

```
- state: DANGER_OF_CONGESTION
      discardPriority: 28
- state: CONGESTION_L1
      discardPriority: 20
- state: CONGESTION_L2
      discardPriority: 17
- state: CONGESTED
      discardPriority: 15
```

When PDS service is in congestion state, its response can be configured using PDS service advanced settings in CNC Console, using the key CONGESTION_RESPONSE_CODE. This key is used to configure the response code of the messages that are rejected by the PDS service due to pod's congestion state. By default, PDS service responds with a response code of 503. The user can configure this parameter with either 1xx, 3xx, 4xx, or 5xx response codes. Following are the list of configurable keys that can be added to set the message priority:

Table 4-78 Configuring Message Priority

Key	Default Value	Allowed Values
PDS_NOTIFY_USER_DATA_REQUEST_PRIORITY	18	0-100
PDS_GET_USER_DATA_REQUEST_PRIORITY	18	0-100
PDS_UPDATE_USER_DATA_REQUEST_PRIORITY	18	0-100
PDS_DELETE_USER_DATA_REQUEST_PRIORITY	16	0-100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-78 (Cont.) Configuring Message Priority

Key	Default Value	Allowed Values
PDS_AUDIT_NOTIFY_REQUEST_PRIORITY	27	0-100
CONGESTION_RESPONSE_CODE	503	1xx, 3xx, 4xx, or 5xx

> **Note**
>
> For Policy application with Aspen Service Mesh (ASM) setups, add the `CONGESTION_RESPONSE_CODE` set to 500 using PDS Advanced Settings.

Example for Congestion Control Call Flow/Scenario

For the below call flows, consider the following load shedding rule configuration:

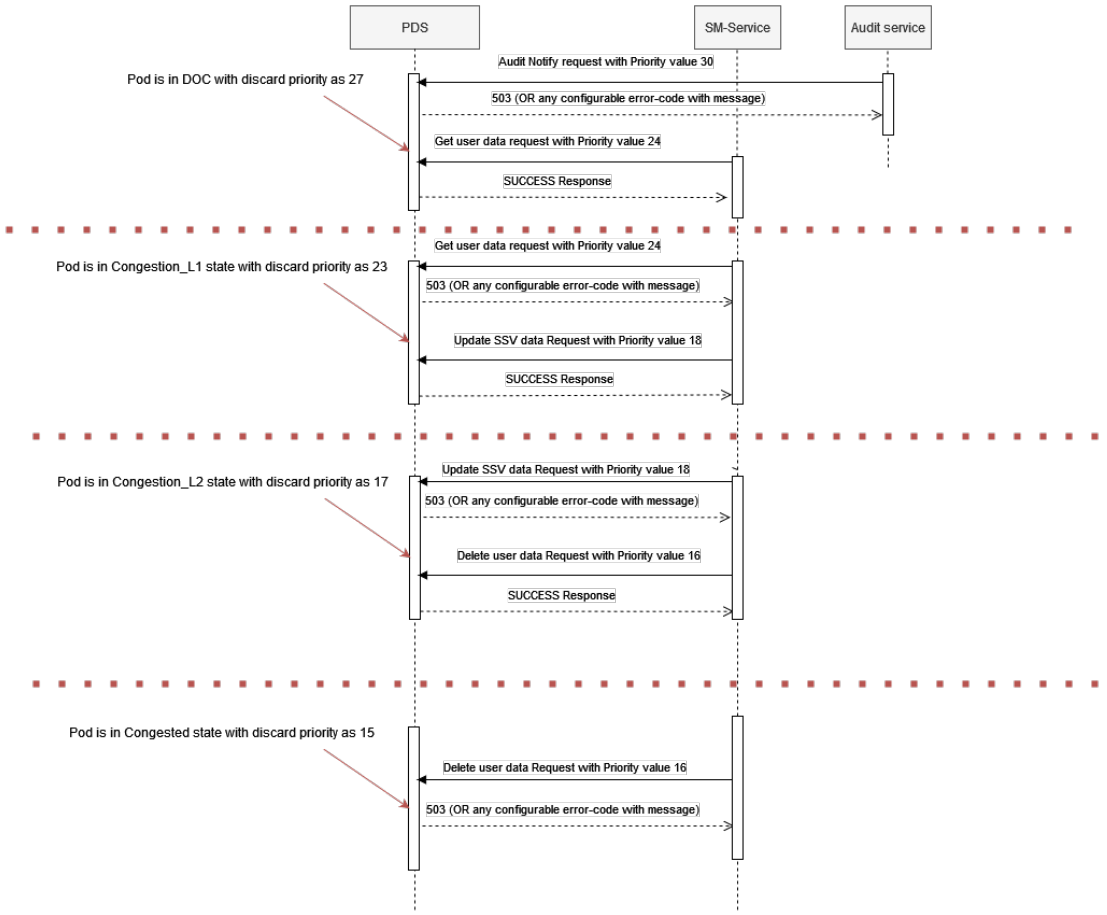
Table 4-79 Load Shedding Rule

Congestion State	Discard Priority
DOC	27
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

The call flow describes the PDS service congestion control mechanism handling the requests from the other Policy services such as SM and Audit services when it is in different congestion state.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-94 PDS Congestion Control Call Flow



PDS pod congestion is in DOC state and the discard priority is configured as 27:

- Audit service sends a notification request with discard priority value set to 30 toward PDS service.
- PDS service responds with a reject 503 status or with any configured error code and message.
- SM service sends a GET user information request with discard priority value set to 24 toward PDS service.
- PDS service responds with the success status.

PDS pod congestion is in Congestion_L1 state and the discard priority is configured as 23:

- SM service sends a GET user information request with discard priority value set to 24 toward PDS service.
- PDS service responds with a reject 503 status or with any configured error code and message.
- SM service sends an Update SSV request with discard priority value set to 18 toward PDS service.
- PDS service responds with the success status.

PDS pod congestion is in Congestion_L2 state and the discard priority is configured as 17:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- SM service sends an Update SSV request with discard priority value set to 18 toward PDS service.
- PDS service responds with a reject 503 status or with any configured error code and message.
- SM service sends a Delete user information request with discard priority value set to 16 toward PDS service.
- PDS service responds with the success status.

PDS pod congestion is in Congested state and the discard priority is configured as 15:

- SM service sends a Delete user information request with discard priority value set to 16 toward PDS service.
- PDS responds with a reject 503 or with any configured error code and message.

Managing PDS service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for PDS service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations**.

To configure SM service pod congestion control feature in CNC Console, see Congestion Control section.

To configure SM service pod congestion control discard messages in CNC Console, see the Advanced Settings section in PDS Settings section.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The following metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `pod_cong_state_report_total`
- `pod_resource_congestion_state_report_total`
- `http_congestion_message_reject_total`

For information about the metrics, see Pod Congestion Metrics.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED

Copyright © 2019, 2026, Oracle and/or its affiliates.

- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Maintain

Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support.

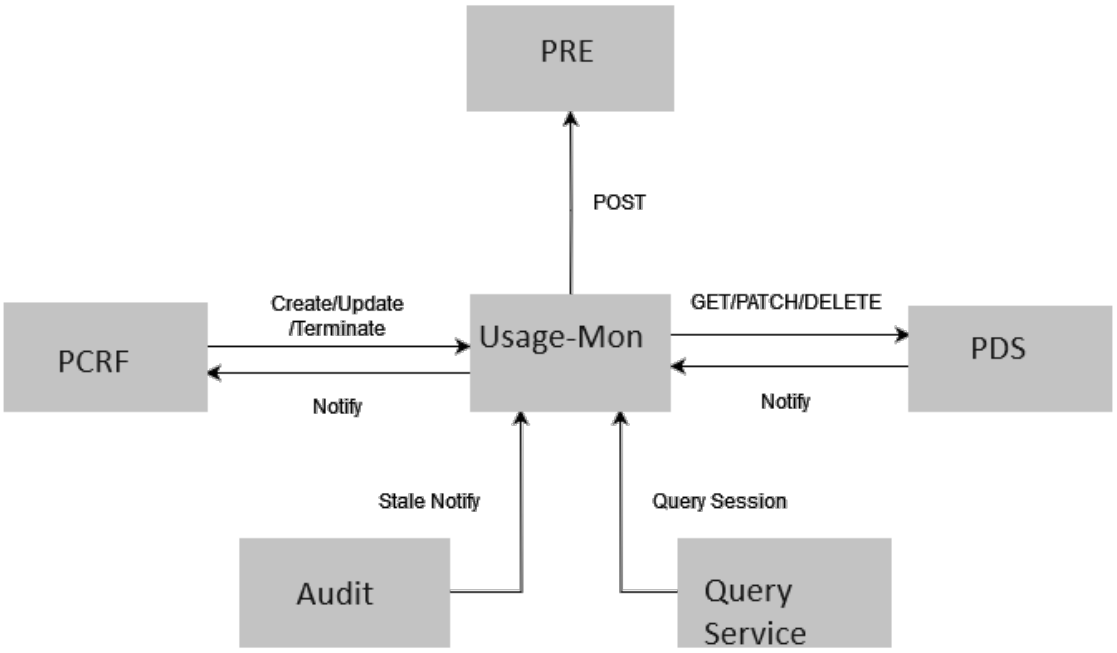
4.30.8 Usage Monitoring Pod Congestion Control

The Policy Usage Monitoring service interacts with PRE and UDR services to get usage monitoring related Policy decisions and it also sends notifications to the subscribers about their current data usage.

Usage Monitoring interacts with other Policy services, as shown in the following diagram:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-95 Usage Monitoring Service and other Policy services



- The PCRF core services send requests to Usage Monitoring service.
- Audit service sends requests to Usage Monitoring service for stale session notification.
- Usage Monitoring service sends requests to PRE for retrieving Policy decisions.
- Usage Monitoring service sends requests to PDS for Subscriber information.

At times, an excessive traffic from these services toward Usage Monitoring service can be observed in the network, which can result in a high CPU utilization, high memory utilization. This can cause performance degradation in Usage Monitoring service responses and eventually reach a state of service unavailability. Congestion control helps to identify such conditions and invoke load shedding rules to address these situations when these load conditions persist. The Usage Monitoring service pod congestion state is identified by CPU utilization and pending requests in the Queue.

The Usage Monitoring pod congestion control mechanism ensures consistent service availability to its consumer.

The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In the pod congestion control mechanism, each Usage Monitoring service pod monitors its congestion state. The congestion control works at 5 levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2

Copyright © 2019, 2026, Oracle and/or its affiliates.

- CONGESTED

The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, `cpuacct.usage`, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

The Usage Monitoring service pod's congestion states and their default congestion parameters, CPU, and Queue values are provided in the following table:

Table 4-80 Usage Monitoring Service Congestion States

Congestion States	CPU (%)	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	65	50
CONGESTION_L1	70	100
CONGESTION_L2	75	150
CONGESTED	80	200

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This REST API parameter can be configured to specify after how many continuous intervals, the pod state can be changed. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This REST API parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. This interval is configured in milliseconds and can range from 50 to 2147483647.

Triggering Pod Congestion Control

Every time Usage Monitoring service receives requests from other services, it checks for the current congestion state of the pod. The Congestion Control mechanism is triggered if the pod's congestion state is in DOC or CONGESTION_L1 or CONGESTION_L2 or Congested.

The requests to the Usage Monitoring service might have priority included as `oc-message-priority` attribute in the request header. If the priority is not included in the request, then the default priorities defined in the Usage Monitoring, CNC Console is considered. The priority value ranges between 0 to 31 with 0 being the highest and 31 being the lowest priority.

Priority-Based Load Shedding

Based on the pod's current congestion state, a load shedding rule is applied to perform priority-based load shedding. The load shedding rule is based on message priority. For example, when the Usage Monitoring service pod state is CONGESTED and the priority of discard messages is 30, then it determines if the message with the assigned priority should be rejected or accepted.

The user can configure load shedding rule for Usage Monitoring service by providing the discard priority for each of the congestion state. If not, a default load shedding rule is active, and messages are discarded based on it. The user can configure the result codes for the

Copyright © 2019, 2026, Oracle and/or its affiliates.

rejected requests when configuring the load rules. The default result code is `503 Service Unavailable` for HTTP messages.

The default load shedding rules for Usage Monitoring service:

```
- state: DANGER_OF_CONGESTION
      discardPriority: 30
- state: CONGESTION_L1
      discardPriority: 27
- state: CONGESTION_L2
      discardPriority: 24
- state: CONGESTED
      discardPriority: 20
```

When Usage Monitoring service is in congestion state, its response can be configured using Usage Monitoring service **Message Default Priority for Congestion Control** settings in CNC Console, using the key CONGESTION ERROR CODE. This key is used to configure the response code of the messages that are rejected by the Usage Monitoring service due to pod's congestion state. By default, Usage Monitoring service responds with a response code of 503. The response code configured should be 5xx error status only. Following is the list of configurable Usage Monitoring API message default priorities for Congestion Control:

Table 4-81 Configuring Message Priority

Key	Default Value	Allowed Values
UM Session Create API	20	0-31
UM Session Update API	17	0-31
UM Session Terminate API	15	0-31
UM Session Notify API	17	0-31
UM Session Audit Subscriber API	31	0-31
UM Session Search Subscriber API	30	0-31
UM Session Audit Notify API	31	0-31
Congestion Error Code	503	5xx

Managing Usage Monitoring service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for Usage Monitoring service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations**.

To configure SM service pod congestion control feature in CNC Console, see Congestion Control section.

To configure SM service pod congestion control discard messages in CNC Console, see Message Default Priority for Congestion Control fields in Configuring Usage Monitoring section.

Configure Using REST API

Copyright © 2019, 2026, Oracle and/or its affiliates.

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The following metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_http_congestion_message_reject_total`

For information about the metrics, see Pod Congestion Metrics.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Maintain

Error logs are generated when the system is congested and the actions are taken to bring the system back to normal. Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.30.9 PCRF Core Pod Congestion Control

Policy and Charging Rules Function (PCRF) service integrates with various Policy services. It receives requests from Diameter Gateway, PDS, PRE or Binding services. At times, an excessive traffic from these services toward PCRF Core service can be observed in the network, which can result in a high CPU and memory utilization. The PCRF Core service gets congested and can cause performance degradation in its service response time and eventually reach a state of service unavailability. By implementing Congestion Control mechanism in PCRF service ensures that its service is protected from congestion and also its service is consistently available to the consumer services.

Congestion control feature in PCRF Core service is an improvement to its Admission Control feature. Admission Control feature decides the congestion state based on pending requests in diameter queue, whereas Congestion Control decides based on the pending requests existing at the overall application level and on the CPU utilization by the pod. By default Admission Control feature is enabled, and Congestion Control feature is disabled.

> **Note**
>
> To use Congestion Control feature, it is recommended to disable Admission Control feature by setting `ADMISSION.Enabled` as false in PCRF Core service advanced settings.

Congestion control mechanism identifies congestion conditions and invokes load shedding rules when such load conditions persist in PCRF Core service. The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In the pod congestion control mechanism, each PCRF Core service pod monitors its congestion state. The congestion control works at 5 levels or states:

- NORMAL
- DANGER_OF_CONGESTION (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

Each state indicates how congested the Pod is, and which requests can be served when the Pod is in certain congestion state.

The pod's congestion state is decided based on CPU consumption and Queue.

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, cpuacct.usage, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This parameter can be configured to specify after how many continuous intervals, the pod state can be changed. This value can range from 1 to 2147483647.
- `stateCalculationInterval`: This parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. This interval is configured in milliseconds and can range from 50 to 2147483647.

For more information about these congestion control configurations, see Congestion Control Settings section in CNC Console.

The pod's state changes when its resources, namely the CPU and Queue buffer usage exceeds the predefined congestion threshold, checked at regular intervals. An active CPU and Queue default threshold profile can be viewed using CNC Console at *Policy → Overload and Congestion Control → Congestion Control → Thresholds* section. The user can create new threshold profile and make it active. The PCRF Core service pod's congestion states and their default congestion parameters, CPU, and Queue counts are provided in the following table:

Table 4-82 PCRF Core Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC	65	250
CONGESTION_L1	70	300
CONGESTION_L2	75	350
CONGESTED	85	400

For more information about these CPU and Queue count thresholds configurations, see Congestion Control Thresholds section in CNC Console.

Triggering Pod Congestion Control

With Congestion Control feature enabled for PCRF service, every time a message is fetched for processing, the system checks the current congestion state of the pod. If the current state is either in `DOC`, `CONGESTION_L1`, `CONGESTION_L2`, or `Congested` state, then the congestion control mechanism is triggered. After verifying that the message type is a request, a request priority is assigned to it. If the request priority is greater than or equal to the discard priority, then the message is rejected, otherwise it is accepted.

Congestion Control Load Shedding using Discard and Request Priority

The PCRF Core service pods performs load shedding by considering the load rule configured for the current congestion state. The load shedding rule is based on message priority configuration. A default load shedding rule is active and the messages are discarded based on it. You can configure these load rules using the Overload and Congestion Control menu in CNC Console. The Diameter Gateway discards the requests based on **Priority**.

Table 4-83 PCRF Core Service Default Discard Priorities:

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	29

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-83 (Cont.) PCRF Core Service Default Discard Priorities:

Congestion State	Discard Priority (Default Value)
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

For more information about discard priority configurations, see Congestion Control Load Shedding Rules section in CNC Console.

Assigning Message Priority:

The HTTP requests to the PCRF service may have message priority included as `oc-message-priority` attribute in the request header. The message priority value ranges between 0 to 100 with 0 being the highest and 100 being the lowest priority. If the priority header is not provided in the requests, then the message priority that is either configured in the Advanced Settings of PCRF Core service or default priority values will be considered. Following is the list of configurable keys that can be added to set the HTTP message priority:

Table 4-84 Configuring Message Priority

Key	Default Value	Description
CONGESTION.HTTP.RESPONSE.CODE	503	Configure the response code of any rejected requests by PCRF Core service due to congestion state. By default, the service sends 503 as response code. If configured then it shall be either 1xx, or 3xx, or 4xx, or 5xx status code.
PDS.NOTIFY.REQUEST.PRIORITY	18	Set request priority for post PDS notification request. **Allowed Values**: 0-100
UM.NOTIFY.REQUEST.PRIORITY	18	Set request priority for post Usage monitoring notification request. **Allowed Values**: 0-100
PCRF.SESSION.DELETE.REQUEST.PRIORITY	30	Set request priority for deleting PCRF session request. **Allowed Values**: 0-100
PCRF.SESSION.GET.REQUEST.PRIORITY	30	Set request priority for fetching PCRF session request. **Allowed Values**: 0-100
AUDIT.NOTIFY.REQUEST.PRIORITY	30	Set request priority for post Audit notification request. **Allowed Values**: 0-100

The Diameter requests to the PCRF service may have AVP named as `OC-Message-Priority`. The message priority value for this AVP ranges between 0 to 100. If Diameter Gateway,

- on receiving Diameter Routing Message Priority (DRMP) from the clients, it sets `OC-Message-Priority` to `DRMP*2` and sends it to PCRF Core service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- on not receiving DRMP from client, then it will not send `OC-Message-Priority` to PCRF Core service.

If the priority AVP is not provided in the request, then the message priority that is either configured in the Advanced Settings of PCRF Core service or default priority values will be considered.

Table 4-85 Configuring Message Priority

Key	Default Value	Description
CONGESTION.USE.EXPERIMENTAL.RESULT.CODE	false	To set if user wants to use experimental result code when rejecting diameter messages. Allowed values are true or false. By default it will be false.
CONGESTION.VENDOR.ID	0	To set the vendor id when user wants to send experimental response code. To use experimental result code, set `CONGESTION.USE.EXPERIMENTAL.RESULT.CODE` as true, and set `CONGESTION.VENDOR.ID` as non-zero positive integer.
CONGESTION.DIAMETER.RESPONSE.CODE	3004	To set response code when rejecting diameter messages. Only valid 3xxx, 4xxx, 5xxx response codes are allowed.
GX.CREATE.REQUEST.PRIORITY	24	Set message priority for Diameter message Gx CCR-I. **Allowed Values**: 0-100
GX.MODIFY.REQUEST.PRIORITY	18	Set message priority for Diameter message Gx CCR-U. **Allowed Values**: 0-100
GX.DELETE.REQUEST.PRIORITY	16	Set message priority for Diameter message Gx CCR-T. **Allowed Values**: 0-100
RX.CREATE.REQUEST.PRIORITY	24	Set message priority for Diameter message Rx AAR-I. **Allowed Values**: 0-100
RX.MODIFY.REQUEST.PRIORITY	18	Set message priority for Diameter message Rx AAR-U. **Allowed Values**: 0-100
RX.DELETE.REQUEST.PRIORITY	16	Set message priority for Diameter message Rx STR. **Allowed Values**: 0-100
SD.MODIFY.REQUEST.PRIORITY	18	Set message priority for Diameter message Sd CCR-U. **Allowed Values**: 0-100
SD.DELETE.REQUEST.PRIORITY	16	Set message priority for Diameter message Sd CCR-T. **Allowed Values**: 0-100

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Currently Diameter Gateway sends `OC-Message-Priority` AVP only when it receives Diameter Routing Message Priority (DRMP) AVP. During PCRF Core pod in congestion state, if Diameter messages received do not have DRMP AVP, then either the configured or default message priority will be considered based on the AppId, CmdCode and RequestType. Due to all these considerations, Pcrf-core may reject requests for APNs and Service-URNs for emergency calls, MCPTT calls, and other special session requests.

Congestion Response Code

You can also configure the result codes for the rejected requests when configuring the load rules. By default, PCRF Core service sends 503 as response code. You can configure the response code using PCRF service advanced settings key `CONGESTION.HTTP.RESPONSE.CODE` in CNC Console. This key is used to configure the response code of the HTTP messages that are rejected by the PCRF service due to pod's congestion state. The configurable response code could be set to 1xx, or 3xx, or 4xx, or 5xx response code.

For Diameter requests, the PCRF Core discards the requests with default `3004 DIAMETER_TOO_BUSY`. You can configure the response code using PCRF service advanced settings key `CONGESTION_DIAMETER_RESPONSE_CODE` in CNC Console. The configurable response code could be set to either `3xxx`, `4xxx`, or `5xxx` response code.

For more information about the advanced keys in PCRF Core service, see Settings menu in CNC Console.

For more information about different response codes that can be configured, see Congestion Control Discard Message Response Code section.

Example for Congestion Control Call Flow/Scenario

For the below call flows, consider the following load shedding rule configuration:

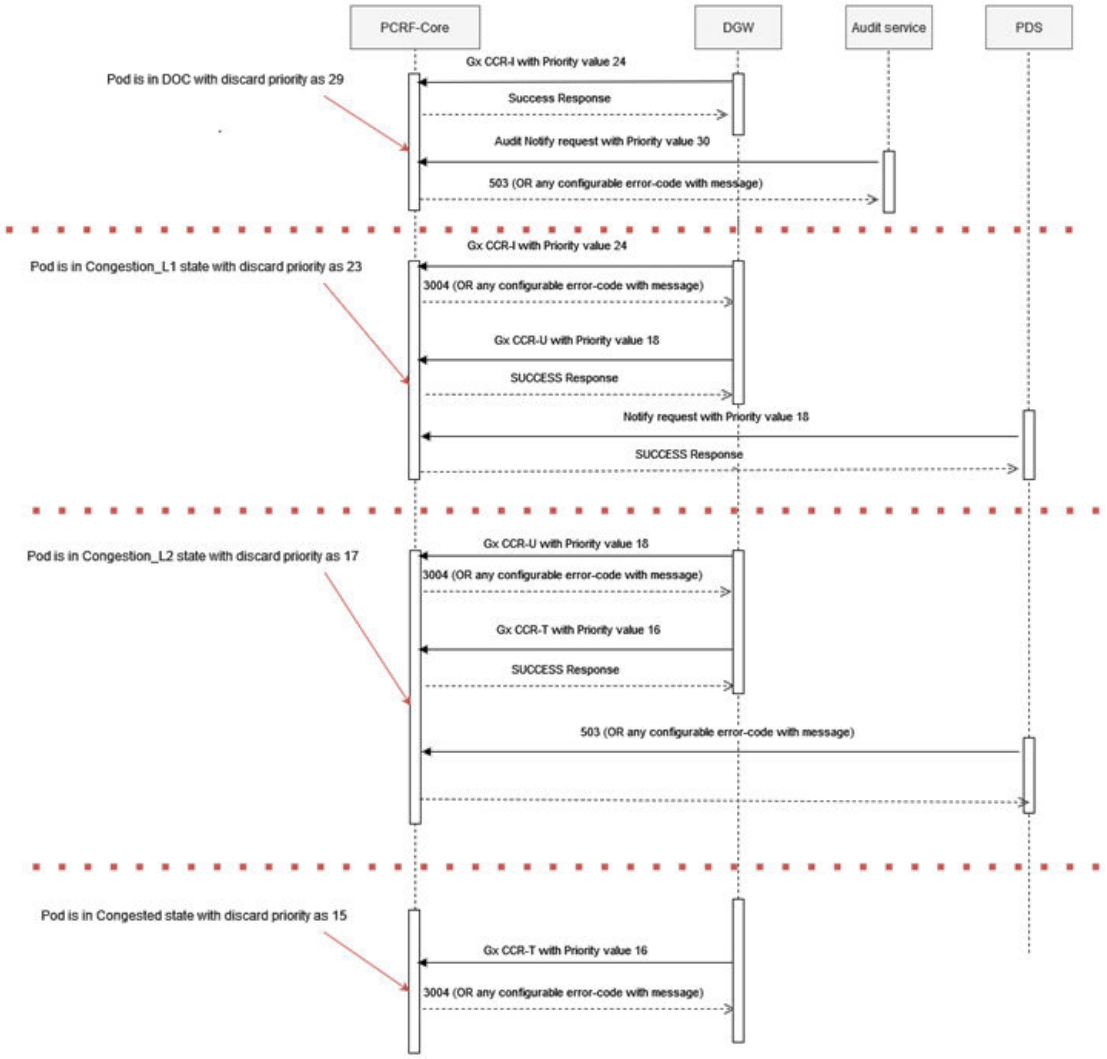
Table 4-86 Load Shedding Rule

Congestion State	Discard Priority
DOC	29
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

The call flow describes the PCRF Core service congestion control mechanism handling the requests from the other Policy services such as Diameter Gateway, PDS and Audit services when its Pod exists in different congestion state.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-96 PCRF Core Service Congestion Control Call Flow



PCRF Core pod is in DOC state and the discard priority is configured as 29:

- Diameter Gateway service sends a Gx CCR-I request with discard priority value set to 24 toward PCRF service.
- PCRF Core service responds with a success status.
- Audit service sends a notification request with discard priority value set to 30 toward PCRF service.
- PCRF Core service responds with a reject 503 status or with any configured error code and message.

PCRF Core pod is in Congestion_L1 state and the discard priority is configured as 23:

- Diameter Gateway service sends a Gx CCR-I request with discard priority value set to 24 toward PCRF service.
- PCRF Core service responds with a reject 3004 status or with any configured error code and message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Diameter Gateway service sends a Gx CCR-U request with discard priority value set to 18 toward PCRF service.
- PCRF Core service responds with a success status.
- PDS service sends a notification request with discard priority value set to 18 toward PCRF service.
- PCRF Core service responds with a success status.

PCRF Core pod is in Congestion_L2 state and the discard priority is configured as 17:

- Diameter Gateway service sends a Gx CCR-I request with discard priority value set to 24 toward PCRF service.
- PCRF Core service responds with a reject 3004 status or with any configured error code and message.
- Diameter Gateway service sends a Gx CCR-T request with discard priority value set to 16 toward PCRF service.
- PDS service responds with the success status.

PCRF Core pod is in Congested state and the discard priority is configured as 15:

- Diameter Gateway service sends a Gx CCR-T request with discard priority value set to 16 toward PCRF service.
- PCRF Core service responds with a reject 3004 status or with any configured error code and message.

Managing PCRF Core service Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for PCRF Core service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations**.

> **Note**
>
> - In a Policy fresh installation the CPU EMA ratio is set to 90:10.
> - When upgrading from 24.3.x to 25.1.200 or higher version then user has to update custom threshold profiles manually, by considering the default values as a reference. Also, it is recommended that user should set CPU EMA ratio as 90:10 in Congestion Control Settings.
> - When upgrading from versions lower than 24.3.0 to 25.1.200 or higher version, then the default profile will be activated and by default CPU EMA ratio will be set as 90:10 in Congestion Control Settings.
> - When exporting data from 24.3.x and importing it in 25.1.200 or higher version then user has to update the custom threshold profiles manually by considering the default values as a reference. Also, it is recommended that user should set CPU EMA ratio as 90:10 in Congestion Control Settings.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure PCRF service pod congestion control feature in CNC Console, see Congestion Control section.

To configure PCRF service pod congestion control discard messages in CNC Console, see the Advanced Settings section in Settings of PCRF Core service.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The following common service metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_congestion_http_pending_request_active_counter`

For information about the metrics, see Pod Congestion Metrics section.

The following PCRF Core service metrics are used to provide information about this feature:

- `occnp_http_congestion_message_reject_total`
- `occnp_diam_congestion_message_reject_total`
- `occnp_http_pending_requests`
- `occnp_diam_pending_requests`
- `occnp_congestion_diam_pending_request_active_counter`
- `occnp_congestion_diam_pending_request_end_to_end_id_map_size`
- `occnp_congestion_DiamMsgBuffer_queue_msg_count`

For information about the metrics, see PCRF Core Metrics section.

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED

Copyright © 2019, 2026, Oracle and/or its affiliates.

- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Maintain

Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support.

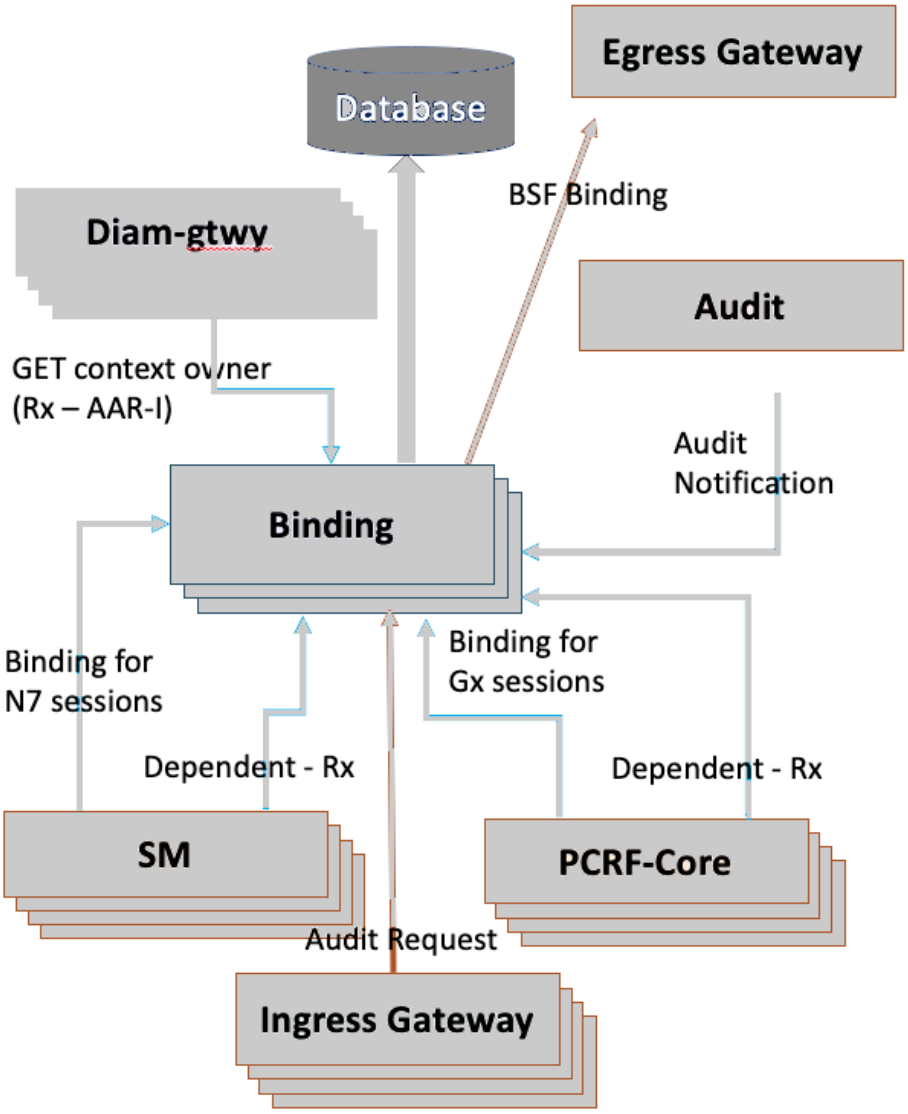
4.30.10 Binding Service Pod Congestion Control

Binding Service, a Policy microservice provides:

- session binding information on receiving binding request from SM service.
- subscriber/Data Network Name (DNN) session limit check across Gx and N7 session or within multiple sessions for a 4G/5G deployments.
- context owner information to Diameter Gateway for routing Rx messages for a 4G/5G deployments.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-97 Binding Service and Other Policy Services



The above diagram shows Binding service interaction with Policy SM, PCRF Core, cnDBTier, Audit, Diameter Gateway and Egress Gateway services. At times, an excessive traffic from these services can be observed in the network, which can result in a high CPU utilization, high memory utilization. This can cause performance degradation in Binding service responses and eventually reach a state of service unavailability. Congestion control is used in order to help in identifying such conditions and invoke rules that address these situations when these load conditions persist.

Pod Congestion Control Mechanism

The Pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Copyright © 2019, 2026, Oracle and/or its affiliates.

Determining Pod Congestion State

Binding service pods exist in any of the following five states at any given time:

- Normal
- Danger of Congestion (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

Figure 4-98 Different Pod Congestion States



Periodically, the state of the pod's congestion gets determined. This interval is configurable, and the default setting is 200 milliseconds.

The pod's state gets determined by considering the following points.

1. Calculate the congestion state for the following resources:
   a. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2 and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.
   b. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the Container (monitored using cgroup parameter - `cpuacct.usage` that provides current cpu usage in nanoseconds) with the configured threshold.
2. The congestion state for pod gets assigned a maximum congested state based on the congestion state of the resources.

The Binding service pod's can be in following Congestion states:

Table 4-87 Binding service Congestion States

Congestion States	CPU Count	Queue Count
DANGER_OF_CONGESTION (DOC)	70	120
CONGESTION_L1	75	150
CONGESTION_L2	80	180
CONGESTED	85	200

Triggering Pod Congestion Control

Every time Binding service receives requests from other services, it checks for the current congestion state of the pod. The Congestion Control mechanism is triggered if the pod's congestion state is in DOC or CONGESTION_L1 or CONGESTION_L2 or Congested.

The requests to the Binding service might have priority included as `oc-message-priority` attribute in the request header. The priority value ranges between 0 to 100 with 0 being the highest and 100 being the lowest priority.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Priority-Based Load Shedding

Based on the pods current congestion state a load shedding rule is applied to perform priority-based load shedding. The load shedding rule is based on message priority, for example, when the Binding service Pod state is CONGESTED, then discard messages with priority 30. It determines if the message with the assigned priority should be rejected or accepted.

The user can configure load shedding rule for Binding service by providing the discard priority for each of the congestion state. If not, a default load shedding rule is active, and messages are discarded based on it. The user can configure the result codes for the rejected requests when configuring the load rules. The default result code is `503 Service Unavailable` for HTTP messages.

The default load shedding rules for Binding service:

```
- state: DANGER_OF_CONGESTION
      discardPriority: 30
- state: CONGESTION_L1
      discardPriority: 27
- state: CONGESTION_L2
      discardPriority: 24
- state: CONGESTED
      discardPriority: 20
```

When Binding service is in congestion state, it's response can be configured using Binding service Advanced settings in CNC Console, using the key CONGESTION_RESPONSE_CODE. This key is used to configure for response code of the messages that is rejected by the Binding service due to pod congestion state. By default Binding Service responds with a response code of 503. The user can configure this parameter with either 1xx, 3xx, 4xx, or 5xx response codes. Following are the list of configurable keys that can be added to set the message priority:

Table 4-88 Configuring Message Priority

Key	Default Value	Allowed Values
AUDIT_MESSAGE_PRIORITY	30	0-100
BSF_AUDIT_MESSAGE_PRIORITY	27	0-100
DEPENDENT_CONTEXT_BINDING_REGISTER_MESSAGE_PRIORITY	24	0-100
DEPENDENT_CONTEXT_BINDING_DEREGISTER_MESSAGE_PRIORITY	16	0-100
DEPENDENT_CONTEXT_BINDING_FIND_CONTEXT_OWNER_MESSAGE_PRIORITY	16	0-100
SESSION_BINDING_REGISTER_MESSAGE_PRIORITY	24	0-100
SESSION_BINDING_UPDATE_MESSAGE_PRIORITY	20	0-100
SESSION_BINDING_DEREGISTER_MESSAGE_PRIORITY	16	0-100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-88 (Cont.) Configuring Message Priority

Key	Default Value	Allowed Values
SESSION_BINDING_SEARCH_MESSAGE_PRIORITY	30	0-100
SESSION_BINDING_FIND_CONTEXT_OWNER_MESSAGE_PRIORITY	16	0-100
SESSION_BINDING_CLEANUP_MESSAGE_PRIORITY	30	0-100
BSF_SESSION_UPDATE_MESSAGE_PRIORITY	20	0-100
STALE_SESSION_TRACKER_REFRESH_MESSAGE_PRIORITY	30	0-100

Note

- When upgrading from 24.1.x to 24.2.x or higher version then user has to update custom Threshold profiles manually, by taking new default values as a reference. When upgrading from versions lower than 24.1.0 to 24.2.x or higher version then the DEFAULT profile will be activated with new values.
- When exporting data from 24.1.x and importing it in 24.2.x or higher version then user has to update the custom Threshold profiles value manually by taking new default values as a reference before import.

Congestion Control Call Flow/Scenario

For the below call flows, consider the following Load shedding rule configuration:

Table 4-89 Load Shedding Rule

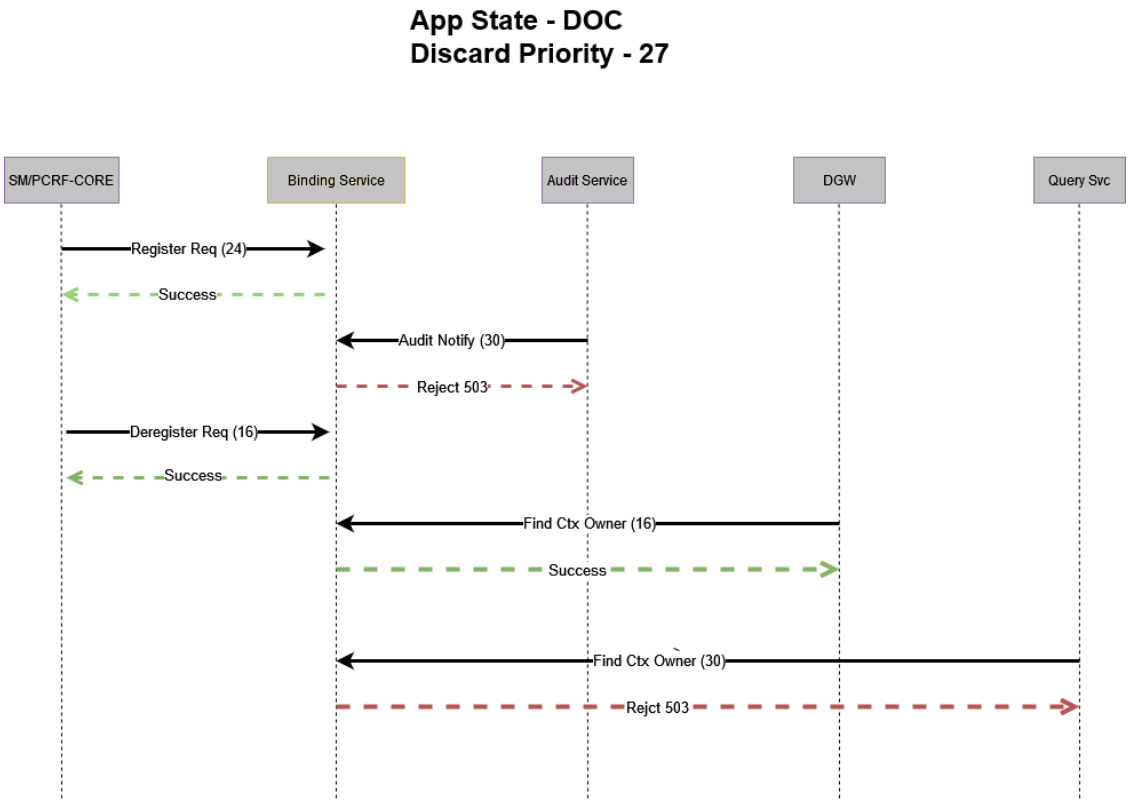
Congestion State	Discard Priority
DOC	27
CONGESTION_L1	23
CONGESTION_L2	18
CONGESTED	10

Binding Service Call Flow in Doc State

The call flow describes the Binding service congestion control mechanism handling the requests from the other Policy services such as SM/PCRF core, Audit, Diameter Gateway, and Query services when it is in Danger of Congestion (DOC) state.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-99 Binding Service Pod in DOC State



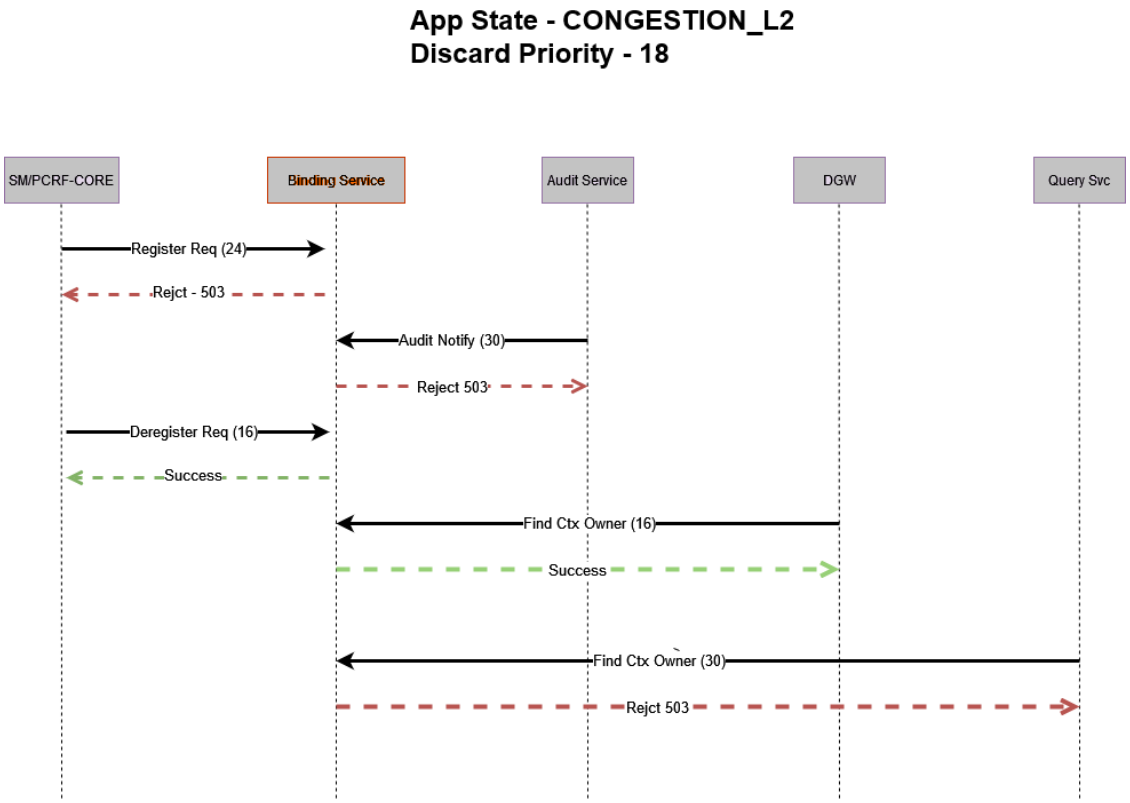
- SM/PCRF-Core services sends a register request with discard priority set to 24 to Binding service and it responds back with success status.
- Audit service sends a audit notification request with discard priority set to 30 to Binding service and it responds back with a reject 503 status.
- SM service sends a de-register request with discard priority set to 16 to Binding service and it responds back with success status.
- Diameter Gateway service sends a find context owner request with discard priority set to 16 to Binding service and it responds with a success status.
- Query Gateway service sends a find context owner request with discard priority set to 30 to Binding service and it responds back with a reject 503 status.

Binding Service Call Flow in Congestion_L2 State

The call flow describes the Binding service congestion control mechanism handling the requests from the other Policy services such as SM/PCRF core, Audit, Diameter Gateway, and Query services when it is in Congestion_L2 state.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-100 Binding Service in Congestion_L2 State



- SM/PCRF-Core service sends a register request with discard priority set to 24 to Binding service and it responds back with a reject 503 status.
- Audit service sends a audit notification request with discard priority set to 30 to Binding service and it responds back the a reject 503 status.
- SM service sends a de-register request with discard priority set to 16 to Binding service and it responds back with success status.
- Diameter Gateway service sends a find context owner request with discard priority set to 16 to Binding service and it responds back with success status.
- Query Gateway service sends a find context owner request with discard priority set to 30 to Binding service and it responds back with a reject 503 status.

The following points needs to be known while assigning request or message priority to an request API:

- For requests coming from Diameter Gateway, the requests priority number is retrieved from *oc-message-priority* parameter in the http request header. But if this request header parameter is not present or its value is not set, then the message priority shall be based on the configured values from Advanced Settings or Default priority values.
- For requests coming from Ingress Gateway, the priority is based on *3gpp-sbi-message-priority* parameter in http request header. But if this request header parameter is not present or its value is not set, then the priority shall be based on configured values from Advanced Settings or on the default priority values.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- The request priority value ranges between 0 to 100, with 0 being the highest, and 100 being the lowest priority. If an invalid value is provided, then the default priority shall be considered.

Thus the precedence order for assigning message priority shall be from `oc-message-priority → 3gpp-sbi-message-priority → Advanced Settings Priority → Default Priority`.

Managing Binding service Pod Congestion Control

Enable

By default, the Pod Congestion control is disabled for Binding service. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable the feature using CNC Console set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations**.

Perform the Binding service Congestion Control feature configurations on the Settings, Threshold and Load Shedding Rules in CNC Console as described in Congestion Control section.

Perform the Binding service Congestion Control feature discard message configurations at Advanced Settings in CNC Console as described in Binding Service section.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

Following metrics were updated in the Pod Congestion Metrics section.

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_http_congestion_message_reject_total`

Alerts

The following alerts generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1

Copyright © 2019, 2026, Oracle and/or its affiliates.

- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

For more information about alerts, see Common Alerts.

Maintain

Error logs are generated when the system is congested and the actions are taken to bring the system back to normal. Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support.

4.30.11 Bulwark Pod Congestion Control

Bulwark, a Policy microservice provides distributed lock mechanism using distributed coherence. It handles concurrent transactions across consumer services. Since the lock is distributed, the deployed pods request a lock for a resource based on a unique identifier in the global system rather than acquiring a lock locally in a single pod.

The traffic at Bulwark service is high as all the consumer services use its distributed lock mechanism to handle concurrent transactions. In the production environment, the Bulwark pods must be protected from traffic congestion. Bulwark pod congestion control functionality helps in regulating the traffic and improves its service availability. The Pod congestion control mechanism is designed to identify congestion conditions and apply load shedding rules to maintain optimal service levels.

The Bulwark service receives every incoming requests, the congestion control mechanism decides to either accept or reject the request based on pods congestion state defined request priority. It invokes the load shedding rules when congestion state persist in the pods. The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

In congestion control mechanism different congestion levels are defined, each level indicates how congested the pod is, and which requests can be served when pod is on certain congestion level. The congestion control works at following five congestion levels or states:

1. Normal
2. Danger of Congestion (DOC)
3. CONGESTION_L1
4. CONGESTION_L2

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. Congested

Each pod monitors its congestion state. The pod's congestion state is decided based on CPU consumption and Queue.

The pod's state gets determined by considering the following points.

1. **CPU** - The CPU usage for congestion state is calculated by comparing the CPU usage of the Container (monitored using cgroup parameter - `cpuacct.usage` that provides current cpu usage in nanoseconds) with the configured threshold. The following formula calculates the CPU usage:

$$\frac{\frac{CurrentCpuUsage - LastCpuUsage}{CurrentTime - LastSampleTime} * 100}{CPUs}$$

2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

To avoid toggling between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. The below configurations are used to define the period that the pod has to be in a particular state for:

- **stateChangeSampleCount**: This parameter can be configured to specify after how many continuous intervals, the pod state can be changed. The default value is 5. This value can range from 1 to 2147483647.
- **stateCalculationInterval**: This parameter can be configured to specify the time duration or interval, after which the pod congestion state will be re-verified. The default value is 200ms. This interval is configured in milliseconds and can range from 50 to 2147483647.

For more information about these congestion control configurations, see Congestion Control Settings section in CNC Console.

CPU and Queue Threshold

The pod's state changes when its resources, namely the CPU and Queue buffer usage exceeds the predefined congestion threshold, checked at regular intervals. An active CPU and Queue default threshold profile can be viewed using CNC Console at *Policy → Overload and Congestion Control → Congestion Control → Thresholds* section. The user can create new threshold profile and make it active. The CPU and Queue threshold should be added in the order of DOC → Congestion_L1 → Congestion_L2 → Congested states. The Bulwark service pod's different congestion states and their default congestion parameters, CPU, and Queue pending counts are provided in the following table:

Table 4-90 Bulwark Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
DANGER_OF_CONGESTION (DOC)	60	6300
CONGESTION_L1	70	7200
CONGESTION_L2	80	8100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-90 (Cont.) Bulwark Service Congestion States

Congestion States	CPU (%)	Queue Count (Pending Requests)
CONGESTED	90	9000

For more information about these CPU and Queue count thresholds configurations, see Congestion Control Thresholds section in CNC Console.

Triggering Congestion Control

With Congestion Control feature enabled for Bulwark service, every time a message is fetched for processing, the system checks the current congestion state of the pod. If the current state is either in `DOC`, `CONGESTION_L1`, `CONGESTION_L2`, or `Congested` state, then the congestion control mechanism is triggered. After verifying that the message type is a request, a request priority is assigned to it. If the request priority is greater than or equal to the discard priority, then the message is rejected, otherwise it is accepted.

Congestion Control Load Shedding using Discard and Request Priority

Bulwark pods performs load shedding by considering the load rule configured for the current congestion state. The load shedding rule is based on message priority configuration. A default load shedding rule is active and the messages are discarded based on it. You can create new load rules using the Overload and Congestion Control menu in CNC Console and make it active. The discard priorities should be added in the order of DOC → Congestion_L1 → Congestion_L2 → Congested states.

Table 4-91 Priority based Message Discards

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	27
CONGESTION_L1	19
CONGESTION_L2	17
CONGESTED	15

For more information about these `Priority` discards configurations, see Congestion Control Load Shedding Profiles page in CNC Console.

SM Service Supporting the Priority Header for Lock and Unlock requests

SM service supports bulwark congestion control by adding the priority attribute `oc-message-priority` in the lock/unlock requests header. The 3gpp-Sbi-Message-Priority header is used to specify the message priority for 3GPP service based interfaces. This header is included in messages when a priority for the message must be conveyed. By default the oc-message-priority uses the 3gpp-Sbi-Message-Priority value to evaluate message priority. Requests without 3gpp-Sbi-Message-Priority header are assigned default values. If the user wants to assign a different priority to the response message than the default ones, this can be configured using the Advanced settings of SM service in the CNC Console. Following are the advanced setting configurable parameters:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-92 SM Service Request Default Priorities

Advanced Settings Key	Value	Message Type
REQUEST_PRIORITY_FOR_SM_CREATE	24	Create
REQUEST_PRIORITY_FOR_SM_UPDATE	18	Update
REQUEST_PRIORITY_FOR_SM_UPDATE_NOTIFY	18	Update Notify
REQUEST_PRIORITY_FOR_SM_DELETE	16	Delete
REQUEST_PRIORITY_FOR_SM_CLEANUP	18	Cleanup
USE_TGPP_SBI_MSG_PRIORITY	true	Set this to false, if the SM service does not want to consider the 3gpp-Sbi-Message-Priority value for `oc-message-priority`.

Congestion Response Code

You can also configure the result codes for the rejected requests when configuring the load rules. By default, Bulwark service sends 503 as response code. You can configure the response code and cause by adding Advance Settings key and value at Bulwark Settings page in CNC Console. The following are the advances settings key and value:

Table 4-93 Advance Setting

Key	Value	Description
CONGESTION_RESPONSE_CODE	503	This is to configure the bulwark result code for the congestion control discards and its value shall be numerical. The value can be set to either 1xx, 3xx, 4xx, or 5xx response codes. If this value is not configured, then default congestion result code shall be *503*. **Default Value**: 503

When Bulwark pod is in congestion state, the response code for the rejected requests can be configured using the `responseCode` Helm parameter in the `values.yaml` file. By default, the `responseCode` parameter for Bulwark service is set to `503 Service Unavailable` response code. The user can configure this parameter with either 1xx, 3xx, 4xx, or 5xx response codes.

Sample Helm Configuration for Bulwark Service:

```
congestion:
     responseCode: 503
```

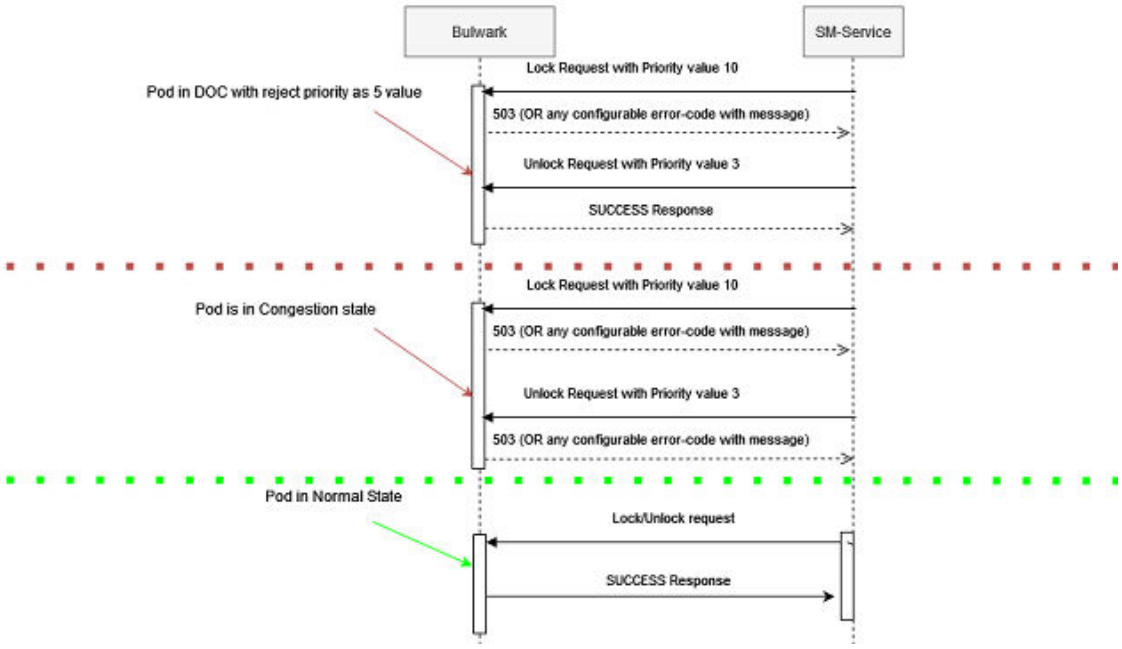
For more information about different response codes that can be configured, see Congestion Control Discard Message Response Code section.

Call Flow

Below diagram shows the call flow for SM service supporting the priority header functionality for the 5 states of congestion, namely, `Danger of Congestion`, `Congestion_L1`, `Congestion_L2`, and `Congested`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-101 Call Flow Diagram for Bulwark Congestion Control



- Bulwark receives an SM service lock request with priority set to 10 when it is in the DOC state with the reject priority set to 5. On comparing both priorities, bulwark rejects the message with result code since the message priority value is higher than the reject priority. The message returns with result code `503 Service unavailable` or any configurable error code with message.
- Bulwark receives an SM service unlock request with priority set to 3 when it is in the DOC state with the reject priority set to 5. On comparing both priorities, bulwark accepts the message with result code `Success` since the message priority value is lower than the reject priority.
- Bulwark receives an SM service lock request with priority set to 10 when it is in the CONGESTED state with reject priority set to 1. On comparing both priorities, bulwark rejects the message with result code since the message priority value is higher than the reject priority. The message returns with result code `503 Service unavailable` or any configurable error code with message.
- Bulwark receives an SM service unlock request with priority set to 5 when it is in the CONGESTED state with reject priority set to 1. On comparing both priorities, bulwark rejects the message with result code since the message priority value is higher than the reject priority. The message returns with result code `503 Service unavailable` or any configurable error code with message.
- Bulwark receives an SM service lock or unlock request when it is in the NORMAL state. Bulwark accepts the message with result code `Success` since the requests do not have priority value set.

Feature Upgrade Impact

With upgrade of Policy application from any of the previous release versions to 25.1.200, the Bulwark pod Congestion Control feature can be updated to use the common Congestion Control mechanism available in 25.1.200. In order to do this, there are some considerations to address, especially due to the difference in configuration data. Bulwark service pod congestion control configurations from the previous version should be migrated to use the current version

Copyright © 2019, 2026, Oracle and/or its affiliates.

configurations. The data migration process is manual and one-time activity that user has to perform, by using either the CNC Console or Congestion Control migration APIs.

Feature Transition

Bulwark Pod Congestion Control feature transition between older version to the Policy 25.1.200 Congestion Control mechanism is based on migration status of the Policy application after the upgrade. The migration status can be either in "Before Migration" or "After Migration".

False (Before Migration): After upgrading to Policy version 25.1.200, the Bulwark pod congestion control feature still operates under the configurations and designs of the pre-upgrade version until the user actively migrates the setup. In this "False" state, the users will only see:

- Old Configurations: The Bulwark Congestion Control configurations from the previous application version.
- Previous CNC Console pages: User will have access to the older user interface rather than the new screen designed for Congestion Control feature.
- Legacy REST APIs: Calls to APIs will still work with the previous version's endpoints.

To enable the common Congestion Control mechanism for Bulwark service, users will need to complete the data migration process.

True (After Migration): After the upgrade to Policy version 25.1.200, perform the data migration for Bulwark pod Congestion Control feature. With this, the migration status will be "True" and Bulwark services can use the updated Congestion Control mechanisms.

For more information related to Congestion Control configuration migration, see "Migration of Bulwark Service Congestion Control Configurations" section in Congestion Control Settings page in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

When Policy 25.1.200 or any of the later versions is fresh installed or when Policy is upgraded from any of the previous versions to Policy 25.1.200 or later versions, after the Bulwark congestion migration is completed, the updated Congestion Control REST API does not accept the configuration of `activeThresholdProfile` parameter in the request body. This is inline with all services congestion control behaviour.

Sample REST API:

```
Method: PUT
URL: ../oc-cnpolicy-configuration/v1/congestionConfigurations/bulwark
Header:
  Content-Type: application/json
  Accept: application/json
Body:
{
 "enable":true,
 "stateChangeSampleCount":5,
 "stateCalculationInterval":5000
}
```

When Policy is upgraded from any of the previous versions to 25.1.200 or later versions, before the Bulwark congestion migration completed, the updated Congestion Control REST API accepts the `activeThresholdProfile` parameter in the Request Body as this is old Bulwark congestion behaviour and is not inline with all services congestion control behaviour.

Sample REST API:

```
Method: PUT
URL: ../oc-cnpolicy-configuration/v1/congestionConfigurations/bulwark
Header:
  Content-Type: application/json
  Accept: application/json
Body:
{
 "activeThresholdProfile":"DEFAULT",
 "enable":true,
 "stateChangeSampleCount":5,
 "stateCalculationInterval":5000
}
```

Managing Bulwark Pod Congestion Control

Enable

By default, the Pod Congestion control is disabled for Bulwark service. You can enable this feature using CNC Console or REST API for Policy.

Feature Migration

If the Policy application is upgraded to 25.1.200, then you can enable this feature by performing the migration process. For more information how to perform the data migration, see

Copyright © 2019, 2026, Oracle and/or its affiliates.

"Migration of Congestion Control Configuration Data" section in Congestion Control Settings page using CNC Console.

Configure

You can customize the configurations related to this feature using the CNC Console or REST APIs for Policy:

- **Configure using CNC Console:**
  To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations** for Bulwark Service.

  To configure Bulwark service pod congestion control feature in CNC Console, see Congestion Control section.
- **Configure using REST API:**
  To enable this feature using REST API, perform the feature configurations as described in "Congestion Control" APIs section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

  If the Policy application is upgraded to 25.1.200, then you can enable this feature by performing the migration process. For more information how to perform the data migration using Congestion Control Migration APIs, see "Congestion Migration" APIs section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

Following metrics were updated in the Pod Congestion Metrics section.

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_congestion_http_pending_request_active_counter`
- `occnp_http_congestion_message_reject_total`

> **Note**
>
> Prometheus automatically injects name of the pod with label name "kubernetes_pod_name" to the metric. This information is further used for alerting purposes.

Alerts:

Following alerts are used by this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION

Copyright © 2019, 2026, Oracle and/or its affiliates.

- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

Maintain

Error logs are generated when the system is congested and the actions taken to bring the system back to normal. Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support for more information on how to raise a service request.

4.30.12 Congestion Control Discard Message Response Code

In Congestion Control mechanism, on Pod being in any of the congested states the messages are discarded based on the message priority. The discarded messages responses can have customized error response. In Policy application, the services supporting the Congestion Control mechanism can configure the discarded messages error response in their service specific Advanced Settings page in CNC Console.

The following table lists the supported HTTP response code:

Table 4-94 Supported HTTP Response Codes

Series	Code	Cause	Type
1xx	101	Continue	INFORMATIONAL
1xx	102	Switching Protocols	INFORMATIONAL
1xx	103	Processing	INFORMATIONAL
1xx	104	Early Hints	INFORMATIONAL
3xx	300	Multiple Choices	REDIRECTION
3xx	301	Moved Permanently	REDIRECTION
3xx	302	Found	REDIRECTION
3xx	303	See Other	REDIRECTION
3xx	304	Not Modified	REDIRECTION
3xx	305	Use Proxy	REDIRECTION
3xx	307	Temporary Redirect	REDIRECTION
3xx	308	Permanent Redirect	REDIRECTION

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-94 (Cont.) Supported HTTP Response Codes

Series	Code	Cause	Type
4xx	400	Bad Request	CLIENT_ERROR
4xx	401	Unauthorized	CLIENT_ERROR
4xx	402	Payment Required	CLIENT_ERROR
4xx	403	Forbidden	CLIENT_ERROR
4xx	404	Not Found	CLIENT_ERROR
4xx	405	Method Not Allowed	CLIENT_ERROR
4xx	406	Not Acceptable	CLIENT_ERROR
4xx	407	Proxy Authentication Required	CLIENT_ERROR
4xx	408	Request Timeout	CLIENT_ERROR
4xx	409	Conflict	CLIENT_ERROR
4xx	410	Gone	CLIENT_ERROR
4xx	411	Length Required	CLIENT_ERROR
4xx	412	Precondition Failed	CLIENT_ERROR
4xx	413	Payload Too Large	CLIENT_ERROR
4xx	414	URI Too Long	CLIENT_ERROR
4xx	415	Unsupported Media Type	CLIENT_ERROR
4xx	416	Requested range not satisfiable	CLIENT_ERROR
4xx	417	Expectation Failed	CLIENT_ERROR
4xx	418	I'm a teapot	CLIENT_ERROR
4xx	419	Insufficient Space On Resource	CLIENT_ERROR
4xx	420	Method Failure	CLIENT_ERROR
4xx	421	Destination Locked	CLIENT_ERROR
4xx	422	Unprocessable Entity	CLIENT_ERROR
4xx	423	Locked	CLIENT_ERROR
4xx	424	Failed Dependency	CLIENT_ERROR
4xx	425	Too Early	CLIENT_ERROR
4xx	426	Upgrade Required	CLIENT_ERROR
4xx	428	Precondition Required	CLIENT_ERROR
4xx	429	Too Many Requests	CLIENT_ERROR
4xx	431	Request Header Fields Too Large	CLIENT_ERROR
4xx	451	Unavailable For Legal Reasons	CLIENT_ERROR
5xx	500	Internal Server Error	SERVER_ERROR
5xx	501	Not Implemented	SERVER_ERROR
5xx	502	Bad Gateway	SERVER_ERROR
5xx	503	Service Unavailable	SERVER_ERROR
5xx	504	Gateway Timeout	SERVER_ERROR
5xx	505	HTTP Version not supported	SERVER_ERROR
5xx	506	Variant Also Negotiates	SERVER_ERROR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-94 (Cont.) Supported HTTP Response Codes

Series	Code	Cause	Type
5xx	507	Insufficient Storage	SERVER_ERROR
5xx	508	Loop Detected	SERVER_ERROR
5xx	509	Bandwidth Limit Exceeded	SERVER_ERROR
5xx	510	Not Extended	SERVER_ERROR
5xx	511	Network Authentication Required	SERVER_ERROR

> **Note**
>
> If the congestion response code other than above supported HTTP response codes is configured, then the default response code 503 shall be assigned and below log message will be logged:
> `Log line => Exception occurred: No matching constant for '512' Rejecting request with default response code: 503.`

The following table lists the supported Diameter result codes:

Table 4-95 Supported Diameter Result Codes

Series	Code	Name
3xxx	3001	DIAMETER_COMMAND_UNSUPPORTED
3xxx	3002	DIAMETER_UNABLE_TO_DELIVER
3xxx	3003	DIAMETER_REALM_NOT_SERVED
3xxx	3004	DIAMETER_TOO_BUSY
3xxx	3005	DIAMETER_LOOP_DETECTED
3xxx	3006	DIAMETER_REDIRECT_INDICATION
3xxx	3007	DIAMETER_APPLICATION_UNSUPPORTED
3xxx	3008	DIAMETER_INVALID_HDR_BITS
3xxx	3009	DIAMETER_INVALID_AVP_BITS
3xxx	3010	DIAMETER_UNKNOWN_PEER
4xxx	4001	DIAMETER_AUTHENTICATION_REJECTED
4xxx	4002	DIAMETER_OUT_OF_SPACE
4xxx	4003	ELECTION_LOST
4xxx	4010	DIAMETER_END_USER_SERVICE_DENIED
4xxx	4011	DIAMETER_CREDIT_CONTROL_NOT_APPLICABLE

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-95 (Cont.) Supported Diameter Result Codes

Series	Code	Name
4xxx	4012	DIAMETER_CREDIT_LIMIT_REACHED
4xxx	4999	SPLIT_BRAIN_SUSPECTED
5xxx	5001	DIAMETER_AVP_UNSUPPORTED
5xxx	5003	DIAMETER_AUTHORIZATION_REJECTED
5xxx	5004	DIAMETER_INVALID_AVP_VALUE
5xxx	5005	DIAMETER_MISSING_AVP
5xxx	5006	DIAMETER_RESOURCES_EXCEEDED
5xxx	5007	DIAMETER_RESOURCES_EXCEEDED
5xxx	5008	DIAMETER_AVP_NOT_ALLOWED
5xxx	5009	DIAMETER_AVP_OCCURS_TOO_MANY_TIMES
5xxx	5010	DIAMETER_NO_COMMON_APPLICATION
5xxx	5011	DIAMETER_UNSUPPORTED_VERSION
5xxx	5012	DIAMETER_UNABLE_TO_COMPLY
5xxx	5013	DIAMETER_INVALID_BIT_IN_HEADER
5xxx	5014	DIAMETER_INVALID_AVP_LENGTH
5xxx	5015	DIAMETER_INVALID_MESSAGE_LENGTH
5xxx	5016	DIAMETER_INVALID_AVP_BIT_COMBO
5xxx	5017	DIAMETER_NO_COMMON_SECURITY
5xxx	5030	DIAMETER_USER_UNKNOWN
5xxx	5031	DIAMETER_RATING_FAILED
5xxx	5032	DIAMETER_ERROR_BYTEME

Note

If the congestion response code other than the above supported diameter result codes is configured, then the default response code `3004` shall be assigned, and below logs message will be logged:

```
Log line => Configured 1234: {} does not belongs to 3xxx, 4xxx or 5xxx
series. using default response code: 3004
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

The following table lists the supported Experimental result code:

Table 4-96 Experimental Result Codes

Series	Code	Name	Vendor Id	Vendor Name
5xxx	5011	DIAMETER_ERROR_FEATURE_UNSUPPORTED	10415	3GPP
5xxx	5997	NO_CAPACITY	21274	Tekelec
5xxx	5453	DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST	10415	3GPP
5xxx	5454	DIAMETER_ERROR_TIMED_OUT_REQUEST	10415	3GPP

4.31 Stale Binding Detection Audit, Report and Recover

While checking the validity of a binding record for a PDU Session in the backend core services, Binding service also verifies if the binding association for the PDU session exists in BSF. Existence of the binding association for the PDU session in BSF confirms the binding association being valid in BSF. If the binding association is missing in BSF, it is restored by validating the association in BSF.

> **Note**
>
> This functionality requires the audit service to be enabled for Binding service. Binding service does not revalidate the binding records reaching TTL expiry within TTL with BSF.

Session Binding Revalidation with BSF

During audit, Binding service verifies the staleness of the binding records of a PDU session from Policy microservices such as SM service. If the binding is valid, it revalidates the binding associations with BSF.

Binding service validates the staleness of the session in Policy microservices. If the session is valid, it revalidates the session binding in BSF.

During revalidation, if the following parameters in the request matches with the stored binding object in BSF, BSF considers it as duplicate and does not perform any database update:

- SUPI/GPSI
- UE IP(IPV4/IPV6),
- IPDomain(if IPV4 was present for UE IP)
- dnn
- snssai
- diamHost/fqdn
- pcfId

Copyright © 2019, 2026, Oracle and/or its affiliates.

If the parameters do not match, Binding service recreates a binding in BSF as it was originally registered, retaining all the headers and attributes with its values except for the Sender Timestamp header.

Restoring PCF Session Binding Association in BSF

During revalidation of the binding session in BSF, Binding Service sends the Binding Association Request as was sent originally, retaining all the headers and attributes with its values except for the Sender Timestamp header. To support the original headers and attributes, Binding service must retrieve the related HTTP headers from the payload object included in the stale session response from Policy microservices, and use them to populate the revalidation request header.

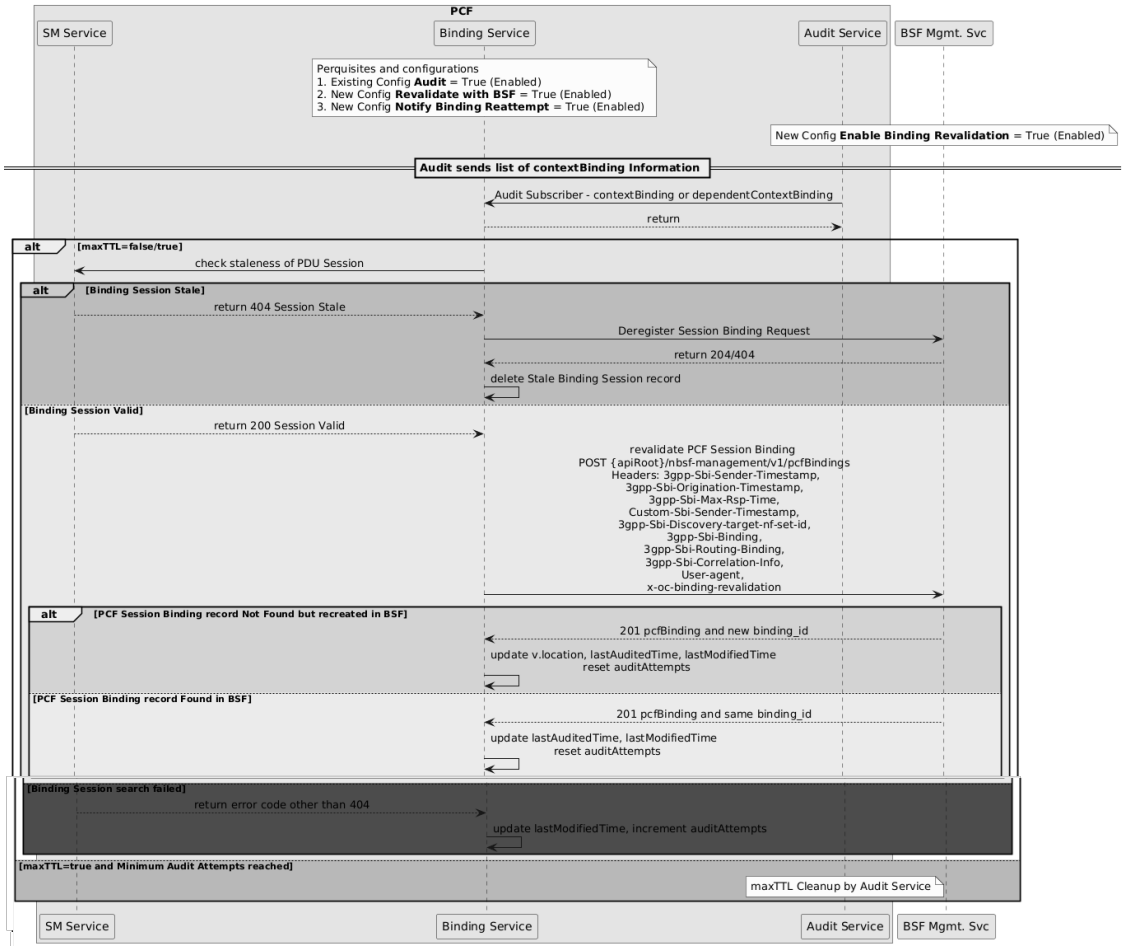
The successful (201) response from BSF includes a location HTTP header field that contains the URI of the created binding information. For example, "{apiRoot}/nbsf-management/v1/pcfBindings/{bindingId}" where {bindingId}" is the new binding identifier for the session. This URI is updated in contextbinding table in Policy.

Call Flow

The following diagram depicts a sample call flow for revalidating the binding information for an SM session with the following configured in Binding service:

- Audit is enabled
- Revalidate with BSF is enabled

Figure 4-102 Stale binding detection and revalidation



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Audit Service sends an audit notification for the contextbinding records in TTL expiry.
2. Binding service sends a request with contextId to SM service to check the staleness of the PDU session.
3. If SM service responds with 404 Session Stale indicating that the PDU session is stale, Binding service sends a request to BSF Management service to deregister the binding for the stale PDU session.
4. BSF Management session deletes the biding record for the stale PDU session and responds to Binding service.
5. Binding service deletes the corresponding information in its database as well.
6. If SM service responds with 200 valid session indicating that the PDU session is still valid, Binding service sends a revalidation request with binding request object in its request body to BSF Management service. It uses the REST API: POST {apiRoot}/nbsf-management/v1/pcfBindings to send the request.
7. BSF performs a lookup in pcf_binding table to search if it is a duplicate binding request. The matching criteria is: SUPI, UE IP(IPV4/IPV6), IPDomain(if IPV4 was present for UE IP), dnn and snssai.
8. If the duplicate binding is found for the same session, indicated by matching any one of pcfId, pcfFqdn, pcfDiamHost, pcfIpEndPoints from the request, BSF returns 201 with the same binding_id, If the duplicate binding is not found, BSF creates a new binding and return 201 with session binding info in the response body.
9. Binding Service receives the response from BSF and updates the binding record only with the new binding_id. Also it updates lastAuditedTime, lastModifiedTime and reset auditAttempts for the same record.
10. Binding Service updates and stores the 3gpp-sbi-target-apiroot header in contextbinding record, if received in revalidation response from BSF in indirect communication.

> **Note**
>
> **Enable Binding Revalidation** field under **BSF Management Service** in CNC Console for Binding Service must be enabled before or together with **Revalidate with BSF** fields under **Audit** section on **Binding Service** page in **Service Configurations** in CNC Console for Policy. Without enabling **Enable Binding Revalidation** in BSF will cause all revalidation requests to recreate a new binding association in BSF with a different `binding_id`.

Managing Stale Binding Detection Audit, Report and Recover

Enable

This feature can be enabled using CNC Console as well as REST API.

Enable using CNC Console

To enable this feature using CNC Console, use **Enable** and **Revalidate with BSF** fields under **Audit** section in **Binding Service** page for **Service Configurations** in CNC Console.

For more information, see Binding Service.

Also configure **Enable Binding Revalidation** field on **Management Service** page under **Service Configurations** in CNC Console for BSF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see *Management Service* section in *Oracle Commuications Cloud Native Core, Binding Support Function User Guide*.

Enable using REST API

To enable this feature using REST API, configure the `enable` and `revalidateEnable` parameters under `audit` section in `Binding service API`: `{apiRoot}/oc-cnpolicy-configuration/v1/services/binding`

For more information, see *Binding Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Also, configure `enableBindingRevalidation` parameter in BSF Management Service API: `{apiRoot}/oc-bsf-configuration/v1/services/managementservice`

For more information, see *Management Service* section in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*.

Configure

This feature requires configuring Binding Service in Policy as well as BSF Management Service in BSF.

This feature can be configured using CNC Console as well as REST API.

Configure using CNC Console

To configure the Binding Service in Policy, configure the fields under **Audit** section along with **SESSION_BINDING_REVALIDATION_MESSAGE_PRIORITY** advanced settings key on **Binding Service** page for **Service Configurations** in CNC Console for Poliocy.

For more information, see Binding Service.

Also configure **Enable Binding Revalidation** field on **Management Service** page under **Service Configurations** in CNC Console for BSF.

For more information, see *Management Service* section in *Oracle Commuications Cloud Native Core, Binding Support Function User Guide*.

Configure using REST API

Configure the parameters under **audit** section in Binding Service API: `{apiRoot}/oc-cnpolicy-configuration/v1/services/binding`.

For more information, see *Binding Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Also, configure the **EnableBindingrevalidate** parameter under Management Service API for BSF: `{apiRoot}/oc-bsf-configuration/v1/services/managementservice`.

For more information, see *Management Service* section in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*.

Observability

Metrics

The following Binding service metrics are used to monitor this feature in Policy:

- occnp_session_binding_revalidation_request_total
- occnp_session_binding_revalidation_response_total
- ocpm_egress_response_total (existing one)

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see Binding Service Metrics

The following BSF Management service metrics are used to monitor this feature in BSF:

- ocbsf_binding_revalidation_request_total
- ocbsf_binding_revalidation_response_total
- ocbsf_binding_revalidation_pcfBinding_missing_total

For more information, see *BSF Management Service* section under *BSF Metrics* in *Oracle Commuications Cloud Native Core, Binding Support Function User Guide*.

Alerts

The following Policy alerts are used for this feature:

- SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_CRITICAL_THRESHOLD
- SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MAJOR_THRESHOLD
- SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD
- SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_CRITICAL_THRESHOLD
- SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MAJOR_THRESHOLD
- SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MINOR_THRESHOLD

For more information, see Common Alerts

The following BSF alerts are used for this feature:

- BINDING_REVALIDATION_PCF_BINDING_MISSING_MINOR
- BINDING_REVALIDATION_PCF_BINDING_MISSING_MAJOR
- BINDING_REVALIDATION_PCF_BINDING_MISSING_CRITICAL

For more information, see *List of Alerts* in *Oracle Commuications Cloud Native Core, Binding Support Function User Guide*.

Logging

The following logs with a specific marker "marker":{"name":"BINDING"}, "Binding Audit:<additional log text>" are generated for this feature:

- If BSF returns 201 with new `binding_id`, it indicates that the missing binding was recreated in BSF. PCF updates its logs. The updated PCF logs include:
  - SUPI
  - DNN
  - S-NSSAI
  - UE-IP (IPv6/IPV4)
  - IPDomain if available
  - PCF FQDN
  - BSF Instance ID at “WARN” level
- If PCF can not reestablish BSF binding after all the session retries, PCF updates its logs. The updated logs include:

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - SUPI
  - DNN
  - S-NSSAI
  - UE-IP (IPv6/IPV4)
  - IPDomain if available
  - PCF FQDN
  - BSF Instance ID at “WARN” level
- If PCF can not reestablish BSF binding after all the reattempts of binding operation, PCF updates its logs. The updated logs include:
  - SUPI
  - DNN
  - S-NSSAI
  - UE-IP (IPv6/IPV4)
  - IPDomain if available
  - PCF FQDN
  - BSF Instance ID at “WARN” level
- If PCF internal Audit check (PDU Session revalidation on core services) of the binding association returns `404: NOT_FOUND`, PCF updates its logs. The updated logs include:
  - SUPI
  - DNN
  - S-NSSAI
  - UE-IP (IPv6/IPV4)
  - IPDomain if available
  - PCF FQDN
  - BSF Instance ID at “WARN” level
- For Revalidation request, if the response from BSF indicates that the binding association is not present in BSF, BSF updates its logs with the failure for the revalidation request. The updated logs include:
  - SUPI
  - DNN
  - S-NSSAI
  - UE-IP (IPv6/IPV4)
  - IPDomain if available
  - PCF FQDN
  - error code and cause at “WARN” level
- For Revalidation request, if BSF can not re-establish or restore the BSF binding after all session retries, BSF updates its logs with the failure for the restoration request.
  - SUPI
  - DNN

Copyright © 2019, 2026, Oracle and/or its affiliates.

- S-NSSAI
- UE-IP (IPv6/IPV4)
- IPDomain if available
- PCF FQDN
- error code and cause at “WARN” level

4.32 Congestion Control Resource Usage Calculation Using EMA Algorithm

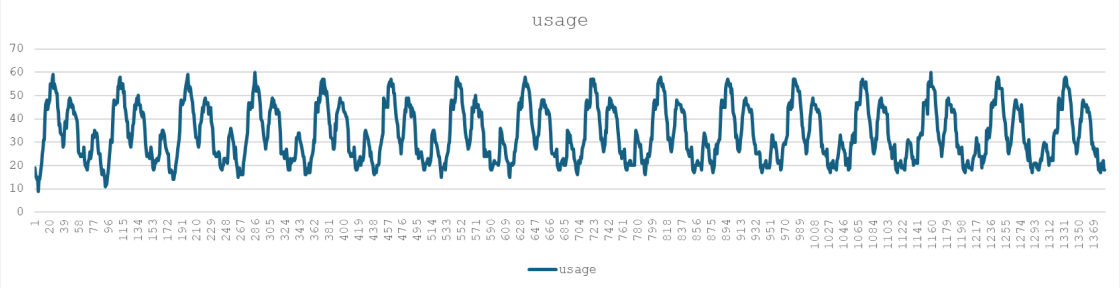
The Congestion Control mechanism used by different Policy services manages the flow of data traffic and prevent pod congestion. It monitors the system to detect situations that match conditions like high CPU usage or queue buffer congestion which can impact the performance under heavy loads.

The Congestion Control feature maintains two pod state, namely `NORMAL` or `CONGESTED(DANGER OF CONGESTION, CONGESTION_L1, CONGESTION_L2, CONGESTED)` state. A pod's state changes when its resource usage exceeds the predefined congestion threshold, checked at regular intervals. During uneven incoming traffic, the pods frequently switches states, leading to high volume of `WARN` level logs that complicates system monitoring.

The Congestion Control mechanism implements the Exponential Moving Average (EMA) algorithm for resource usage calculations, helping to smooth out rapid congestion state changes during fluctuating traffic. An EMA is a type of moving average (MA) that places a greater weight and significance on the most recent data points. It is also referred to as the Exponentially Weighted Moving Average (EWMA).

The EMA algorithm calculates the congestion resource usage by considering the resource consumption data over time, giving more weight to recent usage data, which provides a more accurate picture of current resource utilization compared to a simple average across all data points. This resource usage data is used for pod state change thus enabling smooth transition of congestion states during traffic spikes.

Figure 4-103 Sample Resource Usage Monitoring



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-104 Sample Resource Usage Monitoring using EMA

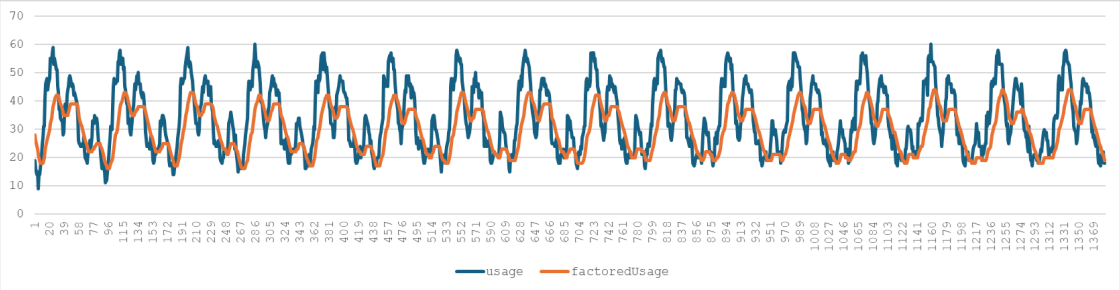


Figure 4-105 Another Sample Resource Usage Monitoring

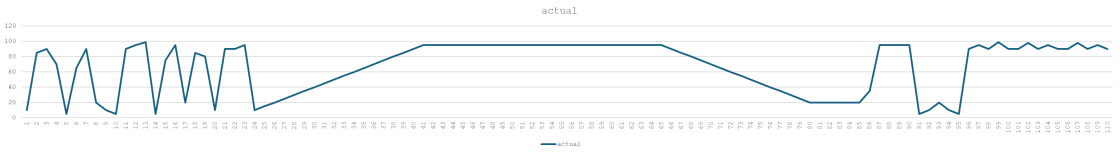
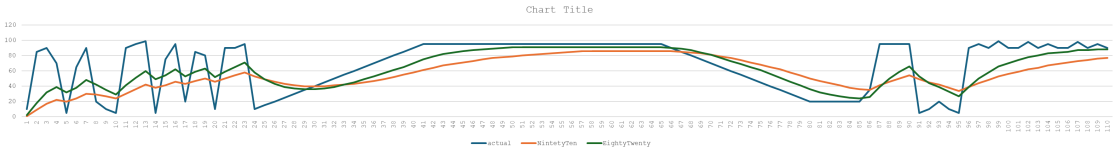


Figure 4-106 Another Sample Resource Usage Monitoring using EMA



The user can configure the Congestion Control feature to use EMA algorithm for resource usage calculations. By default this is disabled and it can be enabled by adding the following keys to the Congestion Control Settings menu, Advance Settings section in the CNC Console:

Table 4-97 EMA Configurable Key and Value

Key	Value	Description
CPU_CONGESTION_RESOURCE_CALC_ALGORITHM	EMA	This enables the congestion control CPU resource calculation to use the algorithm provided.
CPU_CONGESTION_RESOURCE_CALC_INTERVAL_MS	50ms	This configuration sets the time interval in milliseconds for CPU congestion resource to be calculated by the configured algorithm.
QUEUE_CONGESTION_RESOURCE_CALC_ALGORITHM	EMA	This enables the congestion control Queue resource calculation to use the algorithm provided.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-97 (Cont.) EMA Configurable Key and Value

Key	Value	Description
QUEUE_CONGESTION_RESOURCE_CALC_INTERVAL_MS	70ms	This configuration sets the time interval in milliseconds for Queue congestion resource to be calculated by the configured algorithm.

Configure the percentage ratio to consider for current congestion resource usage data point and previous congestion resource usage data point by adding following Advanced setting keys to the Congestion Control Settings menu, Advance Settings section in the CNC Console:

Table 4-98 Configure percentage ratio

Key	Value	Description
EMA_CPU_CONGESTION_RESOURCE_CALC_RATIO	70:30	This configuration will be used to set the EMA ratio in which congestion resource(s) calculated using EMA algorithm to be considered for calculation.
EMA_QUEUE_CONGESTION_RESOURCE_CALC_RATIO	70:30	This configuration will be used to set the EMA ratio in which congestion resource(s) calculated using EMA algorithm to be considered for calculation.

For more information about Congestion Control EMA configurations, see Settings section in CNC Console.

Managing Congestion Control Resource Usage Using EMA Algorithm

Enable

By default, this feature is disabled for all Policy services that support Congestion Control feature. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To enable this feature using CNC Console for Policy services that uses Congestion Control, add the `CPU_CONGESTION_RESOURCE_CALC_ALGORITHM` and `QUEUE_CONGESTION_RESOURCE_CALC_ALGORITHM` advanced keys in the **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations**.

For more information, see Congestion Control Settings section.

Configure Using REST API

Perform the feature configurations as described in "Congestion Control" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.33 Message Feed for SBI Monitoring

In order to enable correlation of the internal and external (request/response) messages for all the transactions initiated by the producer and consumer NFs, Policy supports copying the messages at Ingress and Egress Gateways.

This feature allows NFs using Ingress and Egress Gateways to report every incoming and outgoing message to Oracle Communications Network Analytics Data Director (OCNADD) monitoring system.

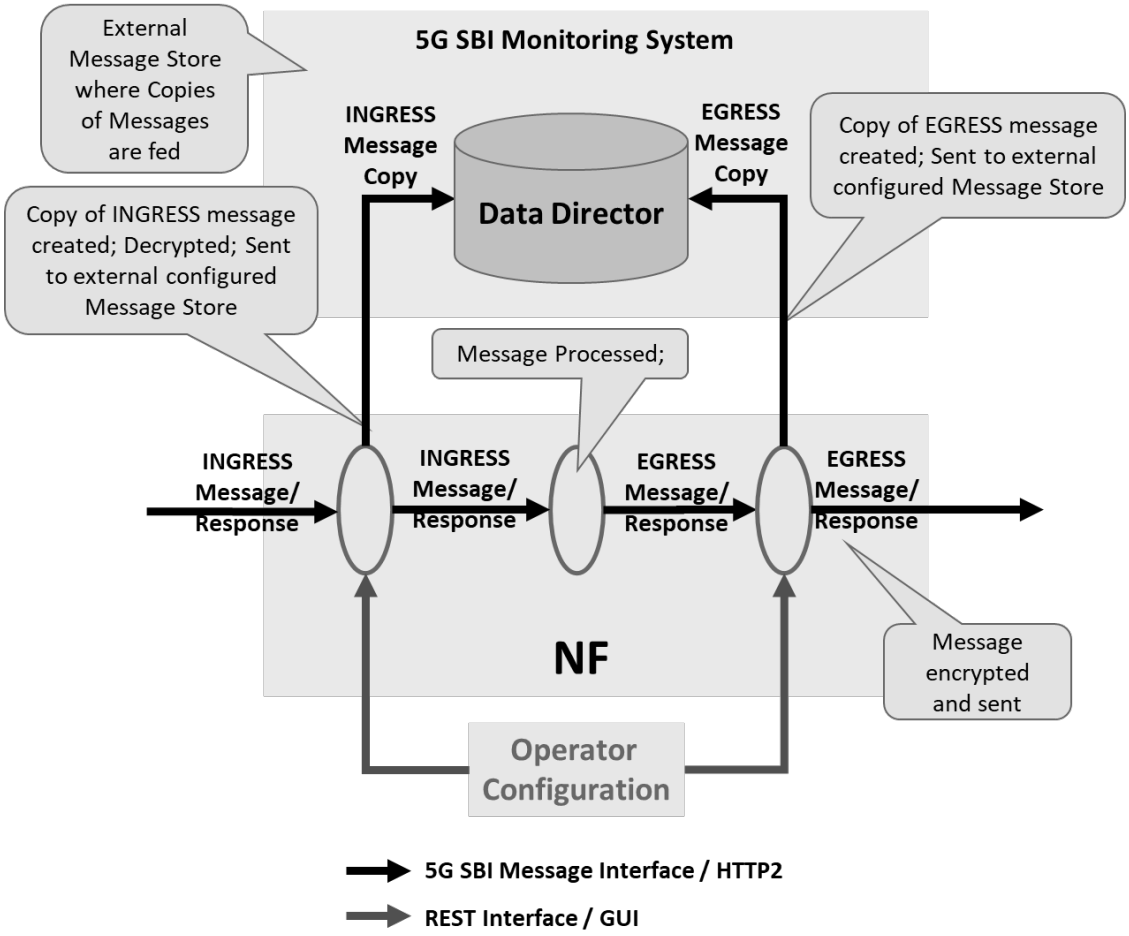
That is, OCNADD is a message store to keep a copy of each request and response processed through Ingress and Egress Gateways.

The insights on these messages enable NFs to integrate with external 5G SBI monitoring system for:

- Call Tracing / Tracking
- Live debugging

Architecture

Figure 4-107 Policy Message Feed Architecture



Copyright © 2019, 2026, Oracle and/or its affiliates.

OCNADD is a Network Data Broker part of the Network Analytics suite of products. OCNADD receives network data traffic information from various sources such as 5G NFs and Non-5G Nodes and sends the data securely to subscribed consumer (3rd Party tools) after applying its powerful and configurable filtering, replication, and aggregation rule corresponding to subscribed consumers. For more information on OCNADD, see *Oracle Communications Network Analytics Data Director User Guide*.

5G NF Kafka Producer is used as the source to send the data stream towards OCNADD. The 5G NFs use integrated Kafka producer services to stream the 5G South Bound Interface (SBI) messages along with metadata added by NFs to OCNADD.

Managing Message Feed for SBI Monitoring

Enable

Message feed feature can be enabled using Helm parameters either at the time of Policy installation or during the software upgrade.

`ingress-gateway.message-copy.enabled` parameter is used to enable copying messages passing through Ingress Gateway.

`egress-gateway.message-copy.enabled` parameter is used to enable copying messages passing through Egress Gateway.

For more information, see *Configuring Ingress Gateway*, *Configuring Egress Gateway*, and *Configuring Kafka for NF Message Feed* sections in *Oracle Communications Cloud Native Core, Converged Policy, Upgrade, and Fault Recovery Guide*.

Configure

Message feed feature can be configured using Helm parameters either at the time of Policy installation or during the software upgrade.

For more information, see *Configuring Ingress Gateway*, *Configuring Egress Gateway*, and *Configuring Kafka for NF Message Feed* sections in *Oracle Communications Cloud Native Core, Converged Policy, Upgrade, and Fault Recovery Guide*.

SASL_SSL Configuration for Policy Message Copy

As there is no certificate-based client authentication required, a trustStore is created at Policy.

Policy contains placeholders to accept caroot certificates, which are then translated into trustStore using Gateway init-containers.

Policy uses native SSL functionality provided by Gateway services. SSL service block gets activated or used, when enableIncomingHttps is set to `true`. The same configuration is used for message copy SSL configuration too.

To configure only Policy-DD SSL communication without native SSL functionality, configure **caBundle** and **trustStorePassword** sections with appropriate secret configurations.

To use both native SSL functionality and Policy-DD SSL communication, add the caRoot certificate of Kafka broker to the existing caRoot certificate by appending Kafka broker ca certificate after the existing certificate.

1. Generate SSL certificates.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Creation process for private keys, certificates and passwords is based on discretion of user or operator.

2. Before copying the certificates to the secret, add the DD Root certificates contents into the CA certificate(**caroot.cer**) generated for NRF.

> **Note**
>
> Make sure to add 8 hyphens "**-**" between 2 certificates.

```
-----BEGIN CERTIFICATE-----
<existing caroot-certificate content>
-----END CERTIFICATE-----
--------
-----BEGIN CERTIFICATE-----
<DD caroot-certificate content>
-----END CERTIFICATE-----
```

3. Create a secret for authentication with DD.
   To create a secret store the password in a text file and use the same file to create a new secret.

```
kubectl create secret generic ocingress-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=caroot.cer --from-file=ssl_rsa_certificate.crt --from-
file=ssl_ecdsa_certificate.crt --from-file=sasl.txt -n <namespace>

kubectl create secret generic ocegress-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=ssl_rsa_private_key.pem --from-
file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=ssl_cabundle.crt --from-file=ssl_rsa_certificate.crt --from-
file=ssl_ecdsa_certificate.crt --from-file=sasl.txt -n <namespace>
```

4. Provide appropriate values for the SSL section.
   SSL configuration:

```
service:
  ssl:

    privateKey:
      k8SecretName: ocegress-secret
      k8NameSpace: pcf
      rsa:
        fileName: rsa_private_key_pkcs1.pem
      ecdsa:
        fileName: ssl_ecdsa_private_key.pem

    certificate:
      k8SecretName: ocegress-secret
      k8NameSpace: pcf
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
      rsa:
        fileName: tmp.cer
      ecdsa:
        fileName: ssl_ecdsa_certificate.crt

    caBundle:
      k8SecretName: ocegress-secret
      k8NameSpace: pcf
      fileName: caroot.cer

    keyStorePassword:
      k8SecretName: ocegress-secret
      k8NameSpace: pcf
      fileName: key.txt

    trustStorePassword:
      k8SecretName: ocegress-secret
      k8NameSpace: pcf
      fileName: trust.txt

    initialAlgorithm: RS256
```

5. Configure the message copy feature.

```
messageCopy:
  enabled: true
  copyPayload: true
  topicName: PCF
  ackRequired: false
  retryOnFailure: 0
  security:
    enabled: true
    protocol: SASL_SSL
    tlsVersion: TLSv1.2
    saslConfiguration:
     userName: ocnadd
     password:
       k8SecretName: ocegress-secret
       k8NameSpace: pcf
       fileName: sasl.txt
```

6. Make sure to configure the correct SASL_SSL port in `kafka.bootstrapAddress` attribute. To get the correct value of this, refer to DD Kafka's Values.yaml file.

Observability

Metrics

The following metrics are used to count the ingress and egress messages at the gateways:

- oc_ingressgateway_msgcopy_requests_total
- oc_ingressgateway_msgcopy_responses_total
- oc_egressgateway_msgcopy_requests_total
- oc_egressgateway_msgcopy_responses_total

For more information, see:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Ingress Gateway Metrics
- Egress Gateway Metrics

Alerts

The following alerts are raised when OCNADD is not reachable:

- INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
- EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

For more information, see

- INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
- EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

4.34 Support for Dual Stack

Using the dual stack mechanism, applications or NFs can establish connections with pods and services in a Kubernetes cluster using either IPv4, IPv6, or both, depending on the configured deployment mode. Dual stack provides:

- Coexistence strategy that allows hosts to reach IPv4 and IPv6.
- IP address allocation to the Kubernetes clusters during cluster creation. This allocation is applicable for all Kubernetes resources unless explicitly specified during cluster creation.

> **Note**
>
> - The dual stack feature is not supported on Oracle Cloud Native Environment (CNE) but is supported on third-party CNEs.
> - Operator needs to redeploy (Fresh install) the Policy to enable IP Dual Stack functionality.

On a dual stack deployment, externally communicating services of type LoadBalancer such as Ingress Gateway and Diameter Gateway supports dual stack where as internally communicating services such as cnDBTier, CM, and so on, uses single stack based on the preference. Please refer the table below.

Table 4-99 Preference of Deployment Mode

Services	IPv6_Pv4	IPv4_IPv6	IPv6	IPv4
Internal communicating services	IPv6 (Single Stack)	IPv4 (Single Stack)	IPv6 (Single Stack)	IPv4 (Single Stack)
External communicating services	IPv6 preferred (Dual Stack)	IPv4 preferred (Dual Stack)	IPv6 (Single Stack)	IPv4 (Single Stack)

> **Note**
>
> Communication between services and CoreDNS, as well as the Kubernetes API, depends on the cluster's network preference.

Copyright © 2019, 2026, Oracle and/or its affiliates.

IP Address Allocation to Pods

IP address allocation to pods depends on the IP address preference set in the Kubernetes cluster. Pods do not have the privilege to choose an IP address. Consider the following example of a pod deployed in an IPv4 preferred infrastructure. Here, if the Kubernetes cluster has IPv4 preferred configuration, both IPv4 and IPv6 are allocated to the pod, but the primary IP address is IPv4. Example:

```
IP:               10.xxx.xxx.xxx
IPs:
  IP:           10.xxx.xxx.xxx
  IP:           fd00::1:cxxx:bxxx:8xxx:xxxx
```

IP Address Allocation to Services

IP address allocation to all the Policy services, depends on the `DeploymentMode` Helm parameter configuration. This Helm parameter automatically configures IP Family Policy and IP Families attributes for the Policy services. For more information about `DeploymentMode`, see the "Customizing Policy" section in the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*

You can customize the IP address allocation to services based on the `DeploymentMode` Helm parameter. Services route the traffic to the destination endpoints based on this configuration. If the`DeploymentMode` Helm parameter is set to IPv4, then IPv4 is allocated to services, and services use IPv4 pod IPs to send the traffic to endpoints.

The following table describes how IP address allocation, IP Family Policy, and IP Families vary based on the `DeploymentMode` Helm parameter configuration for services:

Table 4-100 IP Address Allocation

Infrastructure Preference	Application Preference (Deployment Mode Helm Parameter)	IP Family Policy Attribute	IP Families Attribute	Pod IP	Service IP	Endpoints
IPv4 Preferred	IPv4	Single Stack	IPv4	IPv4,IPv6	IPv4	IPv4
IPv6 Preferred	IPv4	Single Stack	IPv4	IPv6,IPv4	IPv4	IPv4
IPv4 Preferred	IPv6	SingleStack	IPv6	IPv4,IPv6	IPv6	IPv6
IPv6 Preferred	IPv6	SingleStack	IPv6	IPv6,IPv4	IPv6	IPv6
IPv4 Preferred	IPv4_IPv6 (IPv4Preferred)	RequireDualStack	IPv4 Preferred	IPv4,IPv6	IPv4,IPv6	IPv4
IPv6 Preferred	IPv4_IPv6 (IPv4Preferred)	RequireDualStack	IPv4 Preferred	IPv6,IPv4	IPv6,IPv4	IPv4
IPv4 Preferred	IPv6_IPv4 (IPv6Preferred)	RequireDualStack	IPv6 Preferred	IPv4,IPv6	IPv4,IPv6	IPv6
IPv6 Preferred	IPv6_IPv4 (IPv6Preferred)	RequireDualStack	IPv6 Preferred	IPv6,IPv4	IPv6,IPv4	IPv6

Enable

Dual Stack support can be enabled by setting the `global.deploymentMode` parameter to IPv4_IPv6 or IPv6_IPv4 depending on the preference needed. For more information, see the

Copyright © 2019, 2026, Oracle and/or its affiliates.

Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.

Configure

> **Note**
>
> The `diam-gateway.dualStackPreferredDnsResolutionIpAddressType` parameter is replaced by `global.dgwRoutingMode`. The `diamgateway.envSupportedIpAddressType` parameter is not applicable anymore.

You can configure dual stack using the following parameters:

- `global.deploymentMode`
- `global.egressRoutingMode`
- `global.dgwRoutingMode` (supported values: IPv6, IPv4, IPv6_IPv4, IPv4_IPv6; default value: IPv4_IPv6)
  For more information on these parameters, see "Configuration Parameters for Dual Stack" section in the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Table 4-101 Gateway Routing Mode

dgwRoutingMode/ egressRoutingMode	Description	DNSQuery/k8s endpoints returns IPv4 address only	DNSQuery/k8s endpoints returns IPv6 address only	DNSQuery/k8s endpoints returns both IPv4 and IPv6 address
IPv4	Strict IPv4 only	Gateway attempts connection towards the destination	Gateway will not initiate connection towards the destination	Gateway will pick up the IPv4 address and attempts connection toward the destination
IPv6	Strict IPv6 only	Gateway will not initiate connection towards the destination	Gateway attempts connection towards the destination	Gateway will pick up the IPv6 address and attempts connection toward the destination
IPv4_IPv6	Supports both with IPv4 preferred	Gateway attempts connection towards the destination	Gateway attempts connection towards the destination	Gateway will pick up the IPv4 addresses only and attempts connection toward the destination
IPv6_IPv4	Supports both with IPv6 preferred	Gateway attempts connection towards the destination	Gateway attempts connection towards the destination	Gateway will pick up the IPv6 addresses only and attempts connection toward the destination
None **(Applicable to egressRoutingMode only)**	No changes. Egress Gateway will rely on library to select IPs.	NA	NA	NA

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
Configuration for IPv4 single stack mode	IPv4	IPv4	IPv4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 (Cont.) Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
Configuration for IPv6 stack mode	IPv6	IPv6	IPv6

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 (Cont.) Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
Configuration for dual stack mode with IPv4_IPv6	IPv4_IPv6	IPv4_IPv6	IPv4_IPv6

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 (Cont.) Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
v4 preference			

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 (Cont.) Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
Configuration for dual stack mode with IPv6_IPv4	IPv6_IPv4	IPv6_IPv4	IPv6_IPv4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 (Cont.) Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
v6preference			

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 (Cont.) Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
Configuration as per the cluster preferred	ClusterPreferred	IPv4_IPv6	None

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-102 (Cont.) Recommended Configurations for Dual Stack and Single Stack

Description	global.deploymentMode	global.dgwRoutingMode	global.egressRoutingMode
ncewhereapplicationisdeployed			

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> - In 25.1.200 release, dual stack is not supported for the Egress traffic on LDAP, PER, and Notification service.
> - Egress routing support for automatic fallback between IPv4 and IPv6 is not supported. Customer should connect using their preferred IP address type. If that IP type is unavailable, connection to the peer is considered unavailable.
> - Any combination of dual stack or IPv6 configurations other than recommended values shall be considered as invalid and not supported.

Upgrade details

Table 4-103 Upgrade details

diam-gateway.dualStackPreferredDnsResolutionIpAddressType	global.dgwRoutingMode
IPv4	IPv4
IPv6	IPv6
IPv4_IPv6	IPv4_IPv6
IPv6_IPv4	IPv6_IPv4
both	IPv4_IPv6 or IPv6_IPv4 depending on the preference

Observability

Metrics

The following metrics are added in the Ingress Gateway Metrics section:

- `oc_ingressgateway_incoming_ip_type`
- `oc_ingressgateway_outgoing_ip_type`

The following metrics are added in the Egress Gateway Metrics section:

- `oc_egressgateway_incoming_ip_type`
- `oc_egressgateway_outgoing_ip_type`
- `oc_egressgateway_dualstack_ip_rejected_total`

4.35 Handling of Multiple N1N2Transfer Messages

PCF processes the requests received from the external NFs to initiate the policy evaluation and then triggers the N1N2Transfer to UE. Following is the list of triggers for the policy evaluation:

- UE Policy Create from AMF
- UE Policy Update from AMF

Copyright © 2019, 2026, Oracle and/or its affiliates.

- UE Policy Data updateNotifications received from UDR
- Asynchronous CHF response to Subscription
- Notifications received from CHF
- N1N2Notifications failure from AMF
- N1 Message Notify from AMF carrying the UE message of N1 Message Reject or N1 Message complete
- T3501 timer expiry

The triggers may arrive to PCF when last N1N2 transfer is still in progress. After processing and evaluating the triggers, the policy evaluation results (Install UPSI, Remove UPSI, or UPSIs that needs to be transferred to UE) are sequenced. If PCF receives more than one trigger while the previous N1N2 transfer is in progress and this feature is enabled, then it consolidates and stores the UPSIs with URSP rules that needs to be transferred to UE. Once the UE notification is received for the in-progress N1N2 transfer, final consolidation is performed and consolidated UE policy actions are sent out to UE in a single (assuming no fragmentation is required) N1N2 transfer.

Whenever consolidation will be performed for UE policy action, next N1N2 transfer carrying consolidated UE policy action will have an updated Procedure Transaction Identity (PTI).

Users can optimize the install action using the `UE.POLICY.INSTALLATION.OPTIMIZATION.ENABLED` key in the Advanced Settings of UE service. Here, install action can be optimized by not installing the subscriber session if particular UPSI or URSP specific to PLMN is installed by PCF in current subscriber session. Policy supports the following scenarios:

Scenario 1:

- During Create, Install [UPSI-1 and UPSI-2] received as UE policy action and N1 message Notify successfully received with command complete.
- During Update from AMF, Policy Action is Install [UPSI-2 and UPSI-3].

Case 1: Install Optimization is enabled

Next N1N2 transfer - Install [UPSI-3]. Here, there is no action for UPSI-2 as it is already successfully installed so will not be installed. Install optimization of Policy transfers for UPSI-2 is performed here.

Case 2: Install Optimization is disabled (Default)

Next N1N2 transfer - Install [UPSI-2 and UPSI-3]

Scenario 2:

- During Create, Install [UPSI-1 and UPSI-2] received as UE policy action and N1N2 transfer is sent out and is in progress.
- During Update from AMF, Policy Action is Install [UPSI-2 and UPSI-3] as last N1N2 transfer is still in progress. So, the current policy evaluation will be sequenced.
- N1 message notify received with command Reject for UPSI-1. Policy evaluation result on N1 notify reject is retransmit UPSI-1.
- Consolidation will be performed for sequenced policy evaluation with current policy decision. Consolidated UE policy action: Install [UPSI-1, UPSI-2, UPSI-3].

Case 1: Install Optimization is enabled

Copyright © 2019, 2026, Oracle and/or its affiliates.

Next N1N2 transfer - Install UPSI-1 and UPSI-3 Here, there is no action for UPSI-2 as it is already successfully installed so it will not be installed. Install optimization of Policy transfers for UPSI-2 is performed here.

Case 2: Install Optimization is disabled (Default)

Next N1N2 transfer - Install [UPSI-1, UPSI-2, and UPSI-3]

Managing the Feature

Enable
This feature can be enabled by setting the `Enable Consolidation of UE Policy Decisions` attribute to `true`.

The consolidation for Re-transmissions on T 3501 can be enabled by setting the `Enable Consolidation of UE Policy Decisions for Re-transmission on T3501 Expiration` to `true`. It is applicable only if the `Enable Consolidation of UE Policy Decisions` feature is enabled.

Bulwark must be enabled to ensure exclusive locking for UE policy processing in the Handling of Multiple N1N2Transfer Messages feature. User can set the following advanced setting keys for bulwark in CNC Console:

- `CONCURRENCY.N15.UE_NOTIFICATION.LOCK_REQUEST_RETRY_COUNT`
- `CONCURRENCY.N15.UE_NOTIFICATION.LOCK_REQUEST_RETRY_BACKOFF`
- `CONCURRENCY.N15.UE_NOTIFICATION.LOCK_LEASE_DURATION`
- `CONCURRENCY.N15.UE_NOTIFICATION.LOCK_WAIT_DURATION`
- `CONCURRENCY.N15.UE_NOTIFICATION.ENABLED`

For more information, see PCF UE Policy Service.

Configure
Optimization for Install Action: To optimize the install action `UE.POLICY.INSTALLATION.OPTIMIZATION.ENABLED` key must be set to true in the **Advanced Settings** of **PCF UE Policy** configurations. It is disabled by default.

For more information, see PCF UE Policy Service.

The following Policy blocks have been added to UE for policy blocks execution:

- *Pending/In transfer*
- *Discard/Discard All*

The *Operation type* Policy block has been updated with *T3501 Expiry* option.

For more information, see "PCF UE Policy" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.

Observability
The following metrics are used for this feature:

- ue_n1_policy_sequencing
- ue_n1_policy_consolidation

For more information, see UE Service Metrics.

The following alerts are used for this feature:

- UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD

Copyright © 2019, 2026, Oracle and/or its affiliates.

- UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD
- UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD
- UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD
- UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD
- UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD
- UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD

For more information, see PCF Alerts.

4.36 PCF support to not send ASR while Notify-Update fails

Policy Control Function (PCF) receives AAR-I and sends AAA success response immediately, if (Protocol Data Unit) PDU Session is successfully retrieved and mapped. The Notify-Update request is sent asynchronously for the established Rx session. In case, there are some issues at PCF such as network issues, SMF is overloaded, PCF can not send Notify-Update to SMF, or Notify-Update to SMF fails, then PCF triggers an Abort Session Request (ASR) to Application Function (AF) to terminate the voice call.

This feature enables PCF to have the capability to decide whether to tear down the Policy Authorization/Rx session which does not contain Video Media type or any other media type configured by user to be excluded from suppressing ASR, when PCF is not able to successfully update the required PCC and session rules to SMF for the Rx Session of a PDU session. This lets the voice data packets or any other media type configured by user to be carried over default IMS QOS flow.

Managing the Feature

Enable
By default, this feature is disabled. The operator can enable this feature through the CNC Console configurations.

Configure using CNC Console
You can configure the feature by:

1. Adding new configurations for "Rx ReAuth Profile" in **Common Data** under **Service Configurations** in the CNC Console.
   For more information, see Rx Reauth Profiles.
2. Selecting the new "Rx ReAuth Profile" in **PCF Session Management** under **Service Configurations** in the CNC Console.
   For more information, see PCF Session Management.

Observability
The metric *occnp_suppress_notify_total* has been added to measure the number of ASR not send, ASR sent, and RAR sent when the feature is enabled.

For more information, see SM Service Metrics.

The following alerts are used for this feature:

- UPDATE_NOTIFY_FAILURE_ABOVE_30_PERCENT
- UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT

Copyright © 2019, 2026, Oracle and/or its affiliates.

- UPDATE_NOTIFY_FAILURE_ABOVE_70_PERCENT

For more information, see List of Alerts.

4.37 LDAP Timeout and Retry Mechanism

The existing LDAP request timeout can be configured through Helm. To make this run time configurable, the operator must configure **Timeout value** in milliseconds while creating or editing the LDAP datasource.

With this feature, Policy supports retry functionality towards external LDAP server. The operator must first enable the **Retry Enabled** flag to use this functionality. Then, the operator can configure the **Max number of retries** and **Retries on errors/timeout** to configure the multiple error codes including the error code for LDAP timeout (85).

> **Note**
>
> There is no classification about permanent or temporary error for LDAP failure response. Hence, all the failure responses come under the error category. The timeout is observed as error code 85 (timeout) and connection related error is observed as error code 91 (connectError) by the ldap-gw applications. In the case of timeout/ connection retry, operator has to set corresponding value in the retry error code list in CNC Console.

When retry condition hits the LDAP, the request is retried or reattempted to the next available LDAP server configured in LDAP datasource. The LDAP request retry happens based on next available (connected) server and not based on read connection setup for the server.

> **Note**
>
> The retries are immediate retry and there is no backoff timer or delayed retry. The retry related to connection is automatically selected as per Data Source configurations, no specific error code configuration is required for such case.

In case multiple servers are configured, the retries would happen as mentioned in the following table:

Table 4-104 LDAP Retry for Multiple Configured Servers

Servers Available	Initial Request	First Retry
Primary, Secondary, Tertiary	Primary	Secondary
Primary, Secondary,	Primary	Secondary
Primary, Tertiary	Primary	Tertiary
Secondary, Tertiary	Secondary	Tertiary
Primary	Primary	Primary
Secondary	Secondary	Secondary
Tertiary	Tertiary	Tertiary

Managing the Feature

Enable

Copyright © 2019, 2026, Oracle and/or its affiliates.

By default, this feature is disabled. The operator can enable this feature through the CNC Console configurations.

Configure Using CNC Console
You can enable the LDAP Retry functionality by using the **Retry Enabled** toggle button.

For more information, see Data Sources.

Configure Using Helm
The following parameters must be used to establish the connection with the LDAP servers configured after reading the datasource configuration:

- `LDAP_CONNECTION_CONNECT_ALL_SERVERS`
- `LDAP_CONNECTION_DATASOURCE_RETRY_COUNT`

For more information, see "LDAP Configurations" section in Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.

Observability
The following metrics are used to count the number of LDAP search requests and responses at the LDAP Gateway:

- occnp_ldap_search_request_total
- occnp_ldap_search_response_total

For more information, see LDAP Gateway.

4.38 Logging Support for Error Response

Policy provides error handling framework as a general purpose error handling tool. This feature used the error handling framework to add more details to the error using 3GPP error response format.

Policy sends error responses to consumer NFs due to exceptions such as signaling, validations, and internal errors. These error responses have payloads containing the problem title, status, details, and cause of the error that are used to investigate the error. Policy provides enhanced logging support for the error responses for the following microservices:

- SM Service
- PDS Service
- User Service
- Binding Service
- PRE Service
- PCRF Core
- Diameter Connector
- Diameter Gateway
- LDAP Gateway
- SOAP Connector
- Usage Monitor

Currently, Policy supports the following log levels:

- **ERROR**: Error is at a service or component level and not per subscriber or call flow level.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **WARN**: An error is not expected in a typical call flow, and there is a need to know if it occurred in production when troubleshooting an issue.
- **INFO**: Informational logs showing what is happening in each service or component during a call flow. All in-out messages to a service should be logged at **INFO** level. It is also beneficial to log messages once during processing by a component within a service.
- **DEBUG**: Provides detailed logs that helps to troubleshoot an issue.
- **TRACE**: Includes detailed logging of messages in and out of each component or method.

The enhanced logging supports error responses during SM/Rx call flows at their default log level. It provides sufficient visibility into issues within or across the external facing interfaces such as SM service, PCRF Core, Diameter Connector, UDR Connector, CHF Connector, PRE, PDS, Bulwark service and Binding service. The current default log level for Policy microservices is WARN.

The enhanced logging (WARN level) support is provided for the following call flows:

- SMPolicyControl Create
  - During SM Create flow, details such as session information (Association ID), URI, method, and error specifics are added to WARN logs.
  - WARN logs are standardized across internal and external interfaces (SMF, UDR, CHF, BSF, NRF).
- SMPolicyControl Update: The enhanced WARN logs includes details about session updates, including any modification restrictions or errors encountered.
- SMPolicyControl Delete: WARN logging for session termination scenarios,captures error details and context such as missing or incorrect parameters.
- SMPolicyControl UpdateNotify/Terminate Notify: WARN logs for notification events include details such as session ID, method, URI, and error-specific context to allow better correlation and RCA.
- CM Config Change
- Rx AAR Initiate: Session information (such as session ID), URI, method, and error specifics are added to WARN logs during the Rx call flow. WARN logs are standardized across relevant internal and external interfaces (PCRF, PRE, BINDING, PDS, BULWARK, ETC).
- Rx AAR Update: WARN logs contain details about session updates, including any modification restrictions or errors encountered.
- Rx STR Terminate: WARN logging for session termination scenarios captures error details and context such as missing or incorrect parameters.
- Rx ASR/RAR Notify: WARN logging for session termination notification scenarios captures error details and context such as missing or incorrect parameters.
- Gx CCR-I: WARN logs include session information such as session ID, URI, method, and error specifics. WARN logs are standardized across relevant internal and external interfaces (PCRF, PRE, BINDING, PDS, BULWARK, DIAM-G,ETC).
- Gx CCR-U: WARN logs contain details about session updates, including any modification restrictions or errors encountered.
- Gx CCR-T: WARN logging for session termination scenarios captures error details and context such as missing or incorrect parameters.
- Gx RAR: WARN logging for session re-authentication scenarios captures error details and context such as missing or incorrect parameters.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Sd TSR: The WARN logs during Sd call flow include detailed session information such as session ID, URI, method, and error specifics. WARN logs are standardized across relevant internal and external interfaces (PCRF, PRE, BULWARK, DIAM-G,ETC).
- Sd CCR-U: The WARN logs during Sd update call flow capture details about session updates, including any modification restrictions or errors encountered.
- Sd CCR-T: WARN logging for session termination scenarios captures error details and context such as missing or incorrect parameters.
- Sd RAR: WARN logging for session re-authentication scenarios captures error details and context such as missing or incorrect parameters.
- Sy SLR: WARN logs during the Sy call flow captures detailed session information such as session ID, URI, method, and error specifics. WARN logs are standardized across relevant internal and external interfaces (SM/PCRF, PRE, PDS, BULWARK, DIAM-C, DIAM-G,ETC).
- Sy SNR: WARN logs for Sy Update-notify call flow capture details about session updates, including any modification restrictions or errors encountered.
- Sy STR: WARN logging for session termination scenarios captures error details and context such as missing or incorrect parameters.

When sending any error response triggered by an HTTP Request, this error response format will be mapped into the following *general log format*:

> **Note**
>
> Each error will be logged at the WARN level, accompanied by additional context to facilitate faster and more efficient troubleshooting.

Logging format for HTTP call flows:

```
{
    "messageTimestamp": “Value”",
    "errorStatus": "Value",
    "errorTitle": "Value",
    "errorDetails": "Value",
    "errorCause": "Value",
    "sender": "Value",
    "receiver": "Value",
    "URI": "Value",
    “method”: “Value”,
    "subscriberId": "Value", #Note:  It is only added if present.
    "associationId": “Value”, #Note: It is only mandatory in SM. In other
services, it is optional.
    "sessionId": “Value”, #Note: It is only mandatory in pcrf-core, diam-
connector. In other services, it is optional.
    "frameIpAddress": "Value",  #Note: It is only added in SM, pcrf-core,
diam-connector for AF call flow if present.
    "frameIpv6Prefix": "Value", #Note: It is only added in SM, pcrf-core,
diam-connector for AF call flow if present.
    "calledStationId": "Value,  #Note: It is only added in SM, pcrf-core,
diam-connector for AF call flow if present.
    "ipDomainId": "Value" #Note: It is only added in SM, pcrf-core, diam-
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
connector for a AF call flow if present.
}
```

> **Note**
>
> - `associationId` is only applicable for SM call flows.
> - The *sender* and *receiver* fields have limitations when including the IDs, because the current pod generating the log does not have information about the other identity. This limitation is related to the pod context: the current HTTP call flow does not send the server header with the sender's pod id in the internal NS request, making it impossible to field the other pod's identity. If the generated error response is logged, the receiver Id will be empty. If the received error response is logged, the sender ID will be empty. For external NF call flows (SMF, UDR, and AF), use the server header to obtain the NF instance Id. The sender and receiver are from within the following structure. senderType + "-" + senderId receivedType + "-" + receivedId The fields will be present, but the IDs may be empty due to call flow limitations.

Diameter call flows

```
{
    "messageTimestamp": “Value”",
    "errorCode": "Value",
    "errorCause": "Value",
    "sender": "Value",
    "receiver": "Value",
    "msgType": "Value",
    "appType": "Value",
    "sessionId": “Value”,
    "subscriberId": "Value", #Note: It is only added if present.
    "frameIpAddress": "Value", #Note: It is only added if present.
    "frameIpv6Prefix": "Value", #Note: It is only added if present.
    "calledStationId": "Value, #Note: It is only added if present.
    "ipDomainId": "Value" #Note: It is only added if present.
}
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

- `associationId` is only applicable for SM call flows.
- The sender and receiver fields are populated based on whether a Diameter error message is generated by a pod or received by a pod. When a pod generates a Diameter error: **sender** = *senderType-senderId*, where: *senderType* is pod server name and *senderId* is pod ID that generated the error. **receiver** = *receiverType-receiverId*, where: *receiverType* is peer node name (For example, rx = AF, gx = PGW, sy = OCS, sd = TDF) and *receiverId* is Origin-Host peer identity from the request message. When a pod receives a Diameter error: **sender** = *senderType-senderId*, where: *senderType* is peer node name (For example, rx = AF, gx = PGW, sy = OCS, sd = TDF) and *senderId* is Origin-Host peer identity from the request message. **receiver** = *receiverType-receiverId*, where: *receiverType* is pod server name and *receiverId* is pod ID that received the error. **Examples**: (proxy) DIAM_GW ← DIAM_C: "message":"Received error response", "sender":"DIAM_C-ocpcf", "receiver":"DIAM_GW-ocpcf-oc-diam-gateway-0" DIAM_C → DIAM_GW (proxy):"message":"Generated error response", "sender":"DIAM_C-ocpcf-oc-diam-connector-6548479c95-xr2lp", "receiver":"AF-TD-DATA-1" The Diameter Gateway (DIAM_GW), acting as a proxy, will receive and generate Diameter error messages as expected. As a proxy, the Diameter Gateway will always receive all errors.
- The diameter-enhanced logging response is added mainly for PCRF Core and Diameter Connector AF call flows. Diameter Gateway only forwards the request and response messages.
- In Diameter Gateway, support is added only for HTTP call flows related to Rx, such as binding search requests and adding the enhanced stack trace and async logging support.
- The Diameter Gateway (DIAM_GW), acting as a proxy, will receive and generate Diameter error messages. The DIAM_GW will log the generated error response if it occurs, for example, due to a timeout. If an error is received, no generated error log will be expected, as it is only forwarding the response, not creating an error; only the received error response will be logged by the DIAM_GW.
- For the `subscriberId` or `subscriptionId`, choose only between GPSI/MSISDN and SUPI/IMSI. If both are present, SUPI/IMSI is taken first.

Table 4-105 General Log Format

Parameter	Description	Example
messageTimestamp	Specifies the timestamp of the error message	-
errorStatus	Specifies the status code of the error.	404, 500, etc.
errorTitle	Specifies the title of the error.	Subscription not found

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-105 (Cont.) General Log Format

Parameter	Description	Example
errorDetails	Specifies the error detail produced by error handling framework in case of PCF as producer. **Note:** For *errorDetails* field to be populated in the required format, error handling framework should be enabled in CNC Console for the required service.	`ocpcf.oracle.com:UDRC:SC:USER NOT FOUND.EI-01-404-01-01-03.USER_NOT_FOUND:EC-OCPCF-UDRC-EI-01-01-404-00008-01-03`
errorCause	Specifies the cause of the error.	SUBSCRIPTION_NOT_FOUND
sender	Specifies the sender which is composed by the nfType plus the instanceId. **Note:** In case of PCF as producer of error, the sender field will be PCF plus the instanceId of the PCF. In case of PCF as consumer of error, the sender field will be the external NF plus the instanceId of the external NF.	`PCF-0adae7a4-ffcd-41ec-aff0-b734789f4477`
receiver	Specifies the receiver which is composed by the nfType plus the instanceId. **Note:** Receiver field will only be present when logging error as a consumer. PCF will get the instanceId of the responding NF from the server header present in the response. In case the server header is not present it will be logged as null (example: UDR-null).	`UDR-0adae7a4-ffcd-41ec-aff0-b734789f4477`
subscriberId	Specifies the subscriberId which can be SUPI or GPSI. It is used per the availability. In case all the subscriberIds are available, following will be the priority order: • SUPI • GPSI	`imsi-65008100001061`
method	-	POST, DELETE, GET
Uniform Resource Identifier (URI)	A string of characters that uniquely identifies a resource on the network. In logs, the URI is important for tracking which resources or endpoints are involved in an error flow.	HTTP address
associationId	A unique identifier is used to track a subscriber's Session Management (SM) session within microservices. This ID is crucial for correlating logs across different services in an SM call flow.	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-105 (Cont.) General Log Format

Parameter	Description	Example
sessionId	A unique identifier is assigned to each user session in a network, facilitating its management and tracking.	-
frameIpAddress	Frame IP address used in SM, PCRF Core, and Diameter Connector for AF call flows if present.	-
frameIpv6Prefix	Used to assign a specific IPv6 prefix to a user session in SM, PCRF Core, and Diameter Connector for AF call flows if present.	-
calledStationId	Specifies the networking identifier of the Network Access Server (NAS) used in SM, PCRF Core, and Diameter Connector for AF call flows if present.	-
ipDomainId	IP domain identifier used in SM, PCRF Core, and Diameter Connector for AF call flows if present.	-
msgType	Specifies the error message type.	-
appType	Specfies the application type	-

Note

For http error response, the `errorStatus` only contains the http error code. The `errorCause` contains the human representation of the HTTP error code such as, `"errorStatus":"503", "errorCause":"SERVICE_UNAVAILABLE"`.

Support for enhanced StackTrace

In case of an exception, Policy allows to log the stack trace, providing sufficient information to help troubleshoot an exception.

For example:


```
{"instant":{"epochSecond":1749565041,"nanoOfSecond":806203000},"thread":"Test
worker","level":"ERROR","loggerName":"ocpm.pcf.util.StackTraceUtil","message":
"message example args
example","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger
","threadId":1,"threadPriority":5,"messageTimestamp":"2025-06-10T08:17:21.806-
0600","triggerClass":"ocpm.bindingservice.helper.LoggingHelperTest","errorName
":"java.lang.Throwable","errorMessage":"throwable message
example","errorStack":"[java.base/
java.lang.Thread.getStackTrace(Thread.java:1621),
ocpm.bindingservice.helper.LoggingHelperTest.enhancedStackTrace(LoggingHelperT
est.java:147), java.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native Method),
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
java.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.
java:77), java.base/
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAcces
sorImpl.java:43)]","ocLogId":"${ctx:ocLogId}"}
```

By configuring the **Truncate Stack Trace** under **General Settings** page on CNC Console, the amount of lines on all stack traces can be truncated. For more details on configuring Stack Trace Truncation feature, see General Settings.

Managing Enhancements to Logging Support for Error Response

This section explains the procedure to enable and configure the feature.

Enable

By default, this feature is disabled. The operator can enable this feature through the CNC Console configurations.

Configure

You can configure logging support for error response using the **Enable Enhanced Logging** and **Enable UE Identifier Information** toggle buttons. These toggle buttons are available in **General Settings** under **General Configurations** on CNC Console for Policy. For information about how to configure for Policy Management Service in CNC Console, see General Settings.

Observability

Metrics

ocpm_ingress_response_total metric is used to support this feature.

For more information, see SM Service Metrics.

4.39 Support for Burst rate limit modification and customization for logs

When the enhanced error response logging feature is enabled, due to certain error scenarios volume of error logs can become huge. In order to control the volume of logs, Policy allows to add a burst filter for logging against logs for all the microservices.

The Burst filter provides a mechanism to control the rate at which LogEvents are processed by silently discarding events after the maximum limit has been reached. It enables to control the frequency and volume of warning messages generated. This ensures that excessive logging does not overwhelm the system or obscure critical information.

Configuring `BurstFilter` property in log4J includes the following parameters:

- `Level`:
  Determines the minimum log level at which the filter becomes active. Log events below this level are not affected.

  Possible values are:

  - `OFF`
  - `TRACE`
  - `DEBUG`

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - `INFO`
  - `WARN`
  - `ERROR`
  - `FATAL`
  - `ALL`

  Default value is `DEBUG`.

- `Rate`:
  Defines the average number of log events allowed per second. Events beyond this rate are suppressed unless allowed by `maxBurst`.

  It accepts any positive integer or decimal value.

  Default value is 500 logs per second.

- `maxBurst`:
  Specifies the maximum number of log events that can be logged in a sudden spike before suppression starts. Helps tolerate short bursts without dropping all messages.

  It accepts any positive integer value.

  Default value is 3000.

- `onMismatch`:
  Defines the filter's behavior when a log event does not match the filter conditions such as below the level or exceeding the rate/burst limit.

  Possible values are:

  - `DENY`: The event is suppressed and not passed to the appender.
  - `NEUTRAL`: The event is passed to the next filter in the chain for further evaluation.
  - `ACCEPT`: The event is always logged regardless of conditions.

  Default value is `DENY`.

> **Note**
>
> The Burst rate limit modification and customization for logs is not supported for the following microservices:
>
> - Policy Runtime Engine (PRE)
> - App-info
> - Perf-info

4.40 Concurrency Handling at Bulwark Service to Reduce Processing Latency of Service

Policy supports the Bulwark service to handle the concurrent requests coming from other Policy services. Bulwark Service provides lock and unlock mechanism over a key (such as SUPI or GPSI) and allows only one notification at a time to proceed. For more information on handling concurrent requests, see Support for Concurrency Handling using Bulwark Service in Policy

Copyright © 2019, 2026, Oracle and/or its affiliates.

Concurrency handling of different service requests for the same key at SM service or PDS (Policy microservices) has high latency in acquiring lock from Bulwark service, on reattempt, if lock was not acquired in the first attempt.

That is, when SM service or PDS sends a lock acquisition request to Bulwark service and Bulwark service fails to acquire the lock within the `lockWaitTimeout` timer, SM service or PDS will have to wait until the `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` expires to resend a lock acquisition request to Bulwark service again.

> **Note**
>
> `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` is an advanced settings key defined at SM service or PDS that indicates the amount of time after which the SM service or PDS can retry to gain the lock, in case the lock acquisition request fails.

SM service or PDS can fail to acquire the lock due to the following reasons:

- Fail to deliver lock request (for reasons due to transport issues, sidecar congestion, or bulwark pods restart).
- Lock is already acquired/busy.

SM service or PDS reattempts to acquire lock after `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` timer expires. SM service or PDS is not aware if the lock is available or if the lock that is released during this time and is available can be gained within the `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` timer expiry duration. This adds to the latency of processing concurrent requests.

> **Note**
>
> Currently, this feature is implemented only for SM service and PDS.

Policy reduces the latency in processing different concurrent service requests at SM service or PDS (Policy microservices) by acquiring the lock for the service request when available earlier than the `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` timer, instead of waiting for `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` timer to expire, if lock acquisition had failed previously.

Latency caused by `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` timer is addressed by using Long polling mechanism.

With this mechanism, SM service or PDS request lock from Bulwark service and wait for `lockWaitTimeout` or `RequestTimeout` period, for Bulwark service to respond. If Bulwark service is able to acquire a lock, it responds with acquired lock.

If Bulwark service cannot acquire lock, it uses the Long polling functionality to retry to acquire the lock for the given key (SUPI/GPSI). It starts polling to know when the existing lock is released. For this purpose, Bulwark service creates a polling task and starts polling to know when the existing lock is released. Whenever an existing lock is released, it tries to acquire the lock for the same key.

If the lock acquisition is successful, it informs SM service or PDS with the acquired lock information, if `lockWaitTimeout` has not expired.

Copyright © 2019, 2026, Oracle and/or its affiliates.

If the acquire lock request fails again, Bulwark service creates a new polling task and retries to acquire the lock within the `lockWaitTimeout` period. If `lockWaitTimeout` is expired, SM service or PDS will request after `CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF` timer again and the same steps to acquire a lock will be followed until maximum number of lock attempts is reached. Bulwark service then sends a failure notice to SM service or PDS .

The maximum number of lock requests to be allowed can be configured using **Maximum Pending Lock Requests allowed per Key** field under **Server Retry on-Already Locked Keys** section on **Bulwark Settings** page in CNC Console.

This feature can be enabled/disabled at SM service and/or PDS as well as at Bulwark service.

This feature can be enabled/disabled at SM service by configuring `CONCURRENCY.LOCK_RETRY_MODE` advance settings key on **Session Management service** page under **Service Configurations** section in CNC Console.

This feature can be enabled/disabled at PDS by configuring `CONCURRENCY.LOCK_RETRY_MODE` advance settings key on **PDS Settings** page under **Service Configurations** section in CNC Console.

This feature can be enabled and configured at Bulwark service using the fields under **Server Retry On Already Locked Keys** section on **Bulwark Settings** page in CNC Console.

If the feature is enabled at SM service and/or PDS, SM service and/or PDS should send the request initiation timestamp (oc-origination-request-timestamp) as header. Otherwise, the retry mechanism is not enabled for that request.

The time interval between which Bulwark service can poll to know if an existing lock is released can be configured using `polling.interval` Helm parameter.

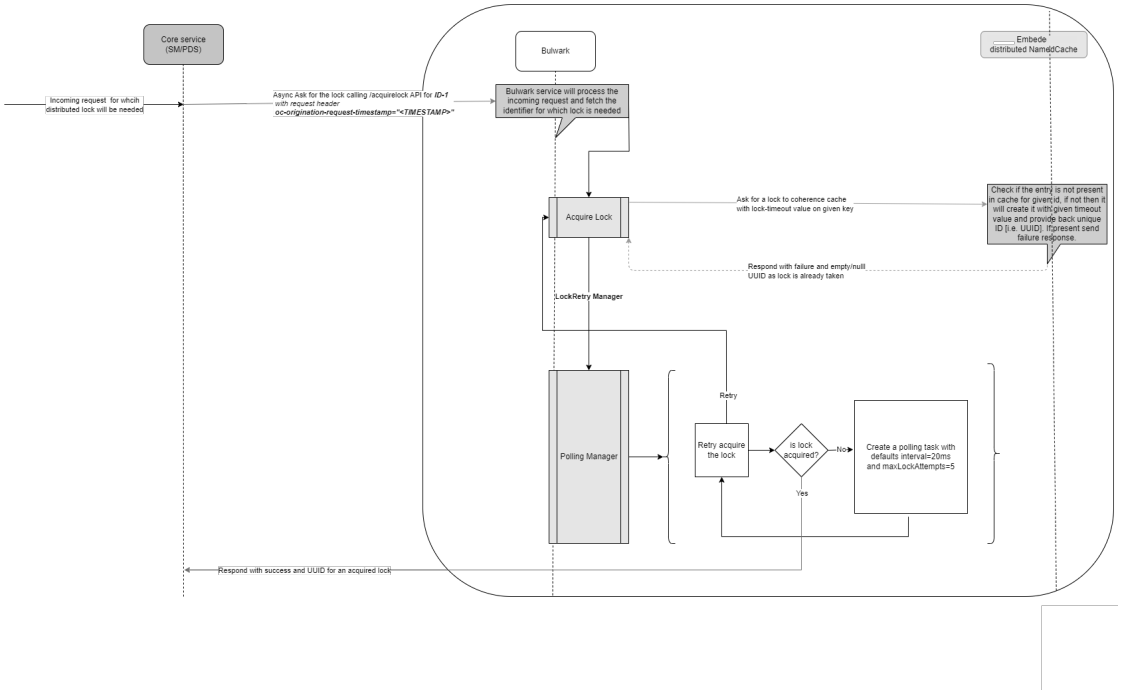
The maximum number of times Bulwark service can retry to attempt the lock can be configured using `polling.maxLockAttempts` Helm parameter.

> **Note**
>
> Bulwark service supports Long polling functionality for both single and multi keys.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

Figure 4-108 If lock is not available. Register for Long polling mechanism with the configured polling interval (20ms) and max lock re-attempts (5)



1. In case of multiple Create, Update, Delete, Notify, Update Notify requests for the same subscriber, SM service or PDS request a lock for the SUPI or GPSI value from the Bulwark service.
2. Bulwark service processes the lock request and fetches the identifier for which the lock is required.
3. Bulwark service tries to gain a lock from its cache. If there is no existing lock held by the given identifier, Bulwark service acquires a lock with the specified timeout value and a unique identifier (UUID) for the acquired lock.
4. Bulwark service responds to SM service or PDS (lock requesting service) with the lock details.
5. If Bulwark service fails to acquire the lock, it creates a new polling task and retries to acquire the lock within the `lockWaitTimeout` period.
6. If `lockWaitTimeout` has expired, Bulwark service sends a 423 lock failure response to SM service or PDS which is requesting the lock.
7. If `lockWaitTimeout` has not yet expired, Bulwark service creates a polling task with the default configuration (`polling.interval`=20ms and `polling.maxLockAttempts`=5).
8. After every 20ms, Bulwark service checks if an existing lock is released and reattempts to acquire the lock.
9. If the acquire lock request fails, Bulwark service continues to check every 20ms to know the availability of a lock and reattempts to acquire the lock until the maximum number of reattempts (`polling.maxLockAttempts`) reaches 5.

Copyright © 2019, 2026, Oracle and/or its affiliates.

10. If Bulwark service acquires the lock during the reattempt, Bulwark service responds to SM service or PDS with the lock details.
11. If the maximum number of reattempts (`polling.maxLockAttempts`) reaches 5 and Bulwark service fails to acquire the lock, Bulwark service sends a 423 lock failure response to SM service or PDS which is requesting the lock.

> **Note**
>
> If feature is enabled at Bulwark service, if the `lockWaitTimeOut` is non-zero, and `oc-origination-request-timestamp` is present in the header, polling mechanism at Bulwark service will be enabled for that request.
>
> SM service or PDS must send the request initiation timestamp (`oc-origination-request-timestamp`) as header. Otherwise, retry mechanism can not be enabled for that request.
>
> Inoder to add the `oc-origination-request-timestamp` to the header in the lock request from SM service or PDS service to Bulwark service, the `LOCK_RETRY_MODE` must be either `SERVER_ONLY` or `CLIENT_AND_SERVER`.

Managing Notifications from Bulwark Service to the Service Requester When Lock is Released

Enable

This feature can be enabled/disabled either at SM service and/or PDS as well as Bulwark service.

This feature can be enabled/disabled at SM service by configuring `CONCURRENCY.LOCK_RETRY_MODE` advance settings key on **Session Management service** page under **Service Configurations** section in CNC Console.

This feature can be enabled/disabled at PDS by configuring `CONCURRENCY.LOCK_RETRY_MODE` advance settings key on **PDS Settings** page under **Service Configurations** section in CNC Console.

This feature can be enabled and configured at Bulwark service using the fields under **Server Retry On Already Locked Keys** section in **Bulwark Settings** page in CNC Console.

For more information, see Bulwark Settings

Configure

This feature can be configured using Helm parameters, CNC Console, and REST API.

To configure the polling functionality by Bulwark service using Helm parameters, configure `polling.interval` and `polling.maxLockAttempts` parameters.

To configure using CNC Console:

- Configure the fields under **Server Retry on-Already Locked Keys** section on **Bulwark Settings** page in CNC Console.
  For more information, see Bulwark Settings.
- To indicate whether the lock retry must be triggered under which service, configure the **CONCURRENCY.LOCK_RETRY_MODE** advanced settings key available under **PCF Session Management** and **PDS** pages in CNC Console.
  For more information, see:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- PCF Session Management
- PDS Settings

To configure using REST API, configure the parameters in the following APIs:

- Acquire Lock
- Release Lock
- Server Retry on already locked keys

For more information, see *Oracle Communications Cloud Native Core, Converged Policy REST API Guide*.

Observability

Metrics

The following metrics are used for this feature:

- lock_request_total
- lock_response_total
- lock_collision_total

For more information, see Bulwark Metrics.

Alerts

The following alerts are used for this feature:

- LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD
- LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD
- LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

For more information, see List of Alerts.

4.41 Support for Stale Requests Cleanup

Policy supports minimizing the processing of stale requests and stale responses by any of the Policy microservices.

The header part of every request that a microservice such as PCRF Core, SM service, or UE Policy service receives includes the timestamp of the request and the maximum time frame to receive the request.

If the time taken for a request to be received by the microservice is more than the maximum time frame specified in the header, then that request is considered as stale.

Similarly, if the time taken by the microservice to process the received request and send its response back to the requester such as Diameter Gateway or Ingress Gateway is more than the time frame specified, such a response is considered as stale response.

The Policy microservice stops further processing of such stale requests and responses and sends a 504 error to the requested NF.

The following sections describe how the stale requests and responses are detected and cleaned at each of the Policy microservices.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Currently, the stale request cleanup functionality is implemented for SM service, PCRF Core, Binding service, Diameter Connector, UDR Connector, UE Policy Service, and CHF Connector.

Stale Requests Cleanup for PCRF Core

A request from Diameter Gateway, PDS, PRE, or Usage Monitoring to PCRF Core is considered as stale when the request takes longer time than the configured time period to reach PCRF Core.

Also, a response from PCRF Core to Diameter Gateway, PDS, PRE, or Usage Monitoring is considered as stale, when PCRF Core takes a longer time than the configured time period to process a request and respond to any of these microservices.

Stale requests or responses by PCRF Core are detected using Attribute Value Pairs (AVPs) for Diameter requests, and using 3GPP headers for HTTP requests.

The following 3GPP headers are included in every request that comes to, or is sent by PCRF Core:

Table 4-106 3GPP Headers in HTTP Requests

Header	Definition
`3gpp-Sbi-Origination-Timestamp`	The header contains the date and time (with a millisecond granularity) when the originating entity initiated the request.
`3gpp-Sbi-Max-Rsp-Time`	This header may be used in a HTTP request to indicate the duration in milliseconds during which the HTTP client waits for a response.
`3gpp-Sbi-Sender-Timestamp`	The header contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated.

If there are no headers included in the Diameter requests, PCRF Core uses the following custom AVPs:

Table 4-107 Custom AVPs in Diameter Requests

Custom AVP	Definition
`OC-Origination-Time-Stamp`	The AVP contains the date and time (with a millisecond granularity) when the originating entity initiated the request.
`OC-Max-Response-Time`	This AVP indicates the duration in milliseconds during which the Diameter Gateway waits for a response.
`OC-Sender-Time-Stamp`	The AVP contains the date and time (with a millisecond granularity) at which a Diameter request or response is originated.

When `OC_Sender_Time_Stamp` AVP or `3gpp-Sbi-Sender-Timestamp` header is present, and (`currentTime` >= `OC_Sender_Time_Stamp` + `OC_Sender_Time_Stamp`), then PCRF Core stops processing the request and returns a 504 error response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

When the `OC_Sender_Time_Stamp` AVP is not present, but `OC_Origination_Time_Stamp` is present and (`currentTime` >= `OC_Origination_Time_Stamp` + `OC_Sender_Time_Stamp`), then PCRF Core stops processing the request and returns a 504 error response.

Ot`OC-Max-Response-Time`herwise, if `OC_Origination_Time_Stamp`, `OC_Sender_Time_Stamp`, or is not present in the headers, PCRF Core processes the request and sends the expected successful response to Diameter Gateway.

PCRF Core rejects the stale requests with the following error codes:

Table 4-108 Error Codes

Response	Default Value
Diameter Response	5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST)
HTTP Response	504 (Gateway Timeout)

When PCRF Core cancels a request, but the request is already sent to PDS, PRE, or Usage Monitoring service, then no cleanup is required.

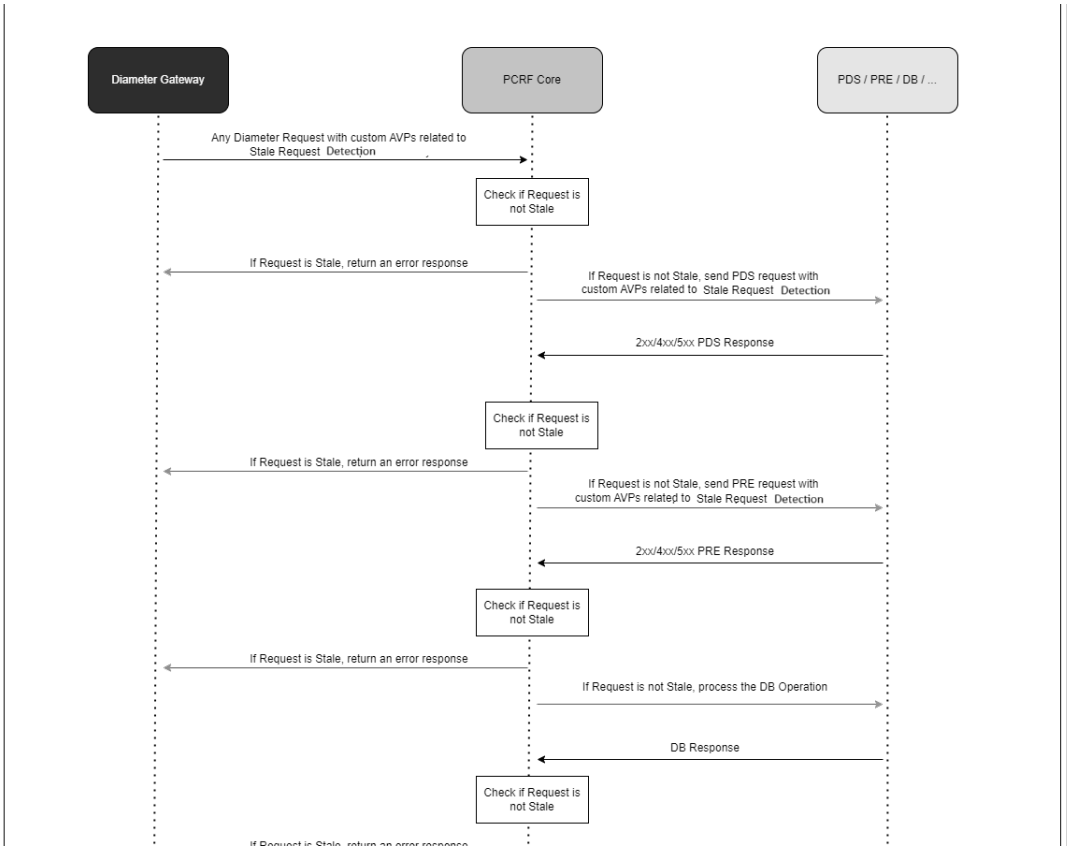
When PCRF Core cancels a request, but the request is already sent to Bulwark service, it is expected to free the lock related to the request.

> **Note**
>
> Any stale session being left behind by PCRF Core in other services, such as PDS, or Usage Monitoring is cleaned up during the audit cycle. PCRF Core does not send any cleanup request related to a stale request cancellation.

Call Flow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-109 Sample call flow for stale requests cleanup by PCRF Core



1. PCRF Core receives a request from Diameter Gateway containing either the custom AVPs or HTTP headers for stale request cleanup functionality.
2. PCRF Core verifies if the request is stale by checking the timestamp of the request.
3. If the request is stale, PCRF Core responds to Diameter Gateway with a 5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST) error.
4. If the request is not stale, PCRF Core sends a request to PDS with the timestamp headers. These headers are used to detect the staleness of the request.
5. PDS processes the request and sends a response back to PCRF Core.
6. PCRF Core verifies if the response received from PDS is stale.
7. If the response from PDS is stale, PCRF Core responds to Diameter Gateway with 5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST) error.
8. If the response from PDS is not stale, PCRF Core sends the request to PRE for evaluation.
9. PRE processes the request and responds to PCRF Core.
10. PCRF Core verifies if the response from PRE is stale.
11. If the response from PRE is stale, PCRF Core responds to Diameter Gateway with 5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST) error.
12. If the response from PRE is not stale, PCRF Core sends the details to be processed in the database and receives a response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

13. If the response for the database processing is stale, PCRF Core responds to Diameter Gateway with 5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST) error.
14. If the response for the database processing is not stale, PCRF Core sends the expected successful response to Diameter Gateway.

Stale Requests Cleanup for SM Service

A request from microservices such as Ingress Gateway to SM service is considered as stale when the request takes longer time than the configured time period to reach SM service.

Also, a response from SM service to the requesting microservice such as Ingress Gateway is considered as stale, when SM service takes a longer time than the configured time period to process a request and respond to any of these microservices.

Stale requests or responses by SM service are detected and cleaned using the following 3GPP headers:

- `3gpp-Sbi-Origination-Timestamp`
- `3gpp-Sbi-Max-Rsp-Time`
- `3gpp-Sbi-Sender-Timestamp`

When **ENABLE_LATE_PROCESSING** Advanced Settings key in **PCF Session Management** page under **Service Configurations** in CNC Console is enabled:

- If `3gpp-Sbi-Sender-Timestamp` header is present and `3gpp-Sbi-Sender-Timestamp` + `3gpp-Sbi-Max-Rsp-Time` is before the `current time`, it means the request has already timed out. Hence, the request gets canceled and SM service responds to Ingress Gateway with **504 (Gateway Timeout)** error.

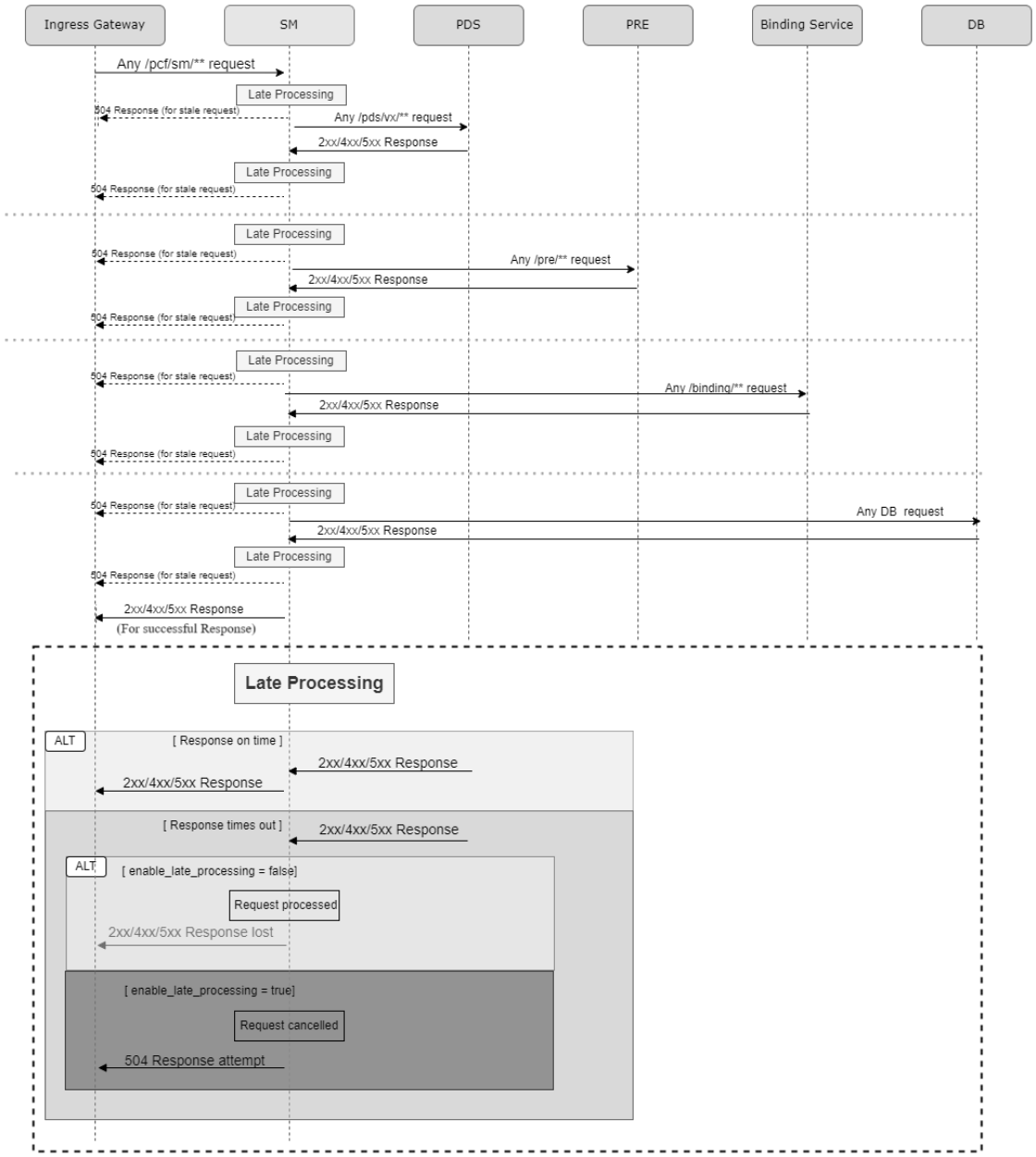
  > **Note**
  >
  > When **ENABLE_LATE_PROCESSING** is enabled, stale check filter responsible for returning **504 Error Response** takes precedence over other error response codes.

- If the `3gpp-Sbi-Sender-Timestamp` header is not present, but `3gpp-Sbi-Origination-Timestamp` is present and `3gpp-Sbi-Origination-Timestamp` + `3gpp-Sbi-Max-Rsp-Time` is before the `current time`, it means the request has already timed out. Hence, the request gets canceled. SM service responds to Ingress Gateway with **504 (Gateway Timeout)** error.
- Otherwise, if `3gpp-Sbi-Origination-Timestamp`, `3gpp-Sbi-Sender-Timestamp`, or `3gpp-Sbi-Max-Rsp-Time` are not present in the headers, SM service processes the request normally.

Call Flow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-110 Sample call flow for stale requests cleanup by SM Service



1. SM service receives a request from Ingress Gateway containing HTTP headers for stale request cleanup functionality.
2. SM service verifies if the request is stale by checking the timestamp of the request.
3. If the request is stale, SM service responds to Ingress Gateway with 504 error.
4. If the request is not stale, SM service sends the request to PDS containing the custom headers for stale request cleanup functionality.
5. PDS processes the request and sends a response back to SM service.
6. If PDS responds with a success message, SM service checks if the response is received within the configured time frame or if it is stale.
7. If the response from PDS is stale, SM service responds to Ingress Gateway with 504 error.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8. If the response from PDS is not stale, SM service sends the request to PRE for evaluation.
9. PRE processes the request and responds to SM service.
10. If PRE responds with a success message, SM service checks if the response is received within the configured time frame or if it is stale.
11. If the response from PRE is stale, SM service responds to Ingress Gateway with 504 error.
12. . If the response from PRE is not stale, SM service sends a request to Binding service to create the binding for the session.
13. Binding service processes the request and responds to SM service.
14. If Binding service responds with a success message, SM service checks if the response is received within the configured time frame or if it is stale.
15. If the response from Binding service is stale, SM service responds to Ingress Gateway with 504 error.
16. If the response from Binding service is not stale, SM service sends a request to other external databases for any database operation and receives a response.
17. If the response for the database processing is stale, SM service responds to Ingress Gateway with 504 error.
18. If the response for the database processing is not stale, SM service sends the expected successful response to Ingress Gateway.

> **Note**
>
> Currently, Policy does not support validating the staleness of the following requests in the SM service call flow:
>
> - Notification requests received from PDS
> - Notification response forwarded towards PDS
> - Staleness verification before sending notification request to PRE
> - Staleness verification after receiving notification response from PRE
> - Asynchronous requests sent towards PDS
> - Asynchronous requests forwarded towards Binding services
> - Signaling generated internally by PCF and coming to SM

Stale Requests Cleanup for Binding service

A request from SM service or PCRF Core to Binding service is considered as stale when the request takes longer time than the configured time period to reach Binding service.

Also, a response from Binding service is considered as stale, when Binding service takes a longer time than the configured time period to process a request and respond to any of these microservices.

Binding service validates the staleness of the request in the following scenarios:

- Whenever Binding service receives a request, it checks if the request has gone stale.
- While Binding service processes a request, it checks before or after performing a task that can take more time if the request has not gone stale.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Stale requests or responses by Binding service are detected and cleaned using 3GPP headers in HTTP requests.

The following 3GPP headers are included in every request that comes to, or is sent by Binding service:

Table 4-109 3GPP Headers in HTTP Requests

Header	Definition
3gpp-Sbi-Origination-Timestamp	The header contains the date and time (with a millisecond granularity) when the originating entity initiated the request. Example value: Fri, 29 Oct 2021 20:43:00.000 GMT
3gpp-Sbi-Max-Rsp-Time	This header may be used in a HTTP request to indicate the duration in milliseconds during which the HTTP client waits for a response. Example value: 3000
3gpp-Sbi-Sender-Timestamp	The header contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated. Example value: Tue, 15 Oct 2030 16:53:35.000 GMT

The stale request cleanup feature for Binding service can be enabled by configuring the value of ENABLE_LATE_ARRIVAL and ENABLE_LATE_PROCESSING advanced settings key for Binding Service on CNC Console to true. By default, the value of these keys are set to false.

A request is identified as stale based on the following criteria:

- When ENABLE_LATE_ARRIVAL advanced settings key for Binding service is enabled on CNC Console, and if the Sender_Timestamp header/AVP is present and currentTime - sender_timestamp > max_response_time, Binding service stops processing the request and returns a 504 (Gateway Timeout) error response.
- When ENABLE_LATE_ARRIVAL advanced settings key for Binding service is enabled on CNC Console, and if the Sender_Timestamp header is not present, but Origination_Timestamp is present and currentTime >= Origination_Timestamp + Max_Response_Time, Binding service stops processing the request and returns a 504 (Gateway Timeout) error response.
- When both Origination_Timestamp and Sender_Timestamp are not present in the header, Binding service considers the late arrival feature as disabled and processes the request normally.

Late arrival requests: Whenever Binding service receives a request, it determines if the received request has gone stale or not upon request arrival based on the timestamp in the header. ENABLE_LATE_ARRIVAL is used to check the staleness of the request when a request is received (before doing any time consuming operations). This task is performed in bounded elastic thread just at the moment it changes from XNIO thread to bounded elastic in Binding service.

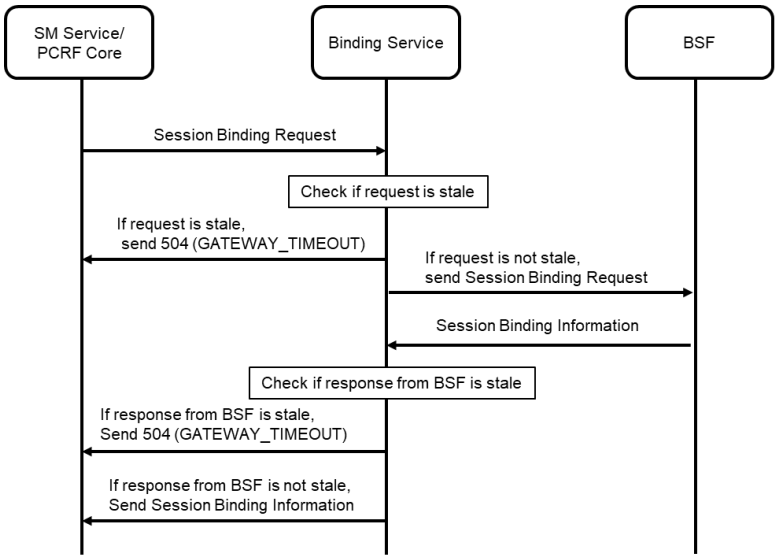
Late processing: Whenever Binding service starts processing a request, each time a response is obtained from BSF, it determines if the original request is still on time. ENABLE_LATE_PROCESSING is used to check the staleness of the request further in the flow (after the database operations and responses from BSF).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Whenever Binding service rejects a request, it returns a 504 (Gateway Timeout) error response. 504 (Gateway Timeout) is the default value of the error response, which can be configured using the Advanced Settings keys for Binding service in CNC Console.

Call Flow

Figure 4-111 Sample call flow for stale requests cleanup by Binding service



1. Binding service receives a request from SM service or PCRF Core through Diameter Gateway containing HTTP headers for stale request cleanup functionality.
2. Binding service verifies if the request is stale by checking the timestamp of the request.
3. If the request is stale, Binding service responds to SM service or PCRF Core through Diameter Gateway with a 504 (GATEWAY_TIMEOUT) error.

   If the request is not stale, Binding service sends a Session Binding Request to BSF.

   Binding service saves the session binding information received from BSF in `context_binding` table.
4. Binding service verifies if the response from BSF is stale.
5. If the response from BSF is stale, Binding service stops the further database operation for limiting the number of sessions and responds to SM service or PCRF Core through Diameter Gateway with a 504 (GATEWAY_TIMEOUT) error.
6. If the response from BSF is not stale, Binding service responds to SM service or PCRF Core through Diameter Gateway with session binding information.

Stale Requests Cleanup for Diameter Connector

All requests from Policy microservices such as SM service or PCRF Core to Diameter Gateway is passed through Diameter Connector. Such requests originated from Policy microservices are considered stale at Diameter Connector when the request takes longer time than the configured time period to reach Diameter Connector.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Also, a response from Diameter Connector to other Policy microservices is considered as stale, when Diameter Connector takes a longer time than the configured time period to process a request and respond to any of these microservices.

Stale requests cleanup functionality for Diameter Connector can be enabled using `enable.late.arrival` and `enable.late.processing` fields in **Diameter Connector** page under **Service Configurations** in CNC Console.

By default, this functionality is disabled.

Stale requests or responses by Diameter Connector are detected and cleaned using Attribute Value Pairs (AVPs) for Diameter requests and using 3GPP headers for HTTP requests.

The following 3GPP headers are included in every request that comes to, or is sent by Diameter Connector:

Table 4-110 3GPP Headers in HTTP Requests

Header	Definition
`3gpp-Sbi-Origination-Timestamp`	The header contains the date and time (with a millisecond granularity) when the originating entity initiated the request. Example: `Fri, 29 Oct 2021 20:43:00.000 GMT`
`3gpp-Sbi-Max-Rsp-Time`	This header may be used in a HTTP request to indicate the duration in milliseconds during which the HTTP client waits for a response. Example: `3000`
`3gpp-Sbi-Sender-Timestamp`	The header contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated. Example: `Tue, 15 Oct 2030 16:53:35.000 GMT`

If there are no headers included in the requests, Diameter Connector uses the following custom AVPs:

Table 4-111 Custom AVPs in Diameter Requests

Custom AVP	Definition
`Origination_Timestamp`	The AVP contains the date and time (with a millisecond granularity) when the originating entity initiated the request. Example: `Fri, 29 Oct 2021 20:43:00.000 GMT`
`Max_Response_Time`	This AVP indicates the duration in milliseconds during which the HTTP client waits for a response. Example: `3000`
`Sender_Timestamp`	The AVP contains the date and time (with a millisecond granularity) at which a Diameter request or response is originated. Example: `Tue, 15 Oct 2030 16:53:35.000 GMT`

Copyright © 2019, 2026, Oracle and/or its affiliates.

When `Sender_Timestamp` AVP or `3gpp-Sbi-Sender-Timestamp` header is present, and (`currentTime` >= `Sender_Timestamp` + `Max_Response_Time`), then stop processing the request and return 504 or 5454 error response.

When `Sender_Timestamp` AVP or `3gpp-Sbi-Sender-Timestamp` header is not present, and (`currentTime` >= `Origination_Timestamp` + `Max_Response_Time`), stop processing the request and return 504 or 5454 error response.

Otherwise, if `Origination_Timestamp`, `Sender_Timestamp`, or `Max_Response_Time` are not present in the headers, process the request normally.

Late arrival requests: In the event where the resulting time of `3gpp-Sbi-Origination-Timestamp + 3gpp-Sbi-Max-Rsp-Time` is in the past, Diameter Connector rejects the message with 504 or 5454 error response.

Late processing: Whenever Diameter-Gateway processes a request, each time a response is obtained from a microservice such as SM service, it determines if the original request is still on time. This process is known as late processing

Diameter Connector rejects the stale requests with the following error codes:

Table 4-112 Error Codes

Response	Default Value
Diameter Response	5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST)
HTTP Response	504 (Gateway Timeout)

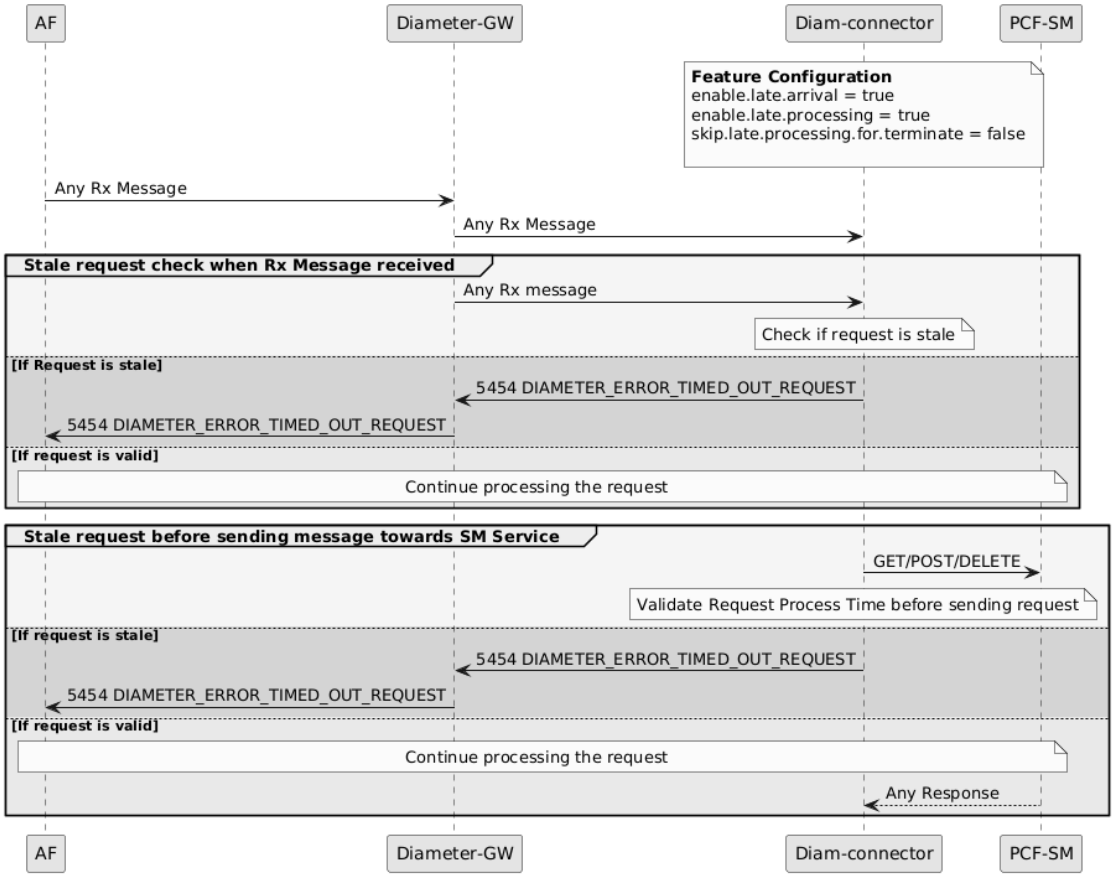
Skipping stale request cleanup for terminate requests
By default, when stale request cleanup for late arrival and late processing requests is enabled, Diameter Connector checks for all types of incoming requests. However, Diameter Connector can be configured to skip this check for TERMINATE requests, as sometimes it is not desirable to leave stale sessions on other services or databases.

This skipping the stale request cleanup for TERMINATE requests can be configured using **Skip Late Processing For Terminate** field under **Diameter Connector** page for **Service Configurations** in CNC Console.

Call Flow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-112 Sample call flow for stale Rx requests cleanup by Diameter Connector

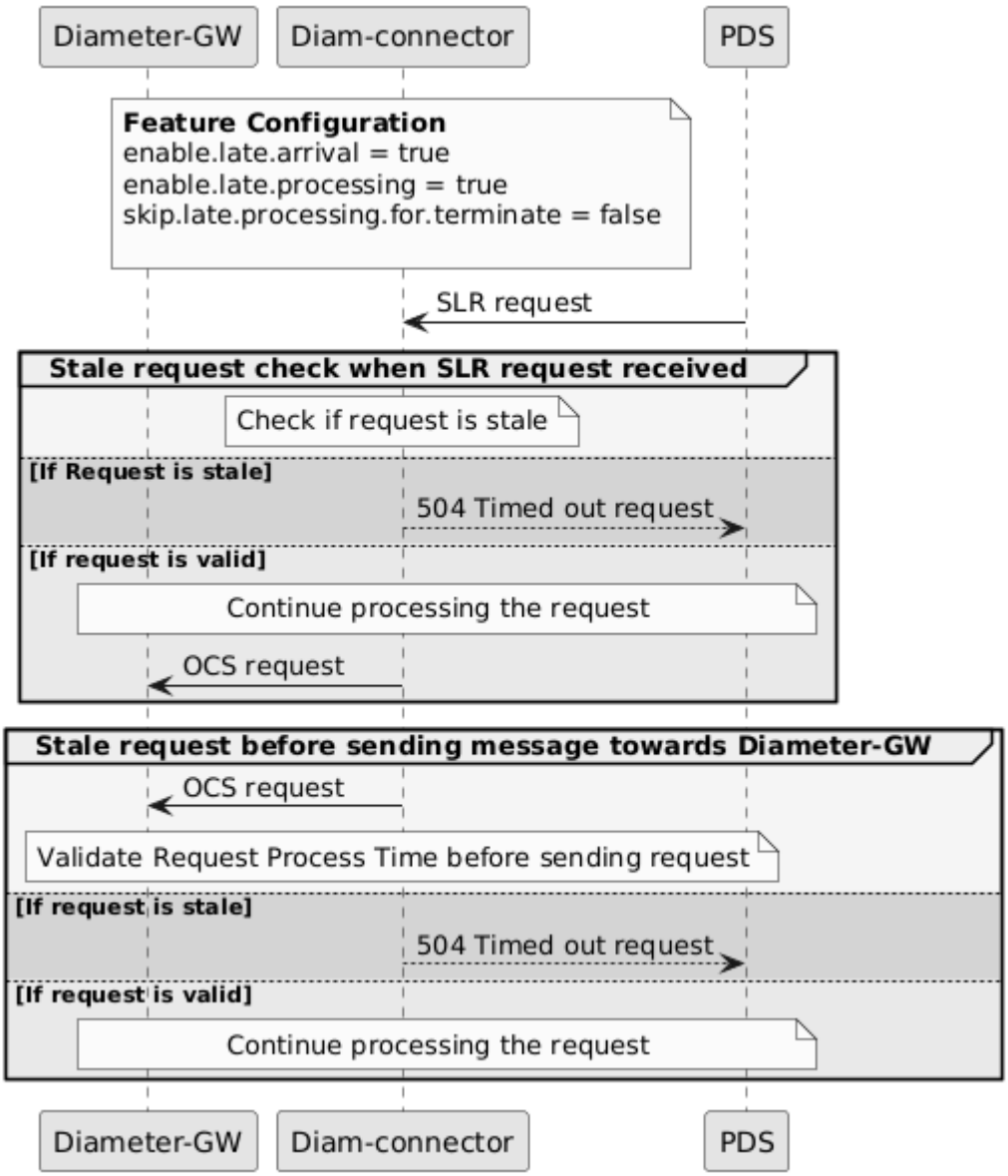


1. Diameter Connector receives a request from AF through Diameter Gateway containing either the custom AVPs or HTTP headers for stale request cleanup functionality.

   In this case, stale request cleanup for late arrival requests is enabled (`enable.late.arrival=true`)) and stale request cleanup for late processing requests is enabled (`enable.late.processing=true` and skip stale request cleanup for TERMINATE requests is disabled (`skip.late.processing.for.terminate=false`).
2. Diameter Connector verifies if the request is stale by checking the timestamp of the request.
3. If the request is stale, Diameter Connector responds to Diameter Gateway with a 5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST) error.
4. If the request is not stale, Diameter Connector sends the request to SM service for further processing of the request with the custom AVPs or custom headers for stale request cleanup functionality.
5. SM service processes the request and sends a response back to Diameter Connector.
6. Diameter Connector verifies if the response received from SM service is stale.
7. If the response from SM service is stale, Diameter Connector responds to Diameter Gateway with 5454 (DIAMETER_ERROR_TIMED_OUT_REQUEST) error.
8. If the response from SM service is not stale, Diameter Connector continues further processing of the RX request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-113 Sample call flow for stale SLR requests cleanup by Diameter Connector



1. Diameter Connector receives an SLR request from PDS containing either the custom AVPs or HTTP headers for stale request cleanup functionality.

   In this case, stale request cleanup for late arrival requests is enabled (`enable.late.arrival=true`)) and stale request cleanup for late processing requests is enabled (`enable.late.processing=true` and skip stale request cleanup for TERMINATE requests is disabled (`skip.late.processing.for.terminate=false`).
2. Diameter Connector verifies if the SLR request is stale by checking the timestamp of the request.
3. If the request is stale, Diameter Connector responds to PDS with a 504 (GATEWAY_TIME_OUT_REQUEST) error.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. If the request is not stale, Diameter Connector sends the request to OCS for further processing of the request with the custom AVPs or custom headers for stale request cleanup functionality.
5. OCS processes the request and sends a response back to Diameter Connector.
6. Diameter Connector verifies if the response received from OCS is stale.
7. If the response from OCS is stale, Diameter Connector responds to PDS with a 504 (GATEWAY_TIME_OUT_REQUEST) error.
8. If the response from OCS is not stale, Diameter Connector continues further processing of the SLR request.

Stale Requests Cleanup for User Service (CHF Connector or UDR Connector)

Whenever User Service (UDR Connector or CHF Connector) receives a request from PDS, it is possible that either the request takes too much time to be received or User Service takes too much time to process the request and send back a response. User Service identifies such requests as stale requests if it takes longer than the configured time to reach the destination. User Service stops further processing of such stale requests and rejects them with 504 (Gateway Timeout) error.

A request from PDS to User Service is considered as stale when the request takes longer time than the configured time period to reach User Service (CHF Connector or UDR Connector).

Also, a response from User Service to PDS is considered as stale, when User Service takes a longer time than the configured time period to process a request and respond to any of these microservices.

> **Note**
>
> Currently, this feature does not validate the staleness of the notification requests received from CHF or UDR to User Service.
>
> User Service forwards the notifications from CHF and UDR to PDS without any validation.
>
> PDS must be configured to handle cleanup of any stale requests received from CHF or UDR.

The stale request cleanup functionality for User Service (CHF Connector or UDR Connector) can be enabled either using Helm parameters at the time of installation or using the following Advanced Settings keys on **User Service** page under **Service Configurations** in CNC Console:

- `CHF.enable.late.arrival`
- `UDR.enable.late.arrival`
- `CHF.enable.late.processing`
- `UDR.enable.late.processing`
- `CHF.skip.late.processing.for.terminate`
- `UDR.skip.late.processing.for.terminate`

Helm parameters:

- `CHF.enableLateArrival`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- CHF.enableLateProcessing
- CHF.skipLateProcessingForTerminate
- UDR.enableLateArrival
- UDR.enableLateProcessing
- UDR.skipLateProcessingForTerminate

Stale requests or responses by User Service are detected and cleaned using 3GPP headers for HTTP requests.

The following 3GPP headers are included in every request that comes to, or is sent by User Service:

Table 4-113 3GPP Headers in HTTP Requests

Header	Definition
3gpp-Sbi-Origination-Timestamp	The header contains the date and time (with a millisecond granularity) when the originating entity initiated the request. Example: Fri, 29 Oct 2021 20:43:00.000 GMT
3gpp-Sbi-Max-Rsp-Time	This header may be used in a HTTP request to indicate the duration in milliseconds during which the HTTP client waits for a response. Example: 3000 **Note**: If the external NF provides negative MRT then it will not be considered and the stale checks will not fail for any requests based on MRT. Currently, the 3gpp-Sbi-Max-Rsp-Time header is not readjusted in any microservice to account for the processing time needed for the individual microservices. Hence when PDS sends this header to User Service it does not keep any buffer time itself to process a data in case User Service sends back the response in the verge of timeout. Cleanup of any CHF subscription will not be triggered by PDS automatically. For validation of such requests, there must be a provision kept by the caller microservice to modify the headers to subtract some time from 3gpp-Sbi-Max-Rsp-Time to account for it's own processing time.
3gpp-Sbi-Sender-Timestamp	The header contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated. Example: Tue, 15 Oct 2030 16:53:35.000 GMT

When Sender_Timestamp AVP or 3gpp-Sbi-Sender-Timestamp header is present, and (currentTime >= Sender_Timestamp + Max_Response_Time), then stop processing the request and return 504 error response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

When `Sender_Timestamp` AVP or `3gpp-Sbi-Sender-Timestamp` header is not present, and (`currentTime` >= `Origination_Timestamp` + `Max_Response_Time`), stop processing the request and return 504 error response.

Otherwise, if `Origination_Timestamp`, `Sender_Timestamp`, or `Max_Response_Time` are not present in the headers, process the request normally.

Late arrival requests: Whenever User Service receives a request, it determines if the received request has gone stale or not upon request arrival.

Late processing requests: Whenever User Service starts processing a request, each time a response is obtained from another service (NRF Client, Alternate Route Service), it determines if the original request is still on time.

> **Note**
>
> Irrespective of the type of request that user Service receives, if the request includes the required headers, User Service performs late arrival stale checks if it is enabled. But, it may not perform the late processing check as notification requests are not checked in late processing part.

By default, User Service does not perform any cleanup of stale requests. Changes made to other services remains until an audit process identifies these sessions as stale and removes them.

> **Note**
>
> If SBI TIMER is enabled and origination timestamp is sent, STS is prioritized over OTS and STS is generated by User Service when SBI TIMER is enabled in User Service and no STS is sent. Hence, late arrival check will not be performed, but late processing check can happen in self populated STS value.

Skipping Stale Request check for Terminate Requests

When `UDR.skipLateProcessingForTerminate` or `CHF.skipLateProcessingForTerminate` Helm parameters are enabled, or if the value of `UDR.skip.late.processing.for.terminate` or `CHF.skip.late.processing.for.terminate` Advanced Settings key is set to `true`, User Service skips validating the staleness of the TERMINATE requests.

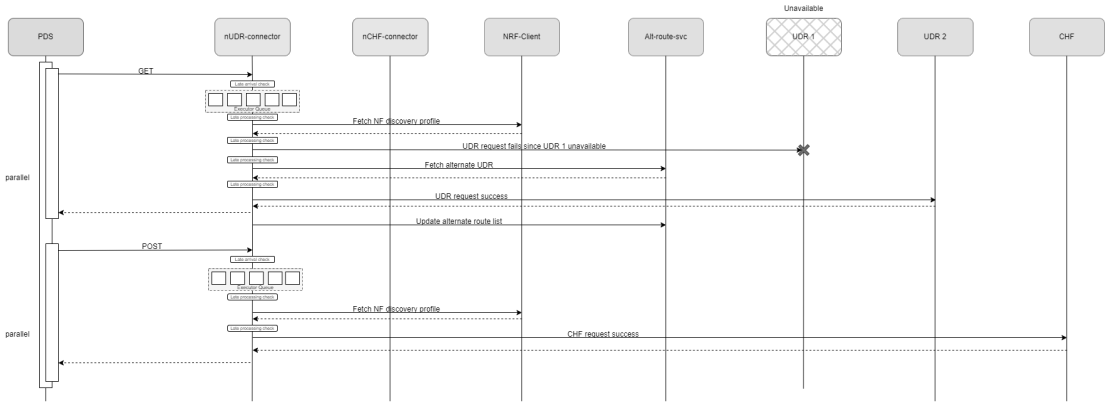
Validation of the TERMINATE requests are skipped only in case of late processing.

Late arrival TERMINATE requests are rejected similar to the other late arrival requests.

Call Flow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-114 Sample call flow for stale requests cleanup by User Service



1. User Service (nCHF Connector or nUDR Connector) receives a GET request from PDS containing the HTTP headers for stale request cleanup functionality.
2. User Service (nCHF Connector or nUDR Connector) verifies if the request is stale by checking the timestamp of the request.
3. If the request is stale, User Service (nCHF Connector or nUDR Connector) responds to PDS with a 504 (GATEWAY_TIME_OUT) error.
4. If the request is not stale, User Service (nCHF Connector or nUDR Connector) sends a request to NRF Client containing the custom headers for stale request cleanup functionality to discover the CHF or UDR profile.
5. If the response from NRF Client to User Service (nCHF Connector or nUDR Connector) is stale, User Service (nCHF Connector or nUDR Connector) responds to PDS with a 504 (GATEWAY_TIME_OUT) error.
6. If the response from NRF Client to User Service (nCHF Connector or nUDR Connector) is not stale, User Service (nCHF Connector or nUDR Connector) sends the request to the discovered CHF or UDR instance.
7. User Service (nCHF Connector or nUDR Connector) sends the response received from CHF or UDR to PDS.
8. When User Service (nCHF Connector or nUDR Connector) receives a POST (Subscription) request from PDS, it verifies if the request is stale.
9. If the received POST request is stale, User Service (nCHF Connector or nUDR Connector) responds to PDS with a 504 (GATEWAY_TIME_OUT) error.
10. If the received POST request is not stale, User Service (nCHF Connector or nUDR Connector) sends a request to NRF Client containing the custom headers for stale request cleanup functionality to discover the CHF or UDR profile.
11. If the response from NRF Client to User Service (nCHF Connector or nUDR Connector) is stale, User Service (nCHF Connector or nUDR Connector) responds to PDS with a 504 (GATEWAY_TIME_OUT) error.
12. If the response from NRF Client to User Service (nCHF Connector or nUDR Connector) is not stale, User Service (nCHF Connector or nUDR Connector) sends the POST request to the discovered CHF or UDR instance.
13. User Service (nCHF Connector or nUDR Connector) sends the response received from CHF or UDR to PDS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

14. If there is a delay of response from external UDR/CHF and feature is enabled, User Service (nCHF Connector or nUDR Connector) closes the channel once Max-Response-Time is reached and responds to PDS with 500 (INTERNAL_SERVER_ERROR) error.

> **Note**
>
> Stale request functionality for the above mentioned calls are implemented for synchronous calls only.

Stale Requests Cleanup for UE Policy service

A request from Ingress Gateway, PDS, PRE, or Bulwark service to UE Policy service is considered as stale when the request takes longer time than the configured time period to reach UE Policy service.

Also, a response from UE Policy service to Ingress Gateway, PDS, PRE, or Bulwark service is considered as stale, when UE Policy service takes a longer time than the configured time period to process a request and respond to any of these microservices.

UE Policy service validates the staleness of the request in the following scenarios:

- Whenever UE Policy service receives a request, it checks if the request has gone stale.
- While UE Policy service processes a request, it checks before or after performing a task that can take more time if the request has not gone stale.
- Currently, N1N2 notification requests received are not considered for stale request cleanup.

> **Note**
>
> Asynchronous requests are not considered when handling stale requests. The response received for asynchronous request should not affect or impact the original request check. An example of this asynchronous request is N1N2 Transfer messages.

Stale requests or responses by UE Policy service are detected and cleaned using 3GPP headers in HTTP requests.

The following 3GPP headers are included in every request that comes to, or is sent by UE Policy service:

Table 4-114 3GPP Headers in HTTP Requests

Header	Definition
`3gpp-Sbi-Origination-Timestamp`	The header contains the date and time (with a millisecond granularity) when the originating entity initiated the request. Example value: `Fri, 29 Oct 2021 20:43:00.000 GMT`
`3gpp-Sbi-Max-Rsp-Time`	This header may be used in a HTTP request to indicate the duration in milliseconds during which the HTTP client waits for a response. Example value: 3000

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-114 (Cont.) 3GPP Headers in HTTP Requests

Header	Definition
3gpp-Sbi-Sender-Timestamp	The header contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated. Example value: Tue, 15 Oct 2030 16:53:35.000 GMT

A request is identified as stale based on the following criteria:

- When the Sender_Timestamp header/AVP is present and currentTime >= Sender_Timestamp + Max_Response_Time, UE Policy service stops processing the request and returns a 504 (Gateway Timeout) error response.
- When the Sender_Timestamp header is not present, but Origination_Timestamp is present and currentTime >= Origination_Timestamp + Max_Response_Time, UE Policy service stops processing the request and returns a 504 (Gateway Timeout) error response.
- Otherwise, Origination_Timestamp, Sender_Timestamp, or Max_Response_Time are not present in the header, UE Policy service processes the request normally.

Late arrival requests: Whenever UE Policy service receives a request, it determines if the received request has gone stale or not upon request arrival based on the timestamp in the header.

Late processing: Whenever UE Policy service starts processing a request, each time a response is obtained from another service such as PDS, PRE, or Bulwark service, it determines if the original request is still on time.

Whenever UE Policy service rejects a request, it returns a 504 (Gateway Timeout) error response.

> **Note**
>
> By default, UE Policy service does not perform a cleanup whenever a request has gone stale. Changes made to other services will remain until an Audit process identifies these sessions as stale and removes them.
>
> However, if required, the cleanup functionality can be enabled either by configuring enableLateProcessingCleanup, helm parameter and ENABLE_LATE_PROCESSING_CLEANUP environmental variable, or by configuring ENABLE_LATE_PROCESSING_CLEANUP advanced setting key for UE Policy service in CNC Console.

Skipping Stale Request Cleanup for Terminate Requests:

When late processing is enabled, UE Policy service checks for all types of requests being processed. But, UE Policy service can skip this check for Terminate requests, as sometimes it is not desirable to leave stale sessions on other services or databases.

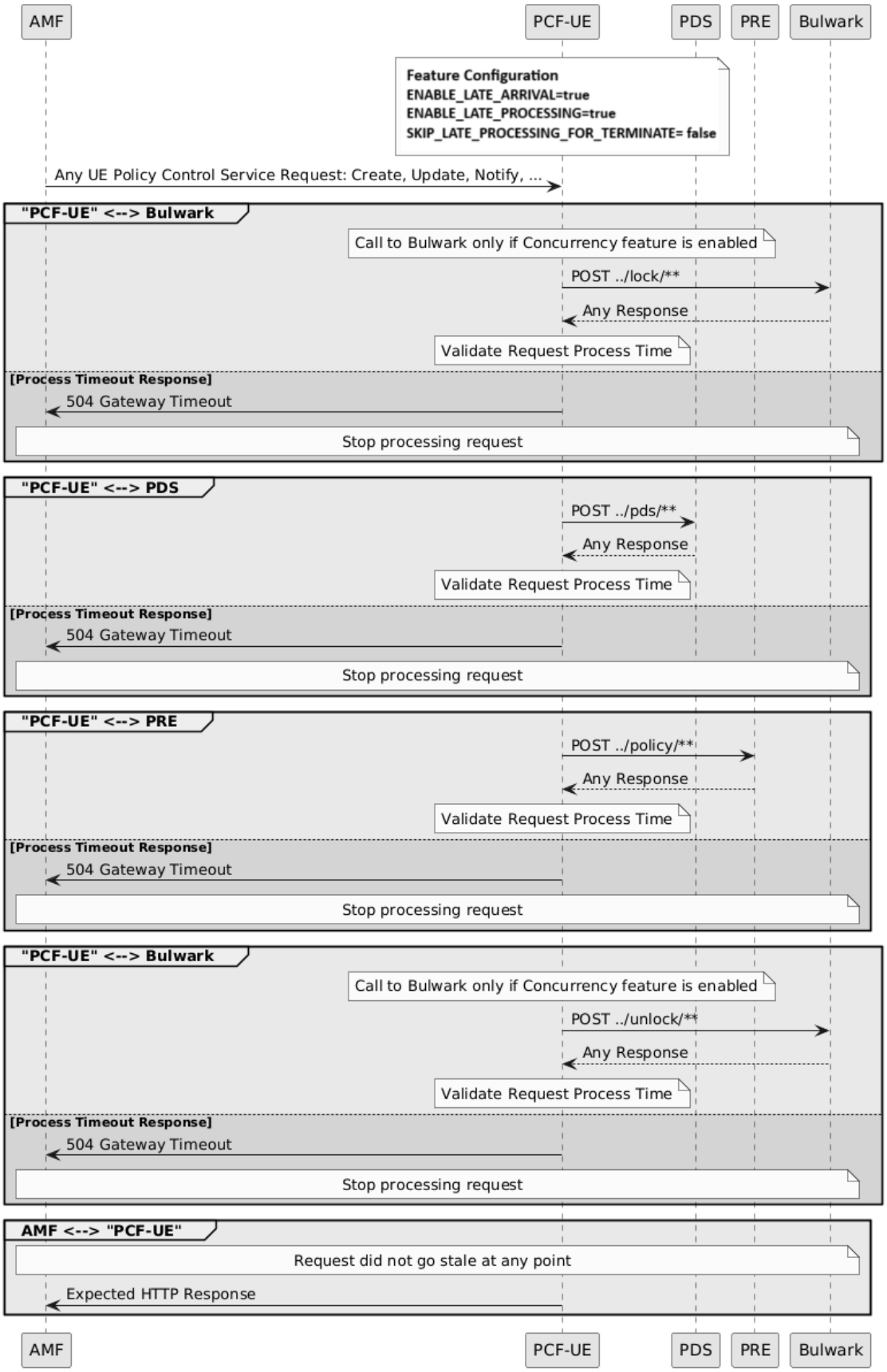
This feature can be enabled either by configuring skipLateProcessingForTerminate Helm parameter and SKIP_LATE_PROCESSING_FOR_TERMINATE environmental variable, or by configuring skip.late.processing.for.terminate advanced settings key for UE Policy service in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-115 Sample call flow for stale requests cleanup by UE Policy service



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. UE Policy service receives a request from AMF through Ingress Gateway containing HTTP headers for stale request cleanup functionality.

   The configuration for UE service in advance settings is the following:

   - ENABLE_LATE_ARRIVAL=true
   - ENABLE_LATE_PROCESSING=true
   - SKIP_LATE_PROCESSING_FOR_TERMINATE=true
2. UE Policy service verifies if the request is stale by checking the timestamp of the request.
3. If the request is stale, UE Policy service responds to AMF through Ingress Gateway with a 504 (GATEWAY_TIMEOUT) error.

   If the request is not stale, UE Policy service sends a acquire lock request to Bulwark service.

   UE Policy service verifies if the response from Bulwark service is stale.
4. If the response from Bulwark service is stale, UE Policy service responds to AMF through Ingress Gateway with a 504 (GATEWAY_TIMEOUT) error.
5. If the response from Bulwark service is not stale, UE Policy service sends a request to PDS with the custom headers for stale request cleanup functionality.
6. PDS processes the request and sends a response back to UE Policy service.
7. UE Policy service verifies if the response received from PDS is stale.
8. If the response from PDS is stale, UE Policy service responds to AMF through Ingress Gateway with a 504 (GATEWAY_TIMEOUT) error.
9. If the response from PDS is not stale, UE Policy service sends the request to PRE for evaluation.
10. PRE processes the request and responds to UE Policy service.
11. UE Policy service verifies if the response from PRE is stale.
12. If the response from PRE is stale, UE Policy service responds to AMF through Ingress Gateway with a 504 (GATEWAY_TIMEOUT) error.
13. If the response from PRE is not stale, UE Policy service sends the details to be processed in the database and receives a response.
14. If the response for the database processing is stale, UE Policy service responds to AMF through Ingress Gateway with a 504 (GATEWAY_TIMEOUT) error.
15. If the response for database processing is not stale, UE Policy service sends unlock request to Bulwark service.
16. UE Policy service verifies if the response from Bulwark service is stale.
    If the response is stale, UE Policy service responds to AMF through Ingress Gateway with a 504 (GATEWAY_TIMEOUT) error.
17. If the response from Bulwark service is not stale, UE Policy service sends the expected successful response to AMF through Ingress Gateway.

Managing Stale Requests Cleanup

Managing Stale Requests Cleanup for PCRF Core

Enable

Stale requests cleanup functionality for PCRF Core can be enabled either using `ENABLE_LATE_ARRIVAL` and `ENABLE_LATE_PROCESSING` Helm parameters at the time of Policy

Copyright © 2019, 2026, Oracle and/or its affiliates.

installation or using `enable.late.arrival` `enable.late.processing` Advanced Settings key in **PCRF Core Settings** page under **Service Configurations** in CNC Console.

By default, this functionality is disabled.

For details on how to enable the functionality using Helm parameter, see *PCRF Core Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

For details on how to enable the functionality using CNC Console, see Settings.

Configure

Stale requests cleanup functionality for PCRF Core can be configured either using Helm parameters at the time of Policy installation or using CNC Console.

Configure using Helm parameters

Configure the following Helm parameters in `custom-values.yaml` file:

- `ENABLE_LATE_ARRIVAL`
- `ENABLE_LATE_PROCESSING`
- `LATE_ARRIVAL_MAX_RESPONSE_TIME`
- `SBI_TIMER_ENABLED`
- `SKIP_LATE_PROCESSING_FOR_TERMINATE`

For more information on these Helm parameters, see *PCRF-Core Configurations* and *Diameter Gateway and Diameter Connector Configuration* sections in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Configure using CNC console

Configure the following Advanced Settings keys in **PCRF Core Settings** page under **Service Configurations** in CNC Console:

- `enable.late.arrival`
- `enable.late.processing`
- `late.arrival.max.resp.time`
- `skip.late.processing.for.terminate`
- `sbi.timer.enabled`

For more information, see Settings.

> **Note**
>
> If there are no Advanced Settings related to stale request cleanup are present, then the Helm configurations will be used. However, if Advanced Settings are present, values of the Advanced Settings keys are used instead of Helm configurations.

Managing Stale Requests Cleanup for SM Service

Enable

Copyright © 2019, 2026, Oracle and/or its affiliates.

Stale request cleanup functionality for SM service can be enabled using **ENABLE_LATE_PROCESSING** Advanced Settings key in **PCF Session Management** page under **Service Configurations** in CNC Console.

By default, this functionality is disabled.

For more information, see PCF Session Management.

Configure

Configure the `ENABLE_LATE_PROCESSING` Advanced Settings keys in **PCF Session Management** page under **Service Configurations** in CNC Console:

For more information, see PCF Session Management.

Managing Stale Requests Cleanup for Binding service

Enable

Stale requests cleanup functionality for Binding service can be enabled either using `ENABLE_LATE_ARRIVAL` and `ENABLE_LATE_PROCESSING` Advanced Settings keys in **Binding Service** page under **Service Configurations** in CNC Console.

By default, this functionality is disabled.

For details on how to enable the functionality using CNC Console, see Binding Service.

Configure

Stale requests cleanup functionality for Binding service can be configured using CNC Console.

Configure using CNC console

Configure the following Advanced Settings keys in **Binding Service** page under **Service Configurations** in CNC Console:

- `ENABLE_LATE_ARRIVAL`
- `ENABLE_LATE_PROCESSING`

For more information, see Binding Service.

In configure `DIAMETER.Timer.Enabled` advanced settings key under **Settings** page for **Diameter Configuration** under **Service Configurations** in CNC Console.

For more information, see Settings.

Managing Stale Requests Cleanup for Diameter Connector

Enable

Stale requests cleanup functionality for Diameter Connector can be enabled using `enable.late.arrival` and `enable.late.processing` fields in **Diameter Connector** page under **Service Configurations** in CNC Console.

By default, this functionality is disabled.

For details on how to enable the functionality using CNC Console, see Diameter Connector.

Configure

Stale requests cleanup functionality for Diameter Connector can be configured using CNC Console.

Configure using CNC console

Copyright © 2019, 2026, Oracle and/or its affiliates.

Configure the following fields in **Diameter Connector** page under **Service Configurations** in CNC Console:

- `enable.late.arrival`
- `enable.late.processing`
- `skip.late.processing.for.terminate`
- `sbi.timer.enabled`

For more information, see Diameter Connector.

If diameter Gateway does not receive the timer AVPs in request, configure diameter Gateway to generate them and send them to Diam Connector by configuring **DIAMETER.Timer.Enabled** Advanced Settings key under **Diameter Configurations** page in **Service Configurations**.

For more information, see Settings.

Managing Stale Requests Cleanup for User Service (CHF Connector and UDR Connector)

Enable

The stale request cleanup functionality for User Service (CHF Connector and UDR Connector) can be enabled either using Helm parameters at the time of installation or using CNC Console.

By default, this functionality is disabled.

Enable using Helm parameters:

- `CHF.enableLateArrival`
- `CHF.enableLateProcessing`
- `CHF.skipLateProcessingForTerminate`
- `UDR.enableLateArrival`
- `UDR.enableLateProcessing`
- `UDR.skipLateProcessingForTerminate`

For more information on these Helm parameters, see *Enabling/Disabling Services Configurations* sections in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Enable using CNC Console:

Configure the following Advanced Settings keys on **User Service** page under **Service Configurations** in CNC Console:

- `CHF.enable.late.arrival`
- `UDR.enable.late.arrival`
- `CHF.enable.late.processing`
- `UDR.enable.late.processing`
- `CHF.skip.late.processing.for.terminate`
- `UDR.skip.late.processing.for.terminate`

For details on how to enable the functionality using CNC Console, see PCF User Connector.

Configure

Copyright © 2019, 2026, Oracle and/or its affiliates.

Stale requests cleanup functionality for User Service can be configured using Helm parameters at the time of installation or using CNC Console.

Configure using Helm parameters

- `CHF.enableLateArrival`
- `CHF.enableLateProcessing`
- `CHF.skipLateProcessingForTerminate`
- `UDR.enableLateArrival`
- `UDR.enableLateProcessing`
- `UDR.skipLateProcessingForTerminate`

For more information on these Helm parameters, see *Enabling/Disabling Services Configurations* sections in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Configure using CNC console

Configure the following Advanced Settings keys on **User Service** page under **Service Configurations** in CNC Console:

- `CHF.enable.late.arrival`
- `UDR.enable.late.arrival`
- `CHF.enable.late.processing`
- `UDR.enable.late.processing`
- `CHF.skip.late.processing.for.terminate`
- `UDR.skip.late.processing.for.terminate`

For details on how to enable the functionality using CNC Console, see PCF User Connector.

Managing Stale Requests Cleanup for UE Policy service

Enable

Stale requests cleanup functionality for UE Policy service can be enabled either using `enableLateArrival` and `enableLateProcessing` Helm parameters at the time of Policy installation or using `ENABLE_LATE_ARRIVAL` and `ENABLE_LATE_PROCESSING` Advanced Settings keys in **PCF UE Policy** page under **Service Configurations** in CNC Console.

By default, this functionality is disabled.

For details on how to enable the functionality using Helm parameter, see *Enabling/Disabling Services Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

For details on how to enable the functionality using CNC Console, see PCF UE Policy Service.

Configure

Stale requests cleanup functionality for UE Policy service can be configured either using Helm parameters at the time of Policy installation or using CNC Console.

Configure using Helm parameters

Configure the following Helm parameters in `custom-values.yaml` file:

- `enableLateArrival`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- `enableLateProcessing`
- `skipLateProcessingForTerminate`

For more information on these Helm parameters, see *Enabling/Disabling Services Configurations* sections in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Configure using CNC console

Configure the following Advanced Settings keys in **PCF UE Policy** page under **Service Configurations** in CNC Console:

- `ENABLE_LATE_ARRIVAL`
- `ENABLE_LATE_PROCESSING`
- `SKIP_LATE_PROCESSING_FOR_TERMINATE`

For more information, see PCF UE Policy Service.

> **Note**
>
> If there are no Advanced Settings related to stale request cleanup are present, then the Helm configurations will be used. However, if Advanced Settings are present, values of the Advanced Settings keys are used instead of Helm configurations.

Observability

Metrics

Metrics for PCRF Core

The following metrics are used for handling stale requests cleanup functionality for PCRF Core:

- occnp_stale_diam_request_cleanup_total
- occnp_stale_http_request_cleanup_total

For more information, see PCRF Core Metrics.

Metrics for SM service

The occnp_late_processing_rejection_total metric is used for handling stale requests cleanup functionality for SM service.

For more information, see SM Service Metrics.

Metrics for Binding service

The following metrics are used for handling stale requests cleanup functionality for Binding service:

- occnp_late_arrival_rejection_total
- occnp_late_processing_rejection_total

For more information, see Binding Service Metrics.

Metrics for Diameter Connector

Copyright © 2019, 2026, Oracle and/or its affiliates.

The `occnp_stale_diam_request_cleanup_total` metric is used for handling stale requests cleanup functionality for Diameter Connector:.For more information, see Diameter Connector Service Metrics.

Metrics for User Service

The following metrics are used for handling stale requests cleanup functionality for User Service:

- occnp_late_arrival_rejection_total
- occnp_late_processing_rejection_total

For more information, see User Service Metrics.

Metrics for UE Policy service

The ocpm_late_arrival_rejection_total and occnp_late_processing_rejection_total metrics are used for handling stale requests cleanup functionality for UE Policy service.

For more information, see UE Service Metrics.

Alerts

Alerts for PCRF Core

The following alerts are used for handling stale requests cleanup functionality for PCRF Core:

- STALE_DIAMETER_REQUEST_CLEANUP_MINOR
- STALE_DIAMETER_REQUEST_CLEANUP_MAJOR
- STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL

For more information, see Common Alerts.

Alerts for SM service

The following alerts are used for handling stale requests cleanup functionality for SM service:

- SM_STALE_REQUEST_PROCESSING_REJECT_MINOR
- SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR
- SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

For more information, see Common Alerts.

Alerts for Binding service

The following alerts are used for handling stale requests cleanup functionality for Binding service:

- STALE_BINDING_REQUEST_REJECTION_CRITICAL
- STALE_BINDING_REQUEST_REJECTION_MAJOR
- STALE_BINDING_REQUEST_REJECTION_MINOR

For more information, see Common Alerts.

Alerts for Diameter Connector

The following alerts are used for handling stale requests cleanup functionality for Binding service:

- STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MINOR
- STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MAJOR

Copyright © 2019, 2026, Oracle and/or its affiliates.

- STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL

For more information, see Common Alerts.

Alerts for User Service

The following alerts are used for handling stale requests cleanup functionality for User Service:

- CHF_C_STALE_HTTP_REQUEST_CLEANUP_MINOR
- CHF_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR
- CHF_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL
- UDR_C_STALE_HTTP_REQUEST_CLEANUP_MINOR
- UDR_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR
- UDR_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

For more information, see Common Alerts.

Alerts for UE Policy service

The following alerts are used for handling stale requests cleanup functionality for UE Policy service:

- UE_STALE_REQUEST_PROCESSING_REJECT_MINOR
- UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR
- UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL
- UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR
- UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR
- UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

For more information, see Common Alerts.

4.42 Support for Diameter Message Response Time Latency Metrics

CnPolicy Diameter Gateway implements latency metrics that provides the time taken to service a request/response in a Diameter call flow. This ensures that the cnPolicy meets the required service level agreements (SLAs) for latency as set by the Customer. The latency measurements are indicators of network health and stability. A sudden increase in latency value can signal an issue either within the cnPolicy or in its interactions with other network elements. Monitoring latency values helps the user to quickly identify and troubleshoot without leading to any service disruptions.

The following latency histogram metrics are implemented to track latency in Diameter Gateway:

- `occnp_diam_response_latency_seconds_bucket`: This metrics provides information on individual call latency time for any calls made by Diameter Gateway towards any network peers or internal back end services.
- `occnp_diam_response_latency_seconds_sum`: This metrics provides information on individual call latency time for any calls made by Diameter Gateway towards any network peers or internal back end services.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- `occnp_diam_response_latency_seconds_count`: This metrics provides information on individual call latency time for any calls made by Diameter Gateway towards any network peers or internal back end services.
- `occnp_diam_response_latency_seconds_max`: This metrics provides information on individual call latency time for any calls made by Diameter Gateway towards any network peers or internal back end services.
- `occnp_diam_service_overall_processing_time_seconds_bucket`: This metrics provide an overall time tracking latency for any request towards Diameter Gateway.
- `occnp_diam_service_overall_processing_time_seconds_sum`: This metrics provide an overall time tracking latency for any request towards Diameter Gateway.
- `occnp_diam_service_overall_processing_time_seconds_count`: This metrics provide an overall time tracking latency for any request towards Diameter Gateway.
- `occnp_diam_service_overall_processing_time_seconds_max`: This metrics provide an overall time tracking latency for any request towards Diameter Gateway.

For Diameter Gateway, a sample of the histogram latency bucket and percentile ranges in milliseconds is provided:

```
diam_response_latency.histogram.latency_bucket=1,2,3,4,6,8,10,20,30,40,60,80,1
00,200,300,400,600,800,1000,2000,3000,4000,6000,8000,10000,+inf
diam_response_latency.histogram.percentile=0.50, 0.90, 0.95, 0.99
```

Observability

Metrics:

The following common service metrics are used to provide information about this feature:

- `occnp_diam_service_overall_processing_time_seconds`

For more information about metrics, see Diameter Gateway Metrics section.

Maintain

To resolve any alerts at the system or application level, see Alerts section. In case the alerts still persist, perform the following:

- **Collect the logs**: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- **Raise a service request**: See My Oracle Support.

4.43 Support for TLS

Policy uses Hypertext Transfer Protocol Secure (HTTPS) to establish secured connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS).

TLS comprises the following components:

- **Handshake Protocol:** Exchanges the security parameters of a connection.
- **Record Protocol:** Receives the messages to be transmitted, fragments the data into multiple blocks, secures the records, and then transmits the result. Received data is delivered to higher-level peers.

Copyright © 2019, 2026, Oracle and/or its affiliates.

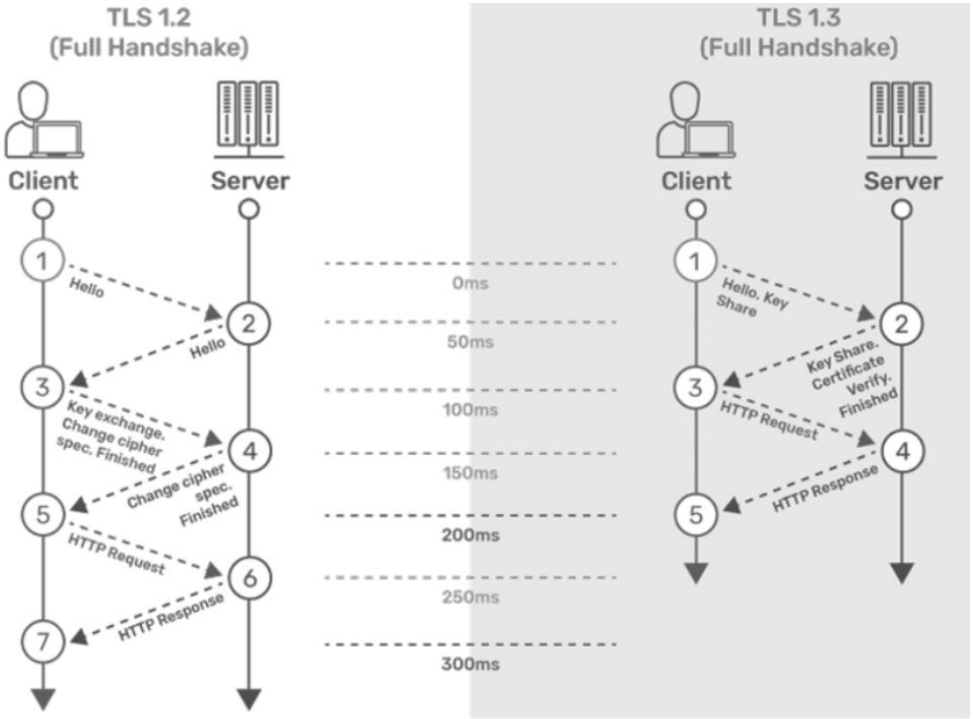
This feature enables the support for TLS 1.3 to all consumer NFs, producer NFs, the Data Director, SBI Interfaces, and any interfaces previously supporting TLS 1.2. Support for TLS 1.2 will remain available.

> **Note**
>
> If both TLS 1.2 and TLS 1.3 are supported, TLS 1.3 is given priority.

TLS 1.2 and TLS 1.3 Handshake

This section describes the differences between TLS 1.3 and TLS 1.2, as well as the advantages of TLS 1.3 over TLS 1.2 and earlier versions.

Figure 4-116 TLS 1.2 and TLS 1.3 Handshake



TLS 1.2

Step 1: The connection or handshake starts when the client sends a "client hello" message to the server. This message consists of cryptographic information such as supported protocols and cipher suites. It also contains a random value or random byte string.

Step 2: To respond to the "client hello" message, the server sends a 'server hello' message. This message contains the CipherSuite that the server has selected from the options provided by the client. The server also sends its certificate, along with the session ID and another random value.

Step 3: The client verifies the certificate sent by the server. When the verification is complete, it sends a byte string encrypted using the public key of the server's certificate.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Step 4: When the server receives the secret, both the client and server generate a master key along with session keys (ephemeral keys). These session keys are used for symmetrically encrypting the data.

Step 5: The client sends an "HTTP Request" message to the server to enable the server to transition to symmetric encryption using the session keys.

Step 6: To respond to the client's "HTTP Request" message, the server does the same and switches its security state to symmetric encryption. The server concludes the handshake by sending an HTTP response.

Step 7: The client-server handshake is completed in two round trips.

TLS 1.3
Step 1: The connection or handshake begins when the client sends a "client hello" message to the server, which includes the list of supported cipher suites and the client's key share for the specific key agreement protocol.

Step 2: To respond to the "client hello" message, the server sends the key agreement protocol that it has chosen. The "Server Hello" message includes the server key share, server certificate, and the "Server Finished" message.

Step 3: The client verifies the server certificate, generates keys since it has the server's key share, and then sends the "Client Finished" message along with an HTTP request.

Step 4: The server completes the handshake by sending an HTTP response.

> **Note**
>
> ASM and TLS are not supported together.

The following table provides comparison of TLS 1.2 with TLS 1.3:

Table 4-115 Comparison of TLS 1.2 with TLS 1.3

Feature	TLS 1.2	TLS 1.3
TLS Handshake	This is less efficient as it requires more round-trips to complete the handshake process.	This is more efficient as it requires less round-trips to complete the handshake process.
Cipher Suites	This has less secured Cipher Suites.	This has more secured Cipher Suites. They support the following ciphers: • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_AES_128_CCM_8_SHA256: This Cipher is not supported by Java library. • TLS_AES_128_CCM_SHA256: This Cipher is not supported by Java library.
Round-Trip Time (RTT)	This has higher RTT during TLS handshake.	This has low RTT.
Performance	This has higher latency during TLS handshake.	This has low latency during TLS handshake.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

- Policy does not prioritize cipher suites on the basis of priorities. To select cipher on the basis of priorities, you must write the cipher suites in the decreasing order of priority.
- Policy does not prioritize supported groups on the basis of priorities. To select supported group on the basis of priorities, you must write the supported group values in the decreasing order of priority.
- If you want to provide values for the signature_algorithms extension using the `clientSignatureSchemes` parameter, the following comma-separated values must be provided to deploy the pods:
  - rsa_pkcs1_sha512
  - rsa_pkcs1_sha384
  - rsa_pkcs1_sha256
- The mandatory extensions as listed in RFC 8446 cannot be disabled on the client or server side. The following is the list of the extensions that cannot be disabled:
  - supported_versions
  - key_share
  - supported_groups
  - signature_algorithms
  - pre_shared_key

The following digital signature algorithms of TLS 1.2 and TLS 1.3 are supported in TLS handshake:

Table 4-116 Digital Signature Algorithms

Algorithm	Key Size (Bits)	Elliptic Curve (EC)
RS256 (RSA)	2048	NA
	4096 This is the recommended value.	NA
ES256 (ECDSA)	NA	SECP384r1 This is the recommended value.

Note

The following functionalities from TLS 1.3 specifications are not supported:

- Zero round-trip time (0-RTT) mode.
- Pre-Shared Key (PSK) exchange.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.43.1 Support for TLS Using HTTPs

Policy uses Hypertext Transfer Protocol Secure (HTTPS) to establish secured connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS).

Enable

This feature is enabled by default at the time of Gateway Services deployment by completing the required Helm configurations.

Configure

You can configure this feature using Helm. For information about Helm configurations, see "Global Parameters" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Observe

The following metrics are available for this feature:

- oc_ingressgateway_incoming_tls_connections
- oc_egressgateway_outgoing_tls_connections
- security_cert_x509_expiration_seconds

For more information about metrics, see section TLS Metrics.

The following alerts are available for this feature:

- CERTIFICATE_EXPIRY_CRITICAL
- CERTIFICATE_EXPIRY_MAJOR
- CERTIFICATE_EXPIRY_MINOR
- POLICY_CONNECTION_FAILURE

For more information about alerts, see Alerts section.

Maintain
If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alert still persists, perform the following:

1. **Collect the logs and Troubleshooting Scenarios**: For more information on how to collect logs and troubleshooting information, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
2. **Raise a service request**: See My Oracle Support for more information on how to raise a service request.

4.43.2 Support for TLS in Diameter Gateway

Policy uses Diameter Gateway to establish secured connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Enable

This feature is disabled by default. It can be enabled using `TLS_ENABLED` parameter using Helm configurations. For information about Helm configurations, see "Global Parameters" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Configure

You can configure this feature using Helm. For information about Helm configurations, see "Global Parameters" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Peer level support for TLS versions can be configured using CNC Console. For more information, see Peer Nodes section.

Observe

The following metrics are available for this feature:

- diam_conn_network
- diam_failed_conn_network
- diam_conn_network_responder
- dgw_tls_cert_expiration_seconds

For more information about metrics, see TLS Metrics section.

The following alerts are available for this feature:

- DGW_TLS_CONNECTION_FAILURE
- DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR
- DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR
- DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

For more information about alerts, see Alerts section.

Following extensions are available for TLS in Diameter Gateway:

- status_request (0x0005)
- status_request_v2 (0x0011)
- supported_groups (0x000A)
- ec_point_formats (0x000B)
- extended_master_secret (0x0017)
- session_ticket (0x0023)
- signature_algorithms (0x000D)
- signature_algorithms_cert (0x0032)
- supported_versions (0x002B)
- psk_key_exchange_modes (0x002D)
- key_share (0x0033)
- renegotiation_info (0xFF01)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Maintain
If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alert still persists, perform the following:

1. **Collect the logs and Troubleshooting Scenarios**: For more information on how to collect logs and troubleshooting information, see *Oracle Communications Cloud Native Core, Binding Support Function Troubleshooting Guide*.
2. **Raise a service request**: See My Oracle Support for more information on how to raise a service request.

4.43.3 TLS 1.3 Support for Kubernetes API Server

In a Kubernetes-based 5G Core deployment, Policy regularly interacts with the Kubernetes API server (Kube-Api-Server) to retrieve the secrets and configmap information.

With the implementation of this feature, Policy supports TLSv1.3 in addition to TLSv1.2 for establishing secure communication with the Kubernetes API server.

Managing TLS 1.3 Support for Kubernetes API Server

Enable and Configure

This feature can be enabled or disabled using *kubeApiServerTlsVersion* flag. If the flag is enabled, user can choose TLS 1.3 or TLS 1.2 for communication between each service and Kubernetes API server. For information, see Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide.

Observe

There are no alerts and metrics for this feature.

4.44 Traffic Segregation

This feature provides end-to-end traffic segregation to Policy based on traffic types. Within a Kubernetes cluster, traffic segregation can divide applications or workloads into distinct sections such as OAM, SBI, Kubernetes control traffic, etc. The Multus CNI container network interface (CNI) plugin for Kubernetes enables attaching multiple network interfaces to pods to help segregate traffic from each Policy microservice.

This feature addresses the challenge of logically separating IP traffic of different profiles, which are typically handled through a single network (Kubernetes overlay). The new functionality ensures that critical networks are not cross-connected or sharing the same routes, thereby preventing network congestion.

With traffic segregation, operators can segregate traffic to external feeds and applications more effectively. Previously, all external traffic was routed through the same external network, but now, egress traffic from the Policy pods can be directed through non-default networks to third-party applications. This separation is achieved by leveraging cloud-native infrastructure and the load balancing algorithms in CNE.

The feature supports the configuration of separate networks, Network Attachment Definitions (NADs), and the Cloud Native Load Balancer (CNLB). These configurations are crucial for enabling cloud native load balancing, facilitating ingress-egress traffic separation, and optimizing load distribution within Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Prerequisites

The CNLB feature is only available in Policy if CNE is installed with CNLB and Multus.

Cloud Native Load Balancer (CNLB)

CNE provides Cloud Native Load Balancer (CNLB) for managing the ingress and egress network as an alternate to the existing LBVM, lb-controller, and egress-controller solutions. You can enable or disable this feature only during a fresh CNE installation. When this feature is enabled, CNE automatically uses CNLB to control ingress traffic. To manage the egress traffic, you must preconfigure the egress network details in the `cnlb.ini` file before installing CNE.

> **Note**
>
> CNLB is supported only for IPv4 stack.

For more information about enabling and configuring CNLB, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*, and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

Network Attachment Definitions for CNLB

A Network Attachment Definition (NAD) is a resource used to set up a network attachment, in this case, a secondary network interface to a pod. Policy supports two types of CNLB NADs:

1. **Ingress Network Attachment Definitions**
   Ingress NADs are used to handle inbound traffic only. This traffic enters the CNLB application through an external interface service IP address and is routed internally using interfaces within CNLB networks.
   - **Naming Convention:**`nf-<service_network_name>-int`
2. **Egress Only Network Attachment Definitions**
   Egress Only NADs enable outbound traffic only. An NF pod can initiate traffic and route it through a CNLB application, translating the source IP address to an external egress IP address. An egress NAD contains network information to create interfaces for NF pods and routes to external subnets.
   - **Requirements:** Destination (egress) subnet addresses are known beforehand and defined under the `cnlb.ini` file's `egress_dest` variable to generate NADs.
   - **Naming Convention:**`nf-<service_network_name>-egr`
3. **Ingress/Egress Network Attachment Definitions**
   Ingress/Egress Network Attachment Definitions enable inbound/outbound traffic. An NF pod can initiate traffic and route it through a CNLB app, translating source IP address to an external egress IP address (defined under **cnlb.ini** file **egress_addr** variable). An Ingress/Egress Network Attachment Definition contains network information to create interfaces for NF pods and routes to external subnets. Even though an Ingress/Egress Network Attachment Definition enables outbound traffic, it also handles inbound traffic, so if inbound/outbound traffic is needed an Ingress/Egress Network Attachment Definition should be used.
   - **Requirements:** Source (ingress) and destination (egress) subnet addresses are known beforehand and defined under **cnlb.ini** file **egress_dest** variable to generate Network Attachment Definitions.
   - **Naming Convention:**`nf-<service_network_name>-ie`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing Ingress and Egress Traffic Segregation

Enable:

This feature is disabled by default. To enable this feature, you must configure the network attachment annotations in the custom values file.

Configuration

For more information about Traffic Segregation configuration, see " Configuring Traffic Segregation" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.*.

Observe

There are no Metrics, KPIs, or Alerts available for this feature.

Maintain

To resolve any alerts at the system or application level, see Alerts section. If the alerts persist, perform the following:

1. **Collect the logs**: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
2. **Raise a service request**: See My Oracle Support for more information on how to raise a service request.

4.45 Support for Optimizing Database Encoding in PCRF Core

This feature aims to optimize encoding and decoding the database fields of PCRF Cores services to reduce the size of data transferred during replication and improve the performance in the call flows.

PCRF Core stores and transfers the data in Java Script Object Notation (JSON) object. In JSON object the key/name describes the value, and the value is the actual data. At present, the PCRF Core JSON objects stored in the database is overly verbose, redundant keys and repetitive structures has increased the data size, causing longer data transfer times during replication.

The feature is implemented by:

- a data encoding technique that shortens all the overly verbose attribute names, and uses a mapping table that holds the long and short names.
- a data encoding technique that shortens all the overly verbose constants or default or enumeration attribute values, and uses a mapping table that holds the long and short values.
- to remove all unused and irrelevant JSON attributes from the value columns in gxsession, rxsession, sdsession tables.

Shorten JSON Attribute Keys

In the data encoding technique, every time before a record is stored in the gxsession, rxsession, sdsession tables it is encoded by mapping long attribute names to short names; when the same record is retrieved it is decoded by converting the short attribute names to its original long names.

For example: `"eventReportIndicationTriggerMask" shorten as "eRITM"`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Shorten JSON Attribute Values

In the data encoding technique, JSON attribute containing longer fixed or default or enumeration values are mapped to shorter values.

For example:

```
geographicLocationField": {"type":
"PCRFDiameterTrackingAreaEUTRANCellGlobalIdentifierImpl"
```

In the above example, the different values that "type" key can take and its mapping is shown below:

```
"PCRFDiameterTrackingAreaEUTRANCellGlobalIdentifierImpl",  we can map it to
"PDTAE";
"PCRFDiameterTrackingAreaIdentifierImpl", we can map it to "PDTAI";
"PCRFDiameterTrackingUpdateImpl", we can map it to "PDUI"
```

In PCRF Core services following Advanced keys are added to implement this feature:

- `DB.GX.DATA.ENCODING.Enabled`
- `DB.RX.DATA.ENCODING.Enabled`
- `DB.SD.DATA.ENCODING.Enabled`
- `DB.GX.ENCODING.MAP.Version`
- `DB.RX.ENCODING.MAP.Version`
- `DB.SD.ENCODING.MAP.Version`
- `DB.ENCODING.MAP.LIST`

Managing Support for Optimizing Database Encoding in PCRF Core

Enable

By default, this feature is disabled for PCRF Core service. You can enable this feature for gxsession, rxsession and rdsession using CNC Console.

Configure

To enable the feature using CNC Console, add the following Advanced Settings keys in the PCRF Core services and set their respective values to `true`:

- `DB.GX.DATA.ENCODING.Enabled`
- `DB.RX.DATA.ENCODING.Enabled`
- `DB.SD.DATA.ENCODING.Enabled`

For more information about the configurations, see PCRF Core Settings

Observability

Metrics

The following metrics are added to provide information about this feature:

- `occnp_data_encoding_total`
- `occnp_data_decoding_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- occnp_data_decoding_fail_total
- occnp_data_encoding_size_before_total
- occnp_data_encoding_size_after_total

For information about the metrics, see PCRF Core Metrics section.

4.46 Support for policyDecFailureReports Attribute

Policy Decision Error Handling is one of the 3GPP-defined features responsible for enabling the policyDecFailureReports attribute.

If the Policy Decision Error Handling is supported and the SMF receives one or more policy decisions and/or condition data which are not referred by any PCC rules or session rules as defined in 3GPP but the storage of the policy decisions and/or condition data was unsuccessful , the SMF behaves as follows:

- When the PCF receives update notify response or SM Update request, it considers all the instances of the policy decisions and/or condition data which are provisioned in the request message as removed from the SMF.
- When the PCF receives the response with HTTP "400 Bad Request" status code but the "policyDecFailureReports" attribute is not included, the PCF considers the request message as removed from the SMF.

The PCF does not remove the PCC rule in case the updatenotify request for rule remove failure. With introduction of the new flag **RULE.ENABLE_PCC_RULE_REMOVE_ON_FAILURE** set to true and if rule remove updatenotify request fails with "400 BAD Request" HTTP error, the association will be updated with PCC rule removed.

> **Note**
>
> If SMF responds with 200 error code and policyDecFailureReport includes the policyDecisionFailureCode for which the policy decision object were not sent will also be processed by PCF and the available policy decision object will be removed. Moreover, if SMF responds with 400 error code and policyDecFailureReport includes the policyDecisionFailureCode for which the policy decision object were not sent, then policy decision objects which were part of update notify request will be removed.

Managing Support for policyDecFailureReports Attribute

Enable and Configure

By default, this feature is not configured on the CNC Policy deployment. You can opt to configure the policyDecFailureReports attribute using the following ways in CNC Console.

- From the navigation menu under **Policy**, navigate to **Service Configurations** to select PolicyDecisionErrorHandling from the drop-down menu of **Override Supported Features** parameter.
- From the navigation menu under **Policy**, navigate to **Service Configurations** to add RULE.ENABLE_PCC_RULE_REMOVE_ON_FAILURE key in the **Advanced Settings**.

For more information about these configurations, see PCF Session Management.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observe

The *occnp_feature_info_received_total* metric is used to support `policyDecFailureReports` attribute. For more information, see SM Service Metrics.

4.47 Enhancements to Error Response

Policy sends error responses to consumer NFs due to some exceptions, such as signaling, validations, and internal errors. These error responses have payloads containing the problem title, status, details, and cause of the error that are used to investigate the error. The details section is now enhanced with application error IDs.

The error handling module gives provision to configure the error response dynamically and the same is responded when Policy is producer of the call flow.

With the enhanced error response mechanism, Policy sends additional information such as server FQDN, micro-service ID, error category, and application error ID in the `detail` attribute of the `ProblemDetails`. This enhancement provides more information about the error and troubleshoot them.

> **Note**
>
> As per the definition of `ProblemDetails` data type in 3GPP, the title and cause fields are optional and can be null or empty.

Application error ID follows the below format.

[EC] [NF ID] [Microservice ID] [Category] [Error ID]

An error code dictionary will be provided to identify the cause and possible solution of the error. For more details of the error code dictionaries for AM, UE, SM, UDR, CHF, and Binding services, see Error Code Dictionary.

Managing Enhancements to Error Response

This section explains the procedure to enable and configure the feature.

Enable

By default, this feature is disabled. The operator can enable this feature through the CNC Console configurations.

Configure

You can configure error handling functionality under **Error Handling** on CNC Console for Policy. For information about how to configure for AM, UE, SM, UDR, CHF, and Binding services in CNC Console, see Error Handling.

Observe

The following metrics have been added in AM, UE, SM, Binding, and User service (UDR and CHF) for this feature:

- error_handler_exec_total
- error_handler_in_total
- error_handler_out_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see CNC Policy Metrics.

4.48 OAuth Access Token Based Authorization

OAuth (Open Authorization) 2.0 an authorization protocol, allows a application to access resources hosted by other API applications on behalf of a user. OAuth provides an authentication layer and separates the role of client from that of the resource owner. On client requests access to resources controlled by the resource owner and hosted by the resource server, OAuth issues **Access Tokens**, a different set of credentials than those of the resource owner. An Access Token is a string that represents the authorization to access resources on behalf of the end user.

Policy supports OAuth 2.0 to authorize requests coming from consumer NFs. Policy application issues the Access Token as JSON Web Token (JWT). This enables Policy, the token issuer to include authorization data in the token itself. The consumer NF requests for Access Token from the issuer Policy, and sends them as part of its requests to Policy. Policy validates the requests and either approves or discards based on Access Token authorization received in the request.

The Access Token is validated with the configured public key certificate in Policy. Policy uses NRF Instance ID to validate the Access Token, where Ingress Gateway stored public keys against NRF instance Id. Policy also uses multiple public certificates for validating Access Tokens by adding support for Key-ID (K-ID) based access token validation, in addition to the existing NRF Instance ID based access token validation.

Ingress Gateway operates in the following three different OAuth Validation Modes:

- INSTANCEID_ONLY : This is the default OAuth Validation Mode used by Ingress Gateway. Ingress Gateway validates access token based on public keys indexed with NRF Instance ID in the issuer field.
- K-ID based ONLY: Ingress Gateway validates Access Token based on public keys indexed with key-id only.
- KID_PREFERRED (K-ID based with Instance ID based as fallback):
  - Ingress Gateway validates Access Token based on public keys indexed with Key-ID. If Key-ID is not FOUND in Access Token, Ingress Gateway attempts token validation using public keys indexed with NRF instance ID in the issuer field.
  - Fallback happens only if the received access token does not contain Key-ID or contains Key-ID but without public key configurations.

> **Note**
>
> - For more information on OAuth client functionality, see "OAuth Authentication and Validation" section in *Oracle Communications Cloud Native Core, Egress Gateway User Guide*.
> - For more information on OAuth validator functionality, see "Ingress Gateway Open Authorization (OAuth) Module" section in *Oracle Communications Cloud Native Core, Ingress Gateway User Guide*.
> - For more information on parameters and their supported values in Policy, see **OAUTH Configuration** section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.
> - For information about OAuth access token attributes like kid, typ, iss, aud, scope etc., see *https://www.rfc-editor.org/rfc/rfc7515.html* page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing OAuth Access Token Based Authorization

Token based Authorization Using Key-ID and NRF Instance ID

For configurations required to enable Access Tokens before deploying Policy, see "Configuring Secrets to Enable Access Token " section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide* .

Configure

To enable access token validation, configure both Helm-based and REST-based configurations on Ingress Gateway.

Configure Using Helm Configuration

For Helm configurations, see "OAUTH Configuration" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide* .

REST API Configuration

After the Helm configuration, send the REST requests to use configured public key certificates. For more information about REST API configuration, see "OAuth Validator REST API Configuration" section in *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide*.

Observability

Metrics

For information on Metrics, see "Oauth Metrics" section in Egress Gateway Metrics.

4.49 Support for End-to-End Log Identifier Across Policy Services

Without a unique end-to-end log identifier, it is difficult to debug use cases where the problem can be at any microservice level.

This feature includes a unique end-to-end identifier to every log message, which can be used to identify the set of logs belonging to a given call flow across all the microservices. For example, a end-to-end log identifier is used across all microservices in an SM Create call flow. Similarly, end-to-end log identifiers used in an SM Update, SM Delete, SM Notify call flows across microservices involved in the flow. This end-to-end log identifier called ocLogId is included in the metadata of every log. the same identifier is used across all the microservices so that logs can be mapped between microservices. Also, a common identifier is used to track a user per microservice.

This feature supports the following call flow for Policy microservices:

- SM Create
- SM Update
- SM Delete
- SM Notify
- SM Rx call flow
- SM Rx RAR call flow

Copyright © 2019, 2026, Oracle and/or its affiliates.

- SM Rx STR call flow
- AM Create
- AM Update
- AM Delete
- AM Notify
- UE Create
- UE Update
- UE Delete
- UE Notify
- AMF discovery for UE Create
- AMF discovery for UE Update
- NRF discovery for Alternate Route Retry call flow
- Binding service call flow for stale session detection
- Audit call flow using Audit service
- Sy interface
- Sd interface
- PCRF callflows passing through the following interfaces:
  - PCRF Core Gx interface
  - Pcrf core Rx
  - N36 interface to interact with UDR
- Audit callflows for PCRF Core
- PCRF Core interaction with Bulwark service
- PCRF Core binding callflows
- Notifier service
- Usage monitoring service
- Soap Connector

Separate log identifiers are created in every georedundancy site. That is, every site creates its own identifier and log the same.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Currently, only Ingress Gateway and Diameter Gateway services can generate ocLogId (when a request from an external NF arrives) and Audit when sending a notification. As a result, there are certain flows and services that are not part of the reception, addition to log metadata and propagation of ocLogId and for which Log Correlation is not ensured. Some of these unsupported services and flows worth to mention are the following:
>
> The following are some of those services for which this feature is not supported:
>
> - Configuration Flows: Configuration flows for each service are not supported as these involve only the services for which configuration is changed and the services where the configuration was added through.
> - Config Service: Config service is not supported as the configuration is either changed or the configuration is add through.
> - Base Diameter Messages as CER/A and DWR/A. ocLogId will not be generated or propagated.
> - CMService: Log Correlation is not supported and CMservice can not generate ocLogId. Any flow that was originated by CMService is not supported, including configuration and session viewer flows.
> - Query Service: Query service is not supported. This service can not receive or propagate ocLogId.
> - LDAP-Gateway
> - Alternate Route Service
>
> If any of the supported services receive requests originated or coming from any of the not yet supported ones, directly or indirectly, ocLogId is not ensured to be received as the propagation through any valid mechanism might be yet implemented.

End-to-end log identifier at different services

The Ingress Gateway creates the ocLogId and adds the same in each log that is generated.

The Ingress Gateway passes the ocLogId in the header to Policy microservice such as SM service.

> **Note**
>
> - For SM Rx call flows (AAR and STR), the ocLogId is generated by Diameter Gateway instead of Ingress Gateway.
> - To determine if ocLogId should be generated (when message is received from external NF) or read from AVPs (when received from microservices within PCF), message needs to be parsed. If there is an exception during parsing, then no oclogid will be generated for the rest of the callflow in Diameter Gateway since trying to add oclogid before parsing may cause other problems.
> - When Audit service sends a notification to the other services, the ocLogId is generated by the Audit service.

Logging by SM service

Copyright © 2019, 2026, Oracle and/or its affiliates.

- When SM service receives the ocLogId from Ingress Gateway, it uses the ocLogId while generating the logs. This information is included as part of all the log levels.
- SM service in turn passes the identifier to other backend services such as PRE, PDS, Egress Gateway, Bulwark, and Binding service.
- When SM service receives the ocLogId for the notification from Audit service, they log the messages with ocLogId.
- When SM service receives the ocLogId for the notification from PDS Service or Binding Service, they log the messages with ocLogId.
- When SM service receives the ocLogId from Diameter Connector for Rx call flow, it uses the ocLogId while generating the logs. This information is included as part of all the log levels.
- SM service in turn passes the identifier as header to other backend services.

Logging by AM service

- When AM service receives the ocLogId from Ingress Gateway, it uses the ocLogId while generating the logs. This information is included as part of all the log levels.
- AM service in turn passes the identifier to other backend services such as PRE, PDS, Egress Gateway, and NRF Client.
- When AM service receives the ocLogId for the notification from Audit service, they log the messages with ocLogId.
- When AM service receives the ocLogId for the notification from PDS service or Binding Service, it logs the messages with ocLogId.

Logging by UE Policy service

- When UE Policy service receives the ocLogId from Ingress Gateway, it uses the ocLogId while generating the logs. This information is included as part of all the log levels.
- UE Policy service in turn passes the identifier to other backend services such as PRE, PDS, Egress Gateway, and NRF Client.
- When UE Policy service receives the ocLogId for the notification from Audit service, they log the messages with ocLogId.
- When UE Policy service receives the ocLogId for the notification from PDS service or Binding Service, it logs the messages with ocLogId.

Logging at PDS

- When PDS receives the ocLogId from SM service, AM service, or UE Policy service, it uses the ocLogId while generating the logs.
- PDS passes this ocLogId as the header to the backend services such as UDR Connector, CHF Connector, LDAP, Diameter Gateway, Diameter Connector.
- When PDS receives the ocLogId for the notification from UDR Connector, CHF Connector, Diameter Gateway, Diameter Connector, or Audit service, PDS logs the messages with ocLogId.
- PDS passes the ocLogId as the header to Policy services such as SM service, AM service, or UE Policy service, while sending the notification. PDS uses the ocLogId saved in the context and does not generate any new identifier.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Only when PDS receives a notification from CHF or UDR, a new ocLogId gets created.

Logging at UDR Connector

- When UDR Connector receives the ocLogId from PDS, it uses the ocLogId while generating the logs.
- UDR Connector passes this ocLogId as the header to the backend services such as Egress Gateway.
- When UDR Connector receives the ocLogId for the notification from Ingress Gateway, it logs the messages with ocLogId.

Logging at CHF Connector

- When CHF Connector receives the ocLogId from PDS, it uses the ocLogId while generating the logs.
- CHF Connector passes the ocLogId as the header to the backend service such as Egress Gateway.
- When CHF Connector receives the ocLogId for the notification from Ingress Gateway, it logs the messages with ocLogId.

Logging at Egress Gateway

When Egress Gateway receives the ocLogId from SM service, CHF Connector, UDR Connector, AM service, or UE Policy service, it uses the ocLogId while generating the logs.

Logging at Audit service

- When Audit service detects a possible stale session, audit service generates the ocLogId.
- Audit service includes the ocLogId in the header and sends it to SM service, AM service, UE Policy service, PDS, and Binding service.

Logging at Binding service

- When Binding service receives the ocLogId for the SM service or Audit service, it logs the messages with ocLogId.
- Also, Binding service receives the ocLogId when BSF sends a request to check if a PcfBinding is still valid or not.

Logging at Diameter Gateway

- Diameter Gateway generates the ocLogId and includes it in all the messages for all the Gx, Rx, and Sd flows coming from external NFs.
- Diameter Gateway uses the ocLogId while generating the logs.
- Diameter Gateway sends the ocLogId as headers/AVP to the backend services such as Diameter Connector and Binding service.

Logging at Diameter Connector

- When Diameter Connector receives the ocLogId from Diameter Gateway, it logs the messages with ocLogId.
- Diameter Connector sends the ocLogId as header to the backend services such as SM service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Logging at PRE

- When PRE receives the ocLogID from SM service, AM service, UE Policy service, or PDS, it uses the ocLogId while generating the logs.
- PRE sends the ocLogId as headers/AVP to the backend service.

Logging at Bulwark service

When Bulwark service receives the ocLogID from SM service, it uses the ocLogId while generating the logs.

Logging at NRF Client

- When NRF Client receives the ocLogId from AM service or UE Policy service, it logs the messages with ocLogId.
- NRF Client sends the ocLogId as headers to the backend services.
- When there is a request initiated by NRF Client (not something from UE or AM) NRF creates the ocLogId by itself and sends it to the subsequent services.

Logging at PCRF Core

- When PCRF Core receives the ocLogId from Diameter Gateway, it uses the ocLogId while generating the logs.
- When PCRF Core service receives the ocLogId for the notification from PDS, Audit Service, or Usage Monitoring service, it logs the messages with ocLogId.
- PCRF Core service sends the ocLogId as headers/AVP to the backend service such as Usage Monitoring service and PRE.

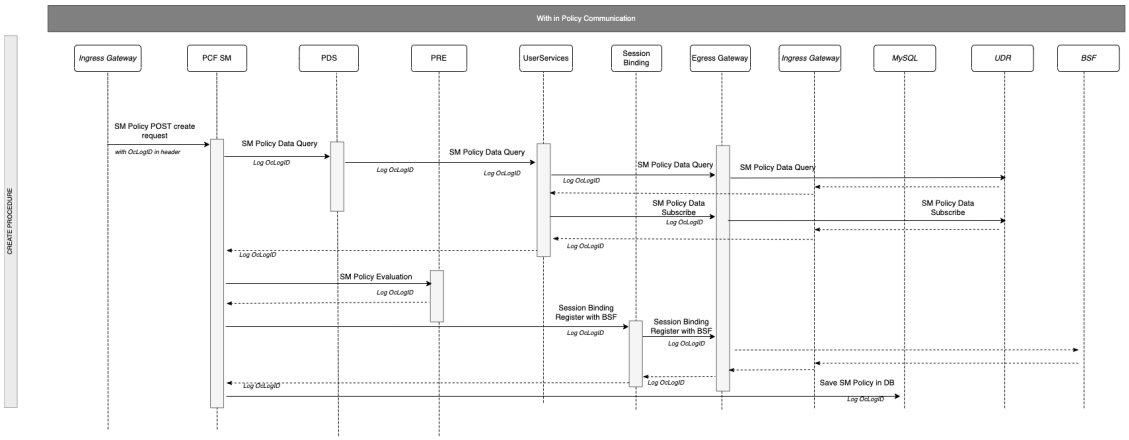
Logging at Notifier service

Notifier service uses the ocLogId while generating the logs.

Logging at Usage Monitoring service

- When Usage Monitoring service receives the ocLogId from PCRF Core, it logs the messages with ocLogId.
- Usage Monitoring service sends the ocLogId as headers/AVP to the backend service such as PDS.
- Usage Monitoring service sends the ocLogId as headers/AVP as the notification to PCRF Core.

Figure 4-117 Example: Unique Identifier for SM Create Call Flow



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Ingress Gateway receives SM session create request from SMF. Ingress Gateway generates the ocLogId and passes the ocLogId in the header to SM service.
2. SM service sends a Get request to PDS to get the SMAssociation details and uses the ocLogId while generating the logs.
3. PDS sends the query to User Service (UDR Connector, CHF Connector). PDS uses the ocLogId while generating the logs. Also, PDS passes this ocLogId as the header to the backend services such as UDR Connector and CHF Connector.
4. UDR Connector in turn forwards the request to UDR through Egress Gateway. UDR Connector uses the ocLogId while generating the logs. Also, it passes the ocLogId as a header to Egress Gateway.
5. UDR responds to the request with the SM Policy data.
6. User service then sends a request to UDR for the subscription through Egress Gateway. The logs generated at Egress Gateway are saved with ocLogId.
7. UDR responds with the subscription details. UDR Connector forwards the subscription details to SM service and logs the transaction with ocLogId.
8. SM service interacts with PRE for Policy evaluation. PRE uses the ocLogId while generating the logs.
9. SM service sends a session binding request with BSF and includes the ocLogId in the header. The session binding request containing ocLodId is sent to BSF through Egress Gateway.
10. SM service receives the response to session binding request from BSF through Ingress Gateway. SM service updates the details in SMAssociation database and logs the transaction with ocLogId.

Managing the End-to-End Log Identifier across Policy Services

`TRACE_ID_GENERATION_ENABLED` Helm parameter is used to enable or disable the addition of the end-to-end identifier through Ingress Gateway. This same flag is also present in Diameter Gateway, Audit service, and NRF Client.

By default, `TRACE_ID_GENERATION_ENABLED` is enabled.

Audit service uses it when initiating a stale session notification.

Diameter Gateway uses the Helm parameter to decide ocLogId generation for all the Gx, Rx, and Sd flows.

NRF Client uses it when initiating a request by its own (a request that was not received from other services).

By default, the value this parameter is set to true and the feature is enabled.

When this feature is enabled, Ingress Gateway generates the ocLogId and propagates the headers to the succeeding microservices, Audit service, Diameter Gateway, NRF Client.

Ingress Gateway passes the ocLogId generated as the header and sends the same to other Policy microservices such as SM service, AM service, or UE Policy service.

4.50 Support for Automated Certificate Lifecycle Management

Public Key Interface (PKI) is the set of elements such as public/private keys, certificate signing request, and certificates that are required to handle secure communications and transactions. Policy uses secure protocols for its communications, such as HTTPS and Secure Socket Layer

Copyright © 2019, 2026, Oracle and/or its affiliates.

(SSL) / Transport Layer Security (TLS) technologies to handle these secure communications. This is achieved with the use of Public and Private Keys, and the presence of trusted authorities, also known as Certificate Authorities (CA), which create and issue certificates. These certificates have a determined validity period. These certificates must be renewed before expiry. They can also be revoked when the CA or its keys are compromised. These certificates must be recreated when required.

This feature enables Policy to support automation of certificate lifecycle management in integration with Oracle Communications Certificate Manager (OCCM).

OCCM provides the option to automatically create, renew, and delete certificates for a given CA, with the possibility to track previously created certificates and renew/delete them when required.

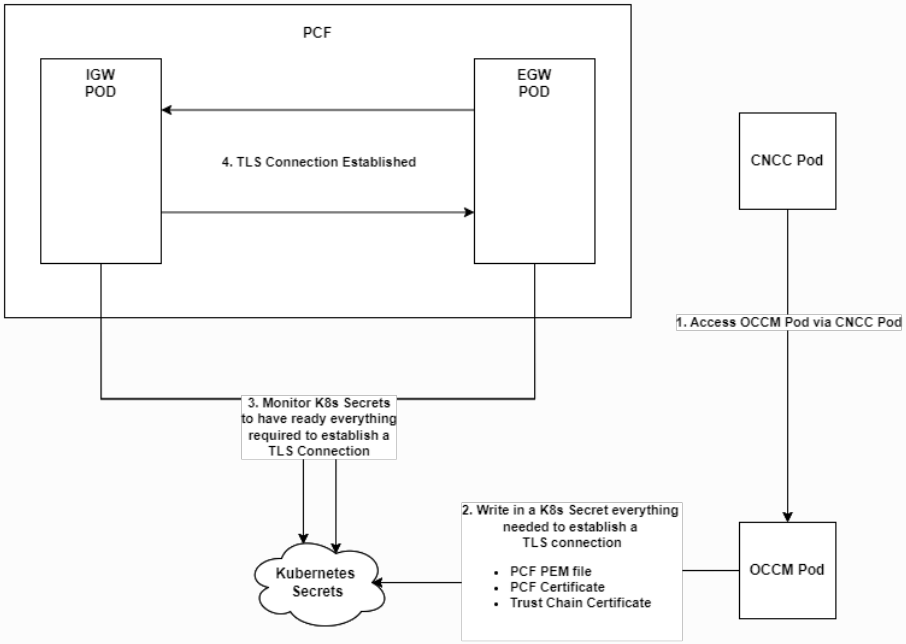
The certificate lifecycle management includes:

- Certificate Creation,
- Certificate Deletion,
- Certificate Monitoring (including the ones that were created using a different tool from OCCM),
- Certificate Renewal.

Note

OCCM do not support OAuth token generation and distribution (currently handled by NRF) used for SBI signaling.

Figure 4-118 Policy Integration with OCCM



Copyright © 2019, 2026, Oracle and/or its affiliates.

There is no direct communication between OCCM and Policy. All the communications are handled using monitoring Kubernetes Secrets.

All the required certificates are configured using OCCM.

After OCCM creates these Kubernetes Secrets, or monitors the already existing ones, the Ingress and Egress Gateways monitor these Secrets and keep track of their current status:

- **VALID**: A Kubernetes Secret which holds a certificate that has not expired and it is properly signed,
- **EXPIRED**: A Kubernetes Secret which holds a certificate that has met its expiration date (the value determined in its `notAfter` value),
- **MISSING**: A Kubernetes Secret which has its certificate missing, or any other essential file for the TLS/SSL bundle.
- **CORRUPT**: A Kubernetes Secret which has its certificate corrupt, either invalid file, invalid signature, or invalid format.

Managing the keys and certificates

Install Guide Considerations

- Upgrade: When Policy is deployed with OCCM, follow the specific upgrade sequence as mentioned in the *Oracle Communications, Cloud Native Core Solution Upgrade Guide*.
- Rollback: You can remove Kubernetes secrets if the current version of Policy does not use that secret by checking the `occnp_custom_values.yaml` file. Before deleting, please make sure that there is no plan to rollback to the Policy version which uses these secrets. Otherwise Rollback will fail. For more information on migrating the secrets from Policy to OCCM and removal of Kubernetes secrets from the yaml file, see *Upgrade Strategy* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Configure

To configure HTTPS in ingress-gateway, the following parameters must be configured in custom-value.yaml file in the ingress-gateway section:

- ingress-gateway.enableIncomingHttps
- ingress-gateway.service.ssl.privateKey.k8SecretName
- ingress-gateway.service.ssl.privateKey.k8NameSpace
- ingress-gateway.service.ssl.privateKey.rsa.fileName
- ingress-gateway.service.ssl.certificate.k8SecretName
- ingress-gateway.service.ssl.certificate.k8NameSpace
- ingress-gateway.service.ssl.certificate.rsa.fileName
- ingress-gateway.service.ssl.caBundle.k8SecretName
- ingress-gateway.service.ssl.caBundle.k8NameSpace
- ingress-gateway.service.ssl.caBundle.fileName
- ingress-gateway.service.ssl.keyStorePassword.k8SecretName
- ingress-gateway.service.ssl.keyStorePassword.k8NameSpace
- ingress-gateway.service.ssl.keyStorePassword.fileName
- ingress-gateway.service.ssl.trustStorePassword.k8SecretName

Copyright © 2019, 2026, Oracle and/or its affiliates.

- ingress-gateway.service.ssl.trustStorePassword.k8NameSpace
- ingress-gateway.service.ssl.trustStorePassword.fileName

For more information, see *Basic Configurations in Ingress Gateway* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

To configure HTTPS in egress-gateway, configure the following parameters under *egress-gateway* section in *custom-value.yaml* file:

- egress-gateway.enableOutgoingHttps
- egress-gateway.egressGwCertReloadEnabled
- egress-gateway.egressGwCertReloadPath
- egress-gateway.service.ssl.privateKey.k8SecretName
- egress-gateway.service.ssl.privateKey.k8NameSpace
- egress-gateway.service.ssl.privateKey.rsa.fileName
- egress-gateway.service.ssl.privateKey.ecdsa.fileName
- egress-gateway.service.ssl.certificate.k8SecretName
- egress-gateway.service.ssl.certificate.k8NameSpace
- egress-gateway.service.ssl.certificate.rsa.fileName
- egress-gateway.service.ssl.certificate.ecdsa.fileName
- egress-gateway.service.ssl.caBundle.k8SecretName
- egress-gateway.service.ssl.caBundle.k8NameSpace
- egress-gateway.service.ssl.caBundle.fileName
- egress-gateway.service.ssl.keyStorePassword.k8SecretName
- egress-gateway.service.ssl.keyStorePassword.k8NameSpace
- egress-gateway.service.ssl.keyStorePassword.fileName
- egress-gateway.service.ssl.trustStorePassword.k8SecretName
- egress-gateway.service.ssl.trustStorePassword.k8NameSpace
- egress-gateway.service.ssl.trustStorePassword.fileName

For more information, see *Basic Configurations in Egress Gateway* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Observability

Monitoring the keys and certificates

Policy supports monitoring and automatic renewal of its' TLS certificates in integration with OCCM.

It is validated that the renewed certificate and key are picked up for any new TLS connections.

Also, the existing TLS connections using the previous key and certificate are gracefully brought down.

Clean up of the certificates are also handled through OCCM.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For information about enabling HTTPS, see *Configuring Secrets for Enabling HTTPS* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Metrics

The oc_certificatemanagement_tls_certificate_info metric is used to support automated certificate lifecycle management.

For more information, see Metrics for Automated Certificate Lifecycle Management.

4.51 Support for Handling Requests From Reduced Capability Devices

Policy supports handling the requests from reduced capability devices (RedCap) to support IoT ecosystem.

RedCap is a device class that is designed to provide a cost-effective way to connect devices that do not require the full capabilities of the 5G system. It reduces device complexity through fewer RX or TX antennas, lesser bandwidth requirement, lower power consumption, relaxed data rates, relaxed processing time and processing capability to support some exciting use cases, primarily around industrial wireless sensors, video surveillance and wearables.

Policy identifies the incoming request from the RedCap devices based on the `NR_REDCAP` enumerated value in the request that indicates NR RedCap RAT Type.

Based on this value, interactions with PRE are performed to make appropriate decisions for the reduced capability UEs.

> **Note**
>
> Policy supports policy decisions on NR RedCap RAT Type for:
>
> - create, update, update notify, and delete message for SM service
> - create message for AM service and UE Policy service

Support for NR_REDCAP value for RAT Type over Rx Interface

PCF supports voice and video calls by reduced capability on Voice over Long-Term Evolution (VoLTE) and Voice over New Radio (VoNR).

For this purpose, PCF establishes binding sessions with BSF and supports Rx diameter procedures for these sessions for RedCap devices by sending `RatType` attribute with `NR_REDCAP` value to BSF, P-CSCF in AAA and RAR.

When an Rx session is established upon receiving a AAR-I for a RedCap device, if **Redcap Support for Rx Interface** field on **Diameter Connector** page under **General** section in CNC console is enabled and the RAT Type is `NR_REDCAP`, PCF sends a AAA message to P-CSCF containing `RATType` AVP with value `NR_REDCAP`.

For more information on configuring **Redcap Support for Rx Interface** field, see Diameter Connector.

When PCF receives SM Update Request from SMF and if policy control request trigger conditions are met or the event occurs, for which P-CSCF has subscribed (that is, `IP-CAN type`

Copyright © 2019, 2026, Oracle and/or its affiliates.

change Notification and RATType has changed for the device), if **Redcap Support for Rx Interface** field is enabled and RATType is NR_REDCAP, PCF sends a RAR message to P-CSCF containing RATType AVP with value NR_REDCAP.

The AAA and RAR messages for the PDU sessions are sent through Diameter Connector service and Diameter Gateway to BSF containing RATType AVP with value NR_REDCAP.

> **Note**
>
> When **Redcap Support for Rx Interface** field is disabled and Rx session is established for the RedCap devices, PCF accepts the session and sends AAA success without RATType.

Managing the Support for RedCap Devices

Enable

To enable support for reduced capability devices, configure value of **RatType** block under **Policy Projects** in CNC Console to NR_REDCAP.

For more information on the **RatType** block, see *PCF UE Policy* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide.*

To enable support for NR_REDCAP value for RAT Type over Rx interface

You can enable the support for NR_REDCAP value for a RAT Type over Rx interface using CNC Console as well as using REST API.

Enable using CNC console

To enable support for NR_REDCAP value in RATType AVP, configure **Redcap Support for Rx Interface** field under **General** section on **Diameter Connector** page for **Service Configurations** in CNC Console.

For more information, see Diameter Connector.

Enable using REST API

To enable support for NR_REDCAP value in RATType AVP, configure ratTypeNRRedCapEnabled parameter for Diameter Connector API.

For more information, see *Diameter Connector* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide.*.

Installation and Upgrade Impact

The feature configuration using **Redcap Support for Rx Interface** field under **Diameter Connector** page for **Service Configurations** will be available in CNC Console for Policy only after installing or upgrading to Policy 25.1.200 or later versions.

> **Note**
>
> - This feature does not involve any change to the context data for SM service.
> - This feature does not involve any change to Policy evaluation.
> - This feature must be enabled only after all the sites in the mated region are upgraded.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observability

Metrics

The `diam_avp_dropped` metric is used to support voice and video calls by reduced capability devices on Voice over Long-Term Evolution (VoLTE) and Voice over New Radio (VoNR) feature.

> **Note**
>
> The `diam_avp_dropped` metric is pegged only when the flag is disabled, and still, SM service sends the `NR_REDCAP` value in `RATType` AVP to the Diameter Connector service when sending AAA and RAR messages.

For more information, see Diameter Connector Service Metrics.

Logging

Following is a sample log that can be used to troubleshoot problems with supporting voice or video calls by RedCap devices in VoLTE or VoNR.


```
{
  "instant": {
    "epochSecond": 1738745556,
    "nanoOfSecond": 301226519
  },
  "thread": "boundedElastic-2",
  "level": "DEBUG",
  "loggerName": "ocpm.diameter.DiameterIncident",
  "message": "Peer oc-diam-gateway(TCP 10.233.109.20:32804
10.233.116.94:3868): Sent message(AAA): \nDiameter Message: AAA\nVersion:
1\nMsg Length: 232\nCmd Flags: PXY\nCmd Code: 265\nApp-Id: 16777236\nHop-By-
Hop-Id: 4028189085\nEnd-To-End-Id: 3779477398\n  Session-Id (263,M,l=10) =
s4\n  Origin-Host (264,M,l=13) = ocpcf\n  Origin-Realm (296,M,l=18) =
xxx.com\n  Auth-Application-Id (258,M,l=12) = 16777236\n  Result-Code
(268,M,l=12) = DIAMETER_SUCCESS (2001)\n  IP-CAN-Type (1027,VM,v=10415,l=16)
= THREEGPP_5GS (8)\n  RAT-Type (1032,V,v=10415,l=16) = NR_REDCAP (1039)\n
Supported-Features (628,V,v=10415,l=56) = \n    Feature-List-ID
(629,V,v=10415,l=16) = 1\n    Vendor-Id (266,M,l=12) = 10415\n    Feature-
List (630,V,v=10415,l=16) = 16\n  Oc-Log-Id (6668,V,v=21274,l=52) =
1738745555727_1_policy-oc-diam-gateway-0\n[1, 0, 0, -24, 64, 0, 1, 9, 1, 0,
0, 20, -16, 25, 73, -99, -31, 70, 63, -106, 0, 0, 1, 7, 64, 0, 0, 10, 115,
52, 0, 0, 0, 0, 1, 8, 64, 0, 0, 13, 111, 99, 112, 99, 102, 0, 0, 0, 0, 0, 1,
40, 64, 0, 0, 18, 111, 114, 97, 99, 108, 101, 46, 99, 111, 109, 0, 0, 0, 0,
1, 2, 64, 0, 0, 12, 1, 0, 0, 20, 0, 0, 1, 12, 64, 0, 0, 12, 0, 0, 7, -47, 0,
0, 4, 3, -64, 0, 0, 16, 0, 0, 40, -81, 0, 0, 0, 8, 0, 0, 4, 8, -128, 0, 0,
16, 0, 0, 40, -81, 0, 0, 4, 15, 0, 0, 2, 116, -128, 0, 0, 56, 0, 0, 40, -81,
0, 0, 2, 117, -128, 0, 0, 16, 0, 0, 40, -81, 0, 0, 0, 1, 0, 0, 1, 10, 64, 0,
0, 12, 0, 0, 40, -81, 0, 0, 2, 118, -128, 0, 0, 16, 0, 0, 40, -81, 0, 0, 0,
16, 0, 0, 26, 12, -128, 0, 0, 52, 0, 0, 83, 26, 49, 55, 51, 56, 55, 52, 53,
53, 53, 53, 55, 50, 55, 95, 49, 95, 112, 111, 108, 105, 99, 121, 45, 111, 99,
45, 100, 105, 97, 109, 45, 103, 97, 116, 101, 119, 97, 121, 45, 48]",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
  "threadId": 106,
  "threadPriority": 5,
  "messageTimestamp": "2025-02-05T08:52:36.301+0000",
  "ocLogId": "1738745555727_1_policy-oc-diam-gateway-0"
}
```

4.52 PCF Support for ME-XX String in Server Header from CHF

When PCF communicates with other NFs, it makes use of a header called server, as defined in 3GPP. PCF uses these header is used by PCF to make decisions on retry strategies when receiving error responses. The header contains the instance or instances that generated the error. Based on the standard defined in 3GPP, the instance(s) inserted in the header must follow the following pattern: **"<NFType>-<NF Instance ID>"** for an NF, where

- **<NF Type>** is the type of the NF or network entity generating the error, set to the NFType value as defined in 3GPP.
- **<NF Instance ID>** is the identity of the NF or network entity generating the error, set to the FQDN of the SCP or SEPP, or to the NF Instance ID of the HTTP server.

For example, when inserted by an NF such as SCP or SEPP, the error originators, the server header pattern looks like "SCP-<SCP FQDN>" for a SCP and "SEPP-<SEPP FQDN>" for a SEPP.

The information carried in the Server Header is useful for troubleshooting. There might be cases where this server header has custom information and does not follow header pattern as defined by the 3GPP. Considering this, if a differently formatted value such as "ME-me-instanceid", is inserted in the header alongside the 3GPP supported ones, PCF, at present, completely ignores the server header, which impacts the retry strategy.

With this feature implementation, PCF core (SM/AM/UE) services ignores the custom server header value such as "ME-me-instanceid" and continue considering the valid SCP, SEPP or other NF type Server Headers.

Model C: PCF (SM/AM/UE) as Consumer Supports Custom Server Header from CHF on N28 Interface

The N28 reference point is defined for the interactions between PCF and Charging Function (CHF). Policy sends initial POST request for subscription to policy counter information from the CHF over N28 interface. If the CHF cannot successfully fulfill the received POST request due to an error, then CHF sends error response to PCF.

On receiving the error response from CHF, the PCF Core services check for `Server Header Support` field status,

- if the field status is set to `Single Instance`, then the regular expression evaluates the server header value. From the header value, only one NF instance of the primary/secondary CHF Producer is filtered and custom server header content such as ME-me-instanceid is ignored.
- if the field status is set to `Multi Instance`, then the regular expression evaluates the server header value. From the header value. two NF instances from all the producer NF instances in the NFSet is filtered and custom server header content such as ME-me-instanceid is ignored.

While creating retry profile, the regular expression to ignore the content in server header is configured for the Policy services. In the CNC Console, a field **Ignore Custom server header value** is added in **Create Retry Profile** section under **Retry Profile**. In this field, you can specify the string pattern that can be ignored in the server header value.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following table maps the configured regular expression that identifies the matching pattern in the custom server header value. The identified pattern, if exists, is ignored and the remaining value is considered as seen in the **Filtered Content** column in the following table.

Table 4-117 CHF Server Header Content Pattern Matching Regular Expression

Configured Regular Expression	Server Header Content	Filtered Content	Server Header Support
ME-.+	ME-me-54804518-4191-46b3-955cac631f953eb91 CHF-54804518-4191-46b3-955cac631f953eb91	CHF-54804518-4191-46b3-955cac631f953eb9	Single Instance
ME-.+	ME-me-54804518-4191-46b3-955c-ac631f953ed82 CHF-54804518-4191-46b3-955c-ac631f953ed82 ME-me54804518-4191-46b3-955c-ac631f953eb91 CHF-54804518-4191-46b3-955c-ac631f953eb91	CHF-54804518-4191-46b3-955c-ac631f953ed82 CHF-54804518-4191-46b3-955c-ac631f953eb91	Multi Instance
ME-.+	CHF-54804518-4191-46b3-955cac631f953eb91 ME-me-54804518-4191-46b3-955cac631f953eb91	CHF-54804518-4191-46b3-955cac631f953eb91	Single Instance
ME-.+	CHF-54804518-4191-46b3-955c-ac631f953ed82 CHF-54804518-4191-46b3-955cac631f953eb91	CHF-54804518-4191-46b3-955c-ac631f953ed82 CHF-54804518-4191-46b3-955cac631f953eb91	Multi Instance
(ME|CHF)-.+	ME-me-54804518-4191-46b3-955cac631f953eb91 CHF-54804518-4191-46b3-955cac631f953eb91	Empty	Single Instance

Managing PCF Support for ME-XX String in Server Header from CHF

Enable

PCF supports ME-XX String in Server Header from CHF as a core functionality. You do not need to enable or disable this feature.

Configure Using CNC Console

To add the regular expression in CNC Console, set the **Ignore Custom server header value** field in **Create Retry Profile** section under **Retry Profile** for **Common Data Configurations** for Policy Services.

Configure Using REST API

Perform the feature configurations as described in "Retry Profile" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Maintain

Error logs are generated when the system is congested and the actions are taken to bring the system back to normal. Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support.

4.53 Sy SLR Enhancements for Signaling Updates and UDR Notification

The Sy reference point is located between CnPolicy and Online Charging System (OCS). It enables transfer of policy counter status information relating to subscriber spending from OCS to CnPolicy.

CnPolicy considers the subscriber's spending status into account for its Policy decisions. The CnPolicy requests the spending limit report for policy counters from the OCS using the initial or intermediate spending limit request. Currently, CnPolicy supports fetching of OCS counters in the following scenario in a synchronous mode:

- In the initial request i.e., when the request is sent for the first time for a Subscriber, the cnPCRF sets the SL-Request-Type AVP to the value, INITIAL_REQUEST and initiates a diameter Sy Spending Limit Request (SLR) towards OCS.
- On a subsequent request on the second IP CAN session for the same subscriber, the PCRF sets the SL-Request-Type AVP to the value, INTERMEDIATE_REQUEST and updates the OCS counters.

With this feature, CnPCRF and CnPolicy fetches OCS counter status over Sy reference point in the following scenarios in a synchronous mode:

- CnPCRF initiates a Sy SLR intermediate request on receiving CCR-U or SM update request for a given subscriber session-id. CnPolicy evaluates policy based on the latest counters received over Sy and sends the policy rules in the CCA-U or SM update response.
- On receiving UDR notification, cnPCRF issues an Sy SLR initial or intermediate requests. CnPolicy evaluates policy and triggers a RAR or Update Notify toward PGW/SMF for all IP CAN or PDU sessions of the subscriber.

Update Signaling Flow for CnPCRF/SM Services

CnPCRF/SM service, on receiving a CCR update or SM update requests from PGW/SMF, performs OCS counters lookup by invoking OCS Sy Spending Limit Request in a synchronous mode to OCS. At PCRF Core and PCF SM services, a flag **Enable Force Lookup for OCS** is added. You can enable or disable this flag in the PCRF Core service or PCF Session Management **Settings** page under **User** tab in the **OCS Spending Limit** section in the CNC Console. By default, this flag is disabled. The purpose of this flag is to force PDS to perform OCS Lookup, but at PDS this will be treated as revalidation. If this flag is enabled in the core

Copyright © 2019, 2026, Oracle and/or its affiliates.

services, then while initiating the OCS spending limit request the "forceLookup" is sent as true toward PDS.

The following call flow describes the fetching of Sy OCS counters on receiving session updates requests from PGW/SMF:

Figure 4-119 Update signaling flow for CnPCRF/SM service



1. PGW/SMF sends a CCR Update or SM Update request to CnPCRF/SM service.
2. The CnPCRF/SM service sends a GET OCSSpendingLimitRequest with "forceLookup" set to true to PDS.
3. If Sy session is not established then PDS sends SLR-Initial request to Diameter Gateway.
4. Diameter Gateway forwards this request to OCS.
5. If OCS responds with DIAMETER_SUCCESS code to Diameter Gateway.
    a. Diameter Gateway responds with OCS response containing `ocsSpendingLimitStatus` information to PDS.
    b. PDS forwards the OCS response with `ocsSpendingLimitStatus` data to CnPCRF/SM service.
6. If OCS responds with DIAMETER_ERROR code to Diameter Gateway.
    a. Diameter Gateway sends the Error Response to PDS. At PDS, an empty context entry is created in the Database if CreateContextOnFailure is enabled from the request from cnPCRF/PCF-SM.
    b. PDS forwards the Error Response to CnPCRF/SM service.
7. If Sy session is already established then PDS sends SLR-Intermediate request to Diameter Gateway
8. Diameter Gateway forwards this request to OCS.
9. If OCS responds back with DIAMETER_SUCCESS code to Diameter Gateway.
    a. Diameter Gateway responds with OCS response containing `ocsSpendingLimitStatus` information to PDS.
    b. PDS forwards the OCS response with `ocsSpendingLimitStatus` data to CnPCRF/SM service.
10. If OCS responds back with DIAMETER_ERROR code to Diameter Gateway. Diameter Gateway sends the error response to PDS. At PDS,
    a. On receiving the response, it evaluates the flag `createContextOnFailure` in the cnPCRF/PCF SM request and if enabled the existing context is updated as dummy context in the database.
    b. With Force Lookup flag enabled, PCF forces PDS to do a lookup towards OCS, but PDS treats this flag as if was part of revalidation flow and retries again as SLR-Initial Revalidation flow.
    c. Deletes the existing record in the database as part of the revalidation procedure.
11. PDS forwards the Error Response to CnPCRF/SM service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

12. CnPCRF/SM service sends a request with OCS information to PRE for Policy evaluation.
13. Policy evaluated information is sent to PGW/SMF as CCA update or SM update response.

UDR Notification Call Flow

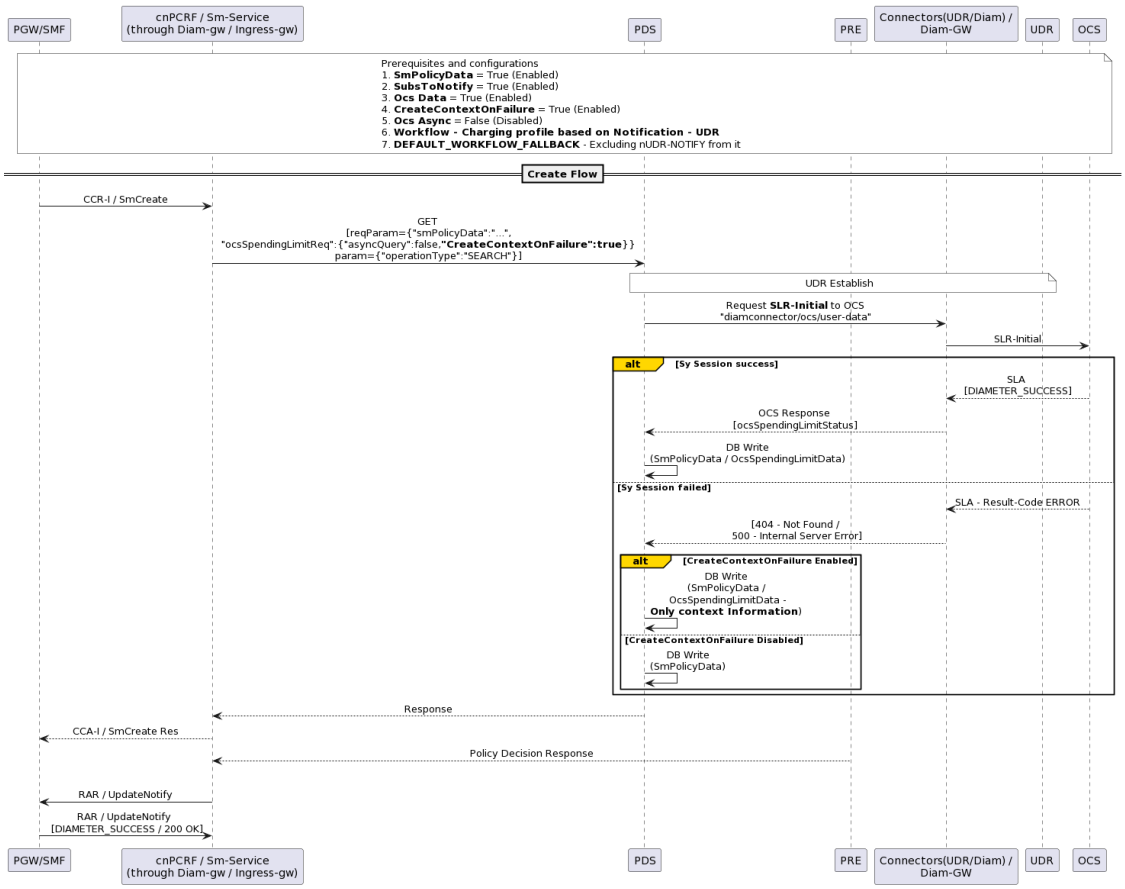
In the UDR notification call flow, the PDS workflow **Charging Profile selection based on Notification - UDR** is added to the list of the existing workflows. On selecting this workflow PDS is instructed to select the user profile based on the notification from UDR. The **Charging Profile selection based on Notification - UDR** workflow is based on the existing **Charging Profile selection based on User Profile - UDR** workflow with two extra tasks added to UDR notify workflow namely, the search and PRE tasks.

In order to use the UDR notification flow that initiates any lookup towards OCS, you need to have the following configurations to be set:

- Select the new workflow **Charging Profile selection based on Notification - UDR** type.
- PDS-OCS dummy context, that is created using either CCR-I/SmCreate or CCR-U/SmUpdate must exist in PDS Database.
- PDS-OCS sy session, that is created using either CCR-I/SmCreate or CCR-U/SmUpdate must exist in PDS Database.

The following call flow describes the fetching of Sy OCS counters during a CCR I/SM Create request from PGW/SMF:

Figure 4-120 UDR PDS - Create Flow



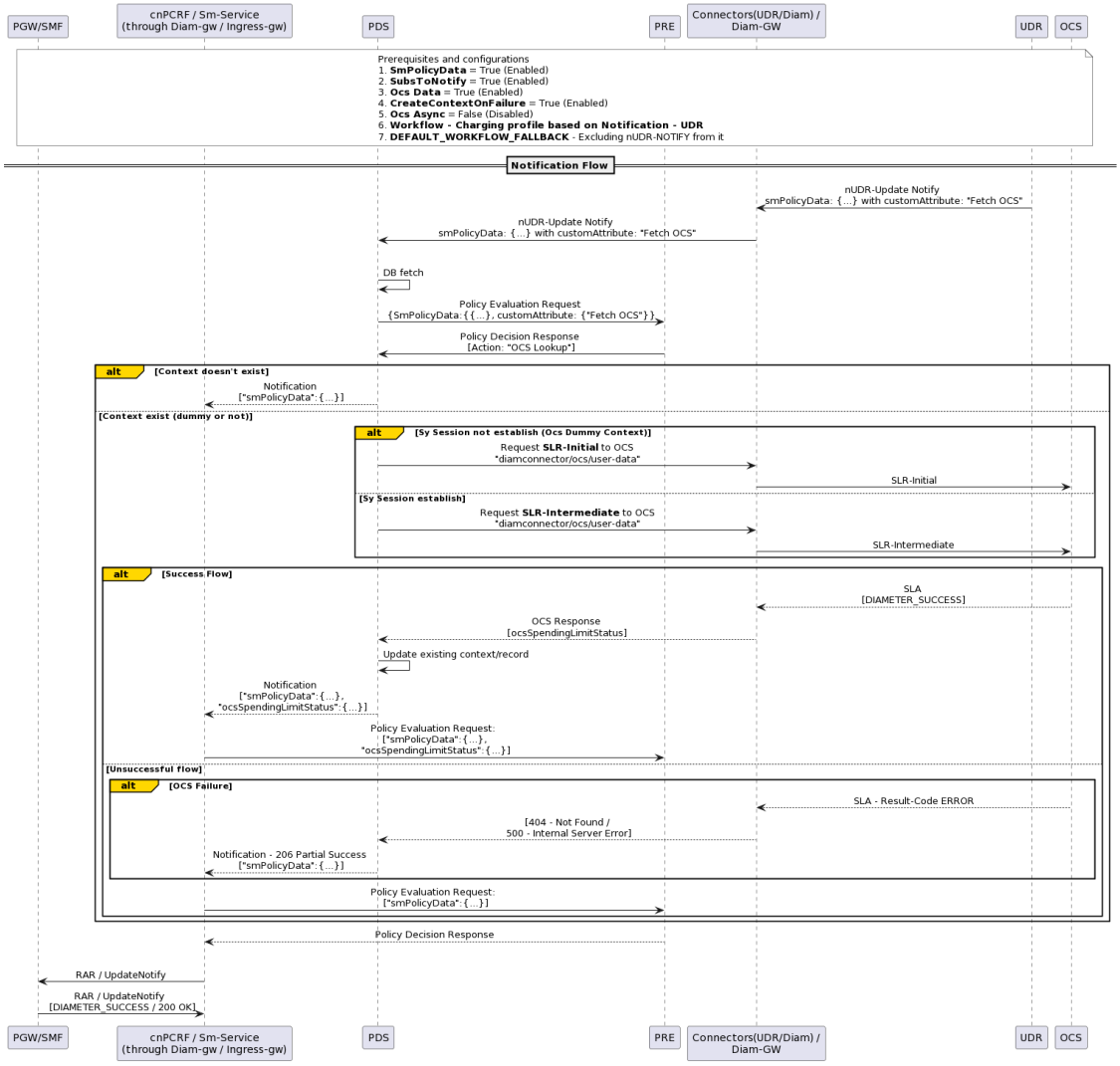
Copyright © 2019, 2026, Oracle and/or its affiliates.

1. PGW/SMF sends a CCR I or SM Create request to CnPCRF/SM service.
2. The CnPCRF/SM service sends a GET OCSSpendingLimitRequest with "createContextonFailure" set to true to PDS.
3. PDS sends SLR-Initial request to Diameter Gateway.
4. Diameter Gateway forwards this request to OCS.
5. If Sy session creation is successful with OCS then it returns DIAMETER_SUCCESS code to Diameter Gateway.
    a. Diameter Gateway responds with OCS response containing `ocsSpendingLimitStatus` information to PDS.
    b. At PDS the `ocsSpendingLimitData` and `smPolicyData` is written into the Database.
6. If Sy session creation is unsuccessful with OCS then it returns DIAMETER_ERROR code to Diameter Gateway.
    a. Diameter Gateway responds with either `404 Not Found` or `500 Internal Server Error` to PDS.
    b. PDS checks for the attribute "createdContextOnFailure" value. On finding it enabled PDS writes only the OCS context information and `smPolicyData` into the Database.
    c. PDS checks for the attribute "createdContextOnFailure" value. On finding it disabled PDS writes only `smPolicyData` into the Database.
7. PDS responds to CnPCRF/SM service.
8. CnPCRF/SM service triggers a CCA I or SM Create response to PGW/SMF.
9. On receiving PRE decision, CnPCRF/SM service triggers a Gx RAR/SM update notify response to PGW/SMF.

The following call flow describes the fetching of Sy OCS counters during a UDR Notification:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-121 UDR PDS Notification Flow



1. UDR triggers an UDR Update Notify request with customAttribute set to "FetchOCS" toward Diameter Gateway.
2. Diameter Gateway forwards this request to PDS.
3. PDS performs a DB fetch and sends Policy evaluation request with the UDR Notification information to PRE.
4. PRE responds back with Policy decision request with an action of "OCS Lookup" to PDS.
5. If OCS Context does not exist then PDS sends notification request to CnPCRF/SM service.
6. If either the dummy OCS Context or actual OCS Context exists then PDS initiates either Sy SLR Initial or Sy SLR Intermediate request to OCS via Diameter Gateway.
7. If OCS sends DIAMETER_SUCCESS code to Diameter Gateway then following call flow runs:
   a. Diameter Gateway responds with OCS response containing `ocsSpendingLimitStatus` information to PDS.
   b. PDS updates the existing OCS context in the database with received OCS data.

Copyright © 2019, 2026, Oracle and/or its affiliates.

c. PDS sends a notification request with `ocsSpendingLimitStatus` data to CnPCRF/SM service.

d. CnPCRF/SM service sends a Policy evaluation request with `ocsSpendingLimitStatus` to PRE.

8. If OCS sends DIAMETER_ERROR code to Diameter Gateway then following call flow runs:

   a. Diameter Gateway responds with either `404 Not Found` or `500 Internal Server Error` to PDS.

   b. PDS sends notification with 206 Partial success to CnPCRF/SM service.

   c. CnPCRF/SM service sends a Policy evaluation request to PRE.

9. PRE sends Policy decision response to CnPCRF/SM service.

10. CnPCRF/SM service triggers a Gx RAR/SM update notify response to PGW/SMF.

Managing Sy SLR Enhancements for Signaling Updates and UDR Notification

Enable

By default, the Sy SLR Enhancements for Signaling Updates and UDR Notification feature is disabled. You can enable this feature using CNC Console or REST API for Policy.

Configure Using CNC Console

To configure the feature using CNC Console, set the **Enable force lookup on Update** parameter to true in **OCS Spending Limit** section under **user** tab on the **Settings** page for **PCRF Core Service Configuration**.

To enable "createContextOnFailure" during UDR Notification flow using the CNC Console, add following keys:

- "USER.ocsSpendingLimit.createContextOnFailure" parameter in the Advanced Settings key in PCRF Core Service Configurations Settings section.
- "USER.CREATE_CONTEXT_ON_FAILURE_OCS_DATA" parameter in the Advanced Settings key in PCF Session Management section.

In the CNC Console the PDS workflow **Charging Profile selection based on Notification - UDR** is selected at PDS Workflow section.

Configure Using REST API

Perform the feature configurations as described in "PCRF Core Service", "Session Management Service" and "PDS Workflow" sections in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

The metric `create_context_on_failure_response` is added to Diameter Connector Service Metrics section.

Maintain

Error logs are generated when the system is congested and the actions are taken to bring the system back to normal. Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

Copyright © 2019, 2026, Oracle and/or its affiliates.

If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support .

4.53.1 Handling N28 and N36 Interfaces Context Information during Subscription Failures

With this feature, PCF supports the N28 and N36 context information such as subscription information, policy and charging related information to be stored in PDS databases during lookup failures. In a scenario, where:

1. SMF initiates a session creation by sending SM create request with received DDN as IMS, the session ID is `session-id-ims` for a subscriber.
2. The fetch request for subscription details from the N28 and N36 fails. PDS does not store any context information for `session-id-ims`.
3. SMF initiates a session creation by sending SM create request with received DNN as internet, the session ID is `session-id-internet` for the same subscriber.
4. If the GET request for subscription details from the N28 and N36 is successful and the POST request for CHF or UDR subscription is also successful then PDS stores the information related to `session-id-internet` in the subscriber context information.
5. PCF receives a SM delete request for the `session-id-internet`.

Currently, PCF deletes the session `session-id-internet` information, even though the other session `session-id-ims` still exists for the subscriber.

This implementation ensures that PCF does not perform deletion of the message toward CHF or UDR prematurely, and keeps the information in the PDS until the subscriber goes away. This feature is implemented for PCRF Core and SM services.

To implement this feature, PCRF core services uses an existing `USER.ocsSpendingLimit.createContextOnFailure` flag and the following new flags:

- `USER.smPolicyData.createContextOnFailure`
- `USER.operatorSpecificData.createContextOnFailure`

If these flags are set to true, then the subscribers policy data and operator specific data are stored in a dummy context created by PDS service during subscription failures from CHF or UDR.

SM service uses an existing `USER.CREATE_CONTEXT_ON_FAILURE_OCS_DATA` flag and the following three new flags:

- `USER.CREATE_CONTEXT_ON_FAILURE_SM_POLICY_DATA`
- `USER.CREATE_CONTEXT_ON_FAILURE_CHF_DATA`
- `USER.CREATE_CONTEXT_ON_FAILURE_OPERATOR_SPECIFIC_DATA`

If these flags are set to true, then the subscribers policy data, operator specific data, and charging data are stored in a dummy context created by PDS service during subscription failures from CHF or UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> This feature works only when subscription (subs-to-notify) flag for UDR data source is true. If the subscription flag is false, then PDS does not create any UDR related resources in the database.

For more information on CNC Console configurations, see "Advanced Settings" in PCF Session Management and PCRF Core Settings sections.

Call Flows

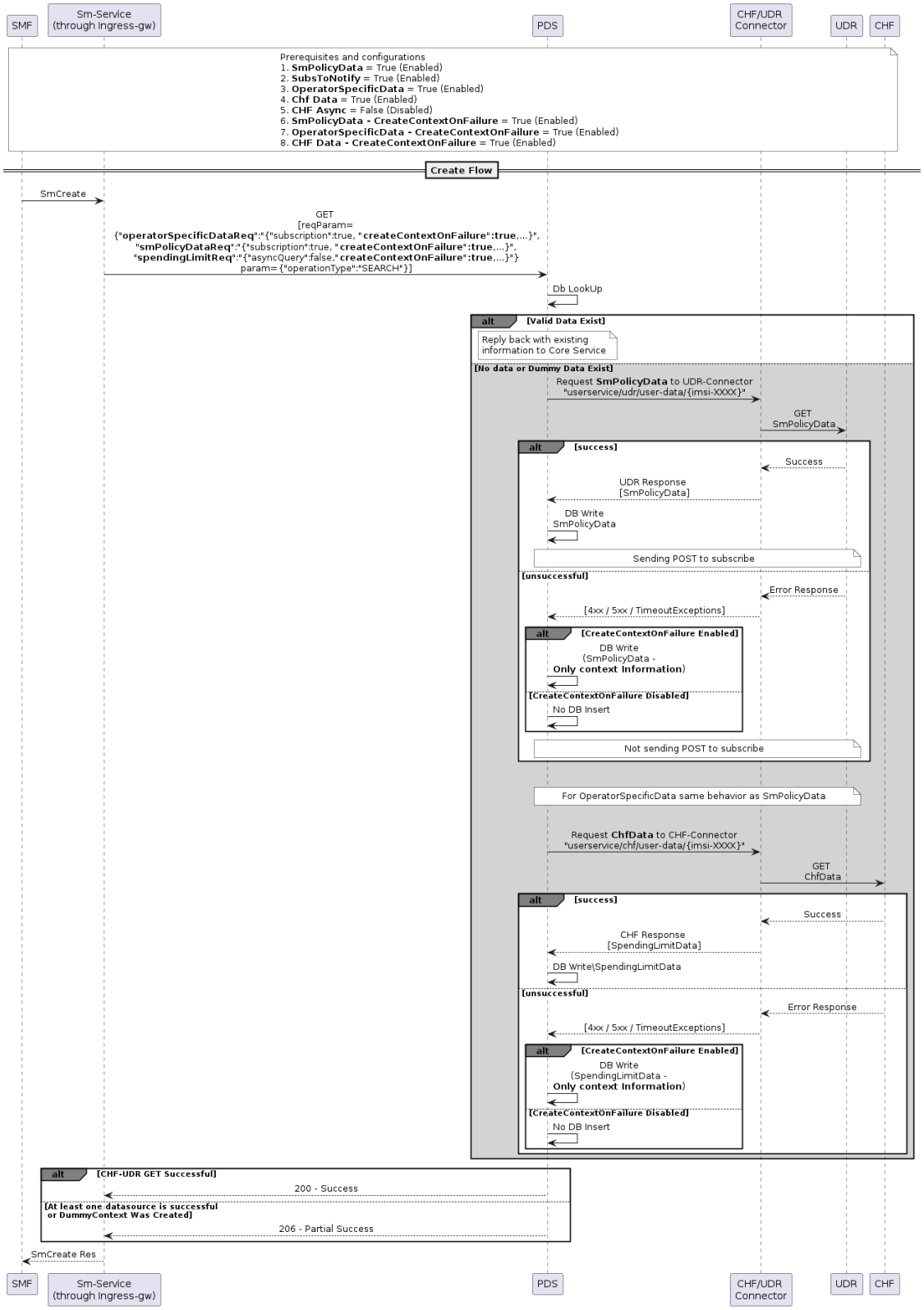
This section describes the procedure of dummy context creation by PDS service during subscription failure scenario in SM and PCRF Core services Create, Update, and Delete call flows.

PDS Dummy Context Creation in SM and PCRF Core Services Create Call Flow

This section describes the SM Create call flow and usage of the flag `createContextOnFailure` during CHF/UDR subscription failure. The same call flow applies to PCRF-Core (CCR-I) without SpendingLimitData (CHF).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-122 PDS Dummy Context Creation during SM and PCRF Core Create Call Flow



1. The SMF sends a SM Create request to SM service via Ingress Gateway.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. If UDR or CHF subscription and charging information is configured in PCF then SM service populates the SM session with these details and sends a request to PDS.
3. The PDS searches for the charging information in the database.
   - If valid data exists, then PDS responds to SM service with the data.
   - If dummy data exists or there is no data, then it sends a GET request for SmPolicyData/OperatorSpecificData toward UDR, and GET request for ChfData toward CHF.
     – UDR responds with SmPolicyData to PDS. This data is stored to the database by PDS.
     – PDS sends Subscription request to UDR. On receiving unsuccessful error response from UDR, PDS checks for the flag "CreateContextOnFailure". If it is set to true, then the SmPolicyData/OperatorSpecificData and ChfData are written to the dummy context by PDS. If the flag is false, there is no database operation done by PDS.
4. PDS sends successful `200 Success` response to SM service for CHF and UDR GET requests.
5. PDS sends partial successful `206 Partial Success` response to SM service on creation of either one datasource or dummy context.
6. SM service responds with SmCreate response to SMF.

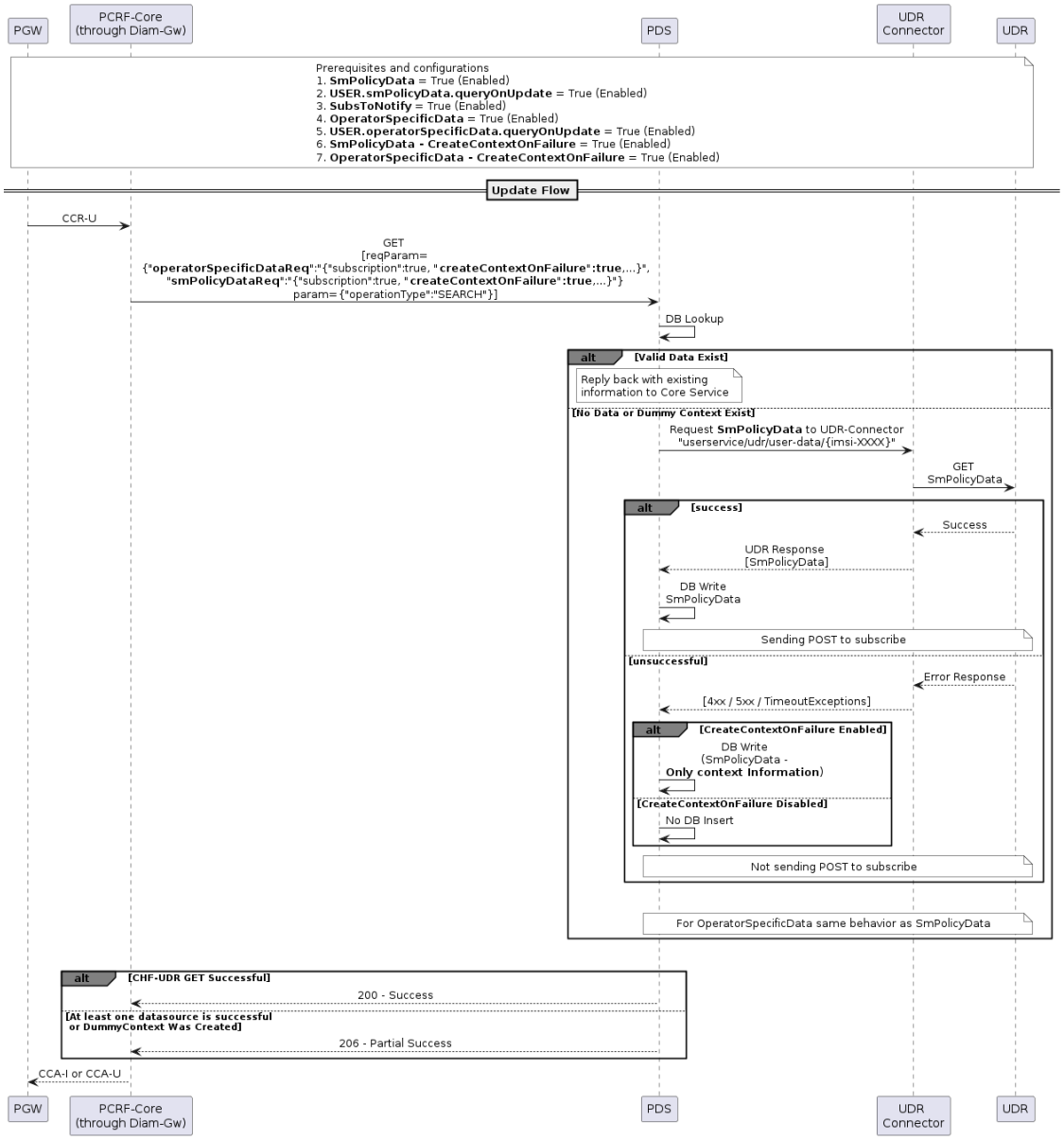
> **Note**
>
> Upon dummy context creation for the data source, it will contain "lastErrorCode" parameter containing status code that provides error details. For example, on receiving 404 error Not Found from UDR, the "lasterrorcode" will be populated as - `lastErrorCode:"USER_NOT_FOUND" or "SUBSCRIPTION_NOT_FOUND"` depending on the type of operation performed.

PDS Dummy Context Creation in SM and PCRF Core Services Update Call Flow

This section describes the PCRF Core Update call flow and usage of the flag `createContextOnFailure` during CHF/UDR subscription failure. The same call flow applies to SM Update with SpendingLimitData (CHF).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-123 PDS Dummy Context Creation during SM or PCRF Core Update Call Flow



1. The PGW sends a CCR-U, an Update request to PCRF core service via Diameter Gateway.
2. If UDR or CHF subscription is configured, then PCRF core service populates its session with these details and sends a request to PDS.
3. The PDS searches for the charging information in the database. If valid data exists, then PDS responds to PCRF core service with the data.
4. The PDS searches for the charging information in the database and if no data or dummy data exists, then
   - If valid data exists, then PDS responds to PCRF core service with the data.
   - If dummy data exists or there is no data, then it sends a GET request for SmPolicyData/OperatorSpecificData toward UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- UDR responds with SmPolicyData to PDS. This data is stored to the database by PDS.
- PDS sends Subscription request to UDR. On unsuccessful error response from UDR, PDS checks for the flag "CreateContextOnFailure" value. If it is true, then the SmPolicyData/operatorSpecificData is written to dummy context by PDS. If the flag is false, there is no database operation done by PDS.

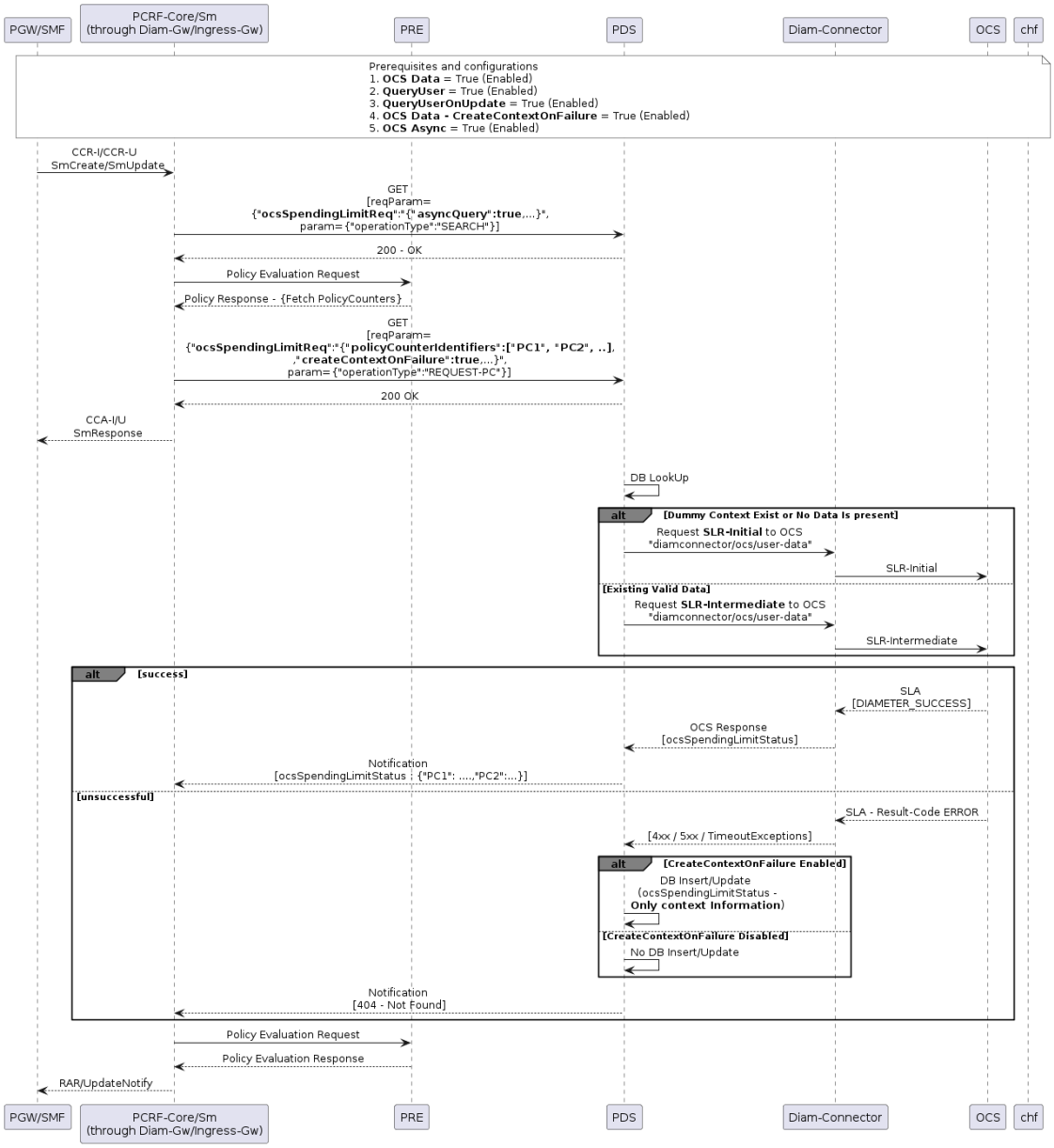
5. PDS sends successful `200 Success` response to PCRF Core service for UDR GET request.
6. PDS sends partial successful `206 Partial Success` response to SM service on creation of either one datasource or dummy context.
7. PCRF Core Service responds with CCA-I or CCA-U response to PGW.

PDS Dummy Context Creation in SM Create/Update Call Flow with OCS in Asynchronous Mode

This section describes PCRF Core CCR-I/CCR-U call flow and usage of the flag `createContextOnFailure` during CHF/UDR subscription failure. For this call flow, the Online Charging System (OCS) is asynchronously enabled using the flag `OCS Aync`. The same call flow applies to SM Update with SpendingLimitData (CHF).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-124 PDS Dummy Context Creation during SM and PCRF Core Create/Update Call Flow with OCS in Async Mode



1. The PGW/SMF sends a CCR-I/SM Create or CCR-U/SM Update requests to PCRF core/SM services via Diameter Gateway/Ingress Gateway.
2. The PCRF core/SM service sends a GET request with `asynchQuery` enabled in OCS spending limit header parameter toward PDS.
3. PDS sends successful `200 Success` response to PCRF core/SM service.
4. The PCRF core/SM service sends a Policy evaluation to PRE.
5. The PRE service responds with fetch policy counters request to PCRF core/SM service.
6. The PCRF core/SM service sends a GET request with `createContextOnFailure` enabled in spending limit header parameter toward PDS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

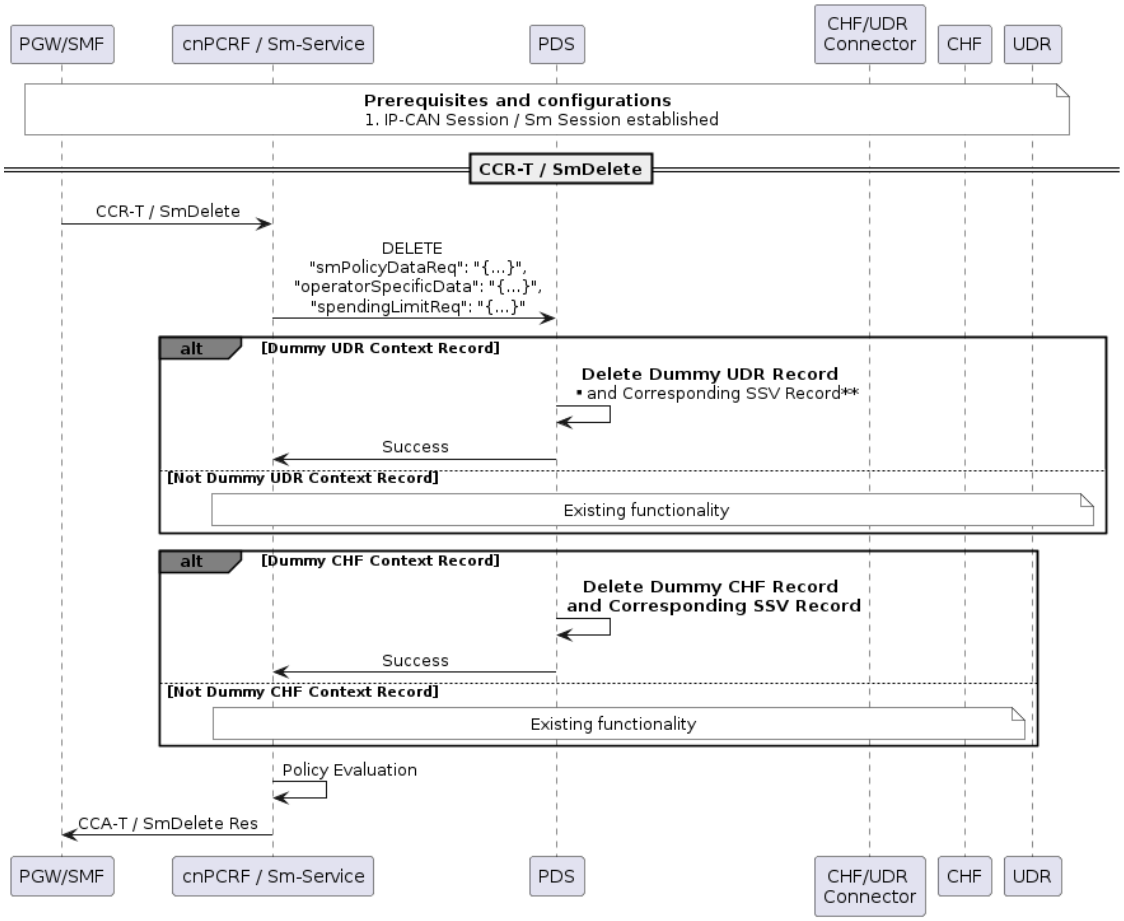
7. PDS sends successful `200 Success` response to PCRF core/SM service.
8. The PCRF core/SM service sends a CCA-I/SMCreateResponse or CCA-U/SMUpdateResponse toward PGW/SMF.
9. The PDS performs Database lockup:
   - If dummy context exists, and there is no valid data, then PDS sends SLR-Initial request toward OCS.
   - If valid data exits, then PDS sends SLR-Intermediate request toward OCS.
10. OCS sends successful "ocsSpendingLimitStatus" response to PDS. PDS sends a notification about "ocsSpendingLimitStatus" to PCRF Core/SM service.
11. OCS sends unsuccessful error response to PDS. If `createContextOnFailure` is enabled then ocsSpendingLimitStatus context information is written to database by PDS. If the flag is false, there is no database operation done by PDS.
12. PDS sends a notification `404 Not Found` request to PCRF Core/SM service.
13. PCRF Core/SM services sends policy evaluation request to PRE service.
14. PRE service sends policy evaluation response to PCRF Core/SM service.
15. PCRF Core/SM service sends RAR/UpdateNotify response to PGW/SMF.

PDS Dummy Context during SM Delete or PCRF Core CCR-T Call Flow

This section describes the SM Delete/CCR-T call flow and usage of the flag `createContextOnFailure` during CHF/UDR subscription failure.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-125 PDS Dummy Context during SM Delete or PCRF Core CCR-T Call Flow



1. The PGW/SMF sends a CCR-T/SM Delete request to PCRF Core/SM services via Diameter Gateway/Ingress Gateway.
2. PCRF core/SM services send delete request to PDS.
3. For the given subscriber, if the dummy context does not exists, then PDS deletes it and also the corresponding Subscriber State Variable (SSV).
4. If dummy context for related to the specific subscriber in the request exists then PDS deletes it and the corresponding Subscriber State Variable (SSV).
5. PDS sends successful `200 Success` response to PCRF core/SM services.
6. PCRF core/SM services perform policy evaluation and send the result as CCA-T/SM Delete response to PGW/SMF.

4.54 Enhancement to PRE Metrics

The following Policy blocks have been added to PRE to evaluate policy block execution counter and policy blocks execution time.

- Increment Counter Label
- Time

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see "Public Category" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.

To enable the PRE metrics, enable the **Enable Metrics** switch in the Policy Engine page under Service Configurations. By default, this switch remains disabled. For more information, see Policy Engine.

The following metrics have been added in PRE service for this feature:

- occnp_block_counter_label
- occnp_block_exec_time_ns

For more information, see PRE Metrics.

4.55 Enhancement to PCF Resiliency

PCF is enhanced to provide the mechanism in consumer service pods to cache the last successful producer pod information and use it when the subsequent producer pod discovery results in failure. Hence, the inter service communication continues to run even when the communication between the Kubernetes services and pods is down.

4.56 Support for cnDBTier APIs in CNC Console

With the implementation of this feature, cnDBTier APIs are integrated into the CNC Console, and Policy users can view specific cnDBTier functions, such as checking the cnDBTier version, status of cnDBTier clusters, and georeplication status on the CNC Console.

> **Note**
>
> This **cnDBTier** options can be accessed only through CNC Console.

The following cnDBTier functionalities are read only and can be viewed in the CNC Console:

- Backup List: This API displays the details of stored backups, such as the ID and size of the backup.
- cnDBTier Backup Status: This API checks the cnDBTier backup status.
- Database Statistics Report: This API displays the number of available database.
- Georeplication Status:
  - Real Time Overall Replication Status: This API displays the overall replication status in multisite deployments. For example, in a four-site deployment, it provides the replication status between the following sites: site1-site2, site1-site3, site1-site4, site2-site3, site2-site4, and site2-site1. This is applicable for all other sites.
  - Site Specific Real Time Replication Status: This API displays the site-specific replication status.
- Georeplication Status Across All Sites: This API is used to retrieve the georeplication status across all the configured sites, offering a consolidated view of the overall replication status.
- cnDBTier Health: This API displays the health status of the following services:
  - Replication Health Status: This API displays the health status of the replication service. It checks the following:

Copyright © 2019, 2026, Oracle and/or its affiliates.

    - if the replication service is up or not
    - if the replication service can connect to database or not
  - Monitor Health Status: This API displays the health status of the monitor service. It checks the following:
    - if the monitor service is up or not
    - if the service can connect to database or not
    - if the metrics are fetched or not (the metrics are fetched when the service is up and vice versa)

  NDB Health Status: This API displays the health status of the NDB service pods like (data pods, sql pods, app-my-sql pods, mgmt pods). It checks the following:

  - if the pod is connected to PVC or not
  - if the pods status is up or not

  > **Note**
  >
  > PVC Health Status attribute is set to NA when some of the database pods are not connected to the PVC.
  >
  > - Backup Manager Health Status: This API displays the health status of the backup manager service. It checks the following:
  >   - if the backup manager service is up or not
  >   - if the service can connect to database or not

- HeartBeat Status: This API displays the connectivity status between the local site and the remote site to which Policy is connected.
- IP Family Preference: This API is used to configure or update the preferred IP family (IPv4 or IPv6) used for communication between the replication channels.
- Georeplication Recovery: This API provides the recovery status of georeplication for the cnDBTier cluster:
  - Update Cluster As Failed: This API is used to mark a disrupted cluster as failed.
  - Start Georeplication Recovery: This API is used to start the georeplication recovery process.
  - Georeplication Recovery Status: This API is used to monitor the recovery status of georeplication for both FAILED and ACTIVE cnDBTier sites.
- Local Cluster Status: This API displays the status of the local cluster.
- On-Demand Backup: This API provides options to initiate as well as the display the status of the on-demand backup. It also displays the status of initiated on-demand backups.
- cnDBTier version: This API displays the cnDBTier version.
- PCF Cluster DB State: This API displays the real-time status of the cluster state and NF database functional state in the cnDBTier database cluster.
- Gracefully Start Georeplication: This API is used to initiate the georeplication between a primary site and one or more remote sites.
- Gracefully Stop Georeplication: This API is used to stop georeplication between a primary site and specified remote sites.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing cnDBTier Functionalities in CNC Console

Enable
This feature is enabled automatically when cnDBTier is configured as an instance during the CNC Console deployment. For more information about integrating cnDBTier functionalities in CNC Console, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

> **Important**
>
> In order to enable this feature, make sure that cnDBTier 25.1.200 or later versions is used.

Configure

You can view cnDBTier functionalities at CNC Console in the Viewing cnDBTier APIs in CNC Console section.

> **Note**
>
> The PCF Cluster DB State configurations can be updated with the `custom.values.yaml` for AppInfo service along with the Helm install/upgrade process. The Helm process update the `configMap` with the configurations which are mounted in the AppInfo pods. Normally, an upgrade between releases should restart pods and reflect the configuration changes. In a rare case that an in-release upgrade is needed, it is mandatory to restart the AppInfo pods manually to sync the configuration.
>
> Also, DB status considers the PCF's status reported by NRF Client. The `status/category/pcf` API is used monitor the PCF status.

Maintain

If you encounter alerts at the system level, see the Alerts section for resolution steps.

In case the alerts persist, perform the following tasks:

1. **Collect the logs**: For information about how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
2. **Raise a service request**: For information about how to raise a service request, see My Oracle Support.

4.57 Support for Non-SUPI based On-Demand Discovery Caching of NF Profiles

Policy supports the caching of NF profiles at NRF Client received from non-SUPI based on-demand discovery from NRF. Caching the NF profiles at NRF Client avoids discovering the NF profiles from NRF for every new call flow.

- N15 - AMF Notification for AM Policy (NFSetid based discovery for retry on Notification Request failure)

Copyright © 2019, 2026, Oracle and/or its affiliates.

- N15 - AMF Notification for UE Policy (NFSetid based discovery for retry on Notification Request failure)
- N7 - SMF Notification for SM Policy (NFSetid based discovery for retry on Notification Request failure)
- N15 - AMF discovery, AMF as a producer for UE Policy N1N2 Message Subscribe (GUAMI, amf-region-id,amf-set-id)
- N15 - AMF rediscovery, AMF as a producer for UE Policy N1N2 Message Transfer failure retry (NFSetid based discovery)
- UDR Rediscovery, UDR as a producer for SM, AM and UE Policy session, when POST(if considered subsequent), PUT, PATCH, Delete request failure, (NFSetid based discovery)

This allows NRF client to map and cache discovery query parameters against their on-demand discovery responses, allowing NRF Client to reuse those responses until they expire and reduces the number of requests sent to NRF for such discoveries.

Policy supports:

- caching the discovered producer/Notify Consumers profiles from NRF along with its query parameter for on-demand discovered NFs.
- rediscovering the NF Profiles whose TTLs have expired, when there is an on-demand discovery request for the same. That is, rediscovering the NF profiles based on the query parameter, when required during a signaling or call flow, if the validity period of the cached discovery response has expired. The expired records are updated with the recently rediscovered records after rediscovery is successful with 2xx response code.
- using the expired discovered profiles, which are in Registered state, if PCF cannot reach any NRFs during rediscovery.

The query from SM service, AM service, UE Policy service towards NRF Client can include the following two headers to support this feature:

- OC-Force-Rediscovery: Indicates whether to cache the NF profiles received from NRF in NRF Client or to skip caching and receive the response directly from NRF.

  Value of this parameter can be 0 or 1. By default, value of this parameter is set to 0.

  – When the value of OC-Force-Rediscovery parameter is set to 0, it enables the feature and caches the NF profiles details received from NRF.

  – When the value of OC-Force-Rediscovery parameter is set to 1, it disables the feature and retrieves the NF profiles directly from NRF while responding to the query from the backend services.
- OC-Retention-Period: Indicates the time a record is allowed to stay in database until the expiry period. This parameter accepts an integer value to indicate the retention period in milliseconds. When retention period is not configured/saved as null, backend will not send this header to NRF connector. By default, value of this parameter is set to 0.

Important

If occnp_nrf_client database is not yet created on NRF Client, you must manually create it. This database is used to store the cached profiles on NRF Client.

For details on how to create the database, see *Configuring Database, Creating Users, and Granting Permissions* section in *Oracle Communications Cloud Native Core, Installation, Upgrade, and Fault Recovery Guide* .

Copyright © 2019, 2026, Oracle and/or its affiliates.

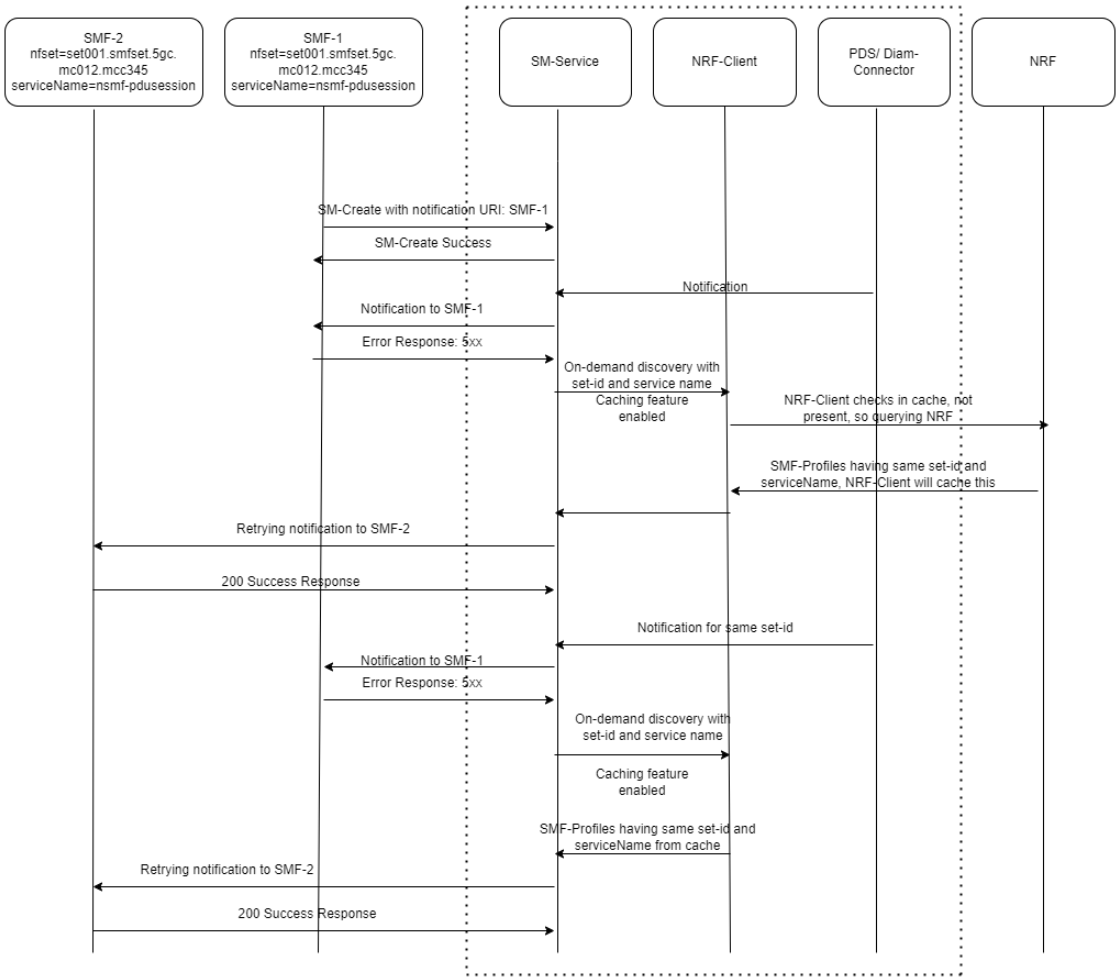
These headers can be configured by applying the configurations under NF Discovery Settings group in NF Communication Profiles for Common Data in Service Configuration.

The configurations are saved in common.public.communication-profile topic in the config server.

> **Note**
>
> The NF communication profile must be created and oc-forced-rediscovery, retention period must be configured before attaching the NF communication profile to service configuration page of SM service, AM service, UE Policy service, and User service.

Call Flow

Figure 4-126 SMF Notification for SM Policy (NFSetid based discovery for retry on Notification Request failure)



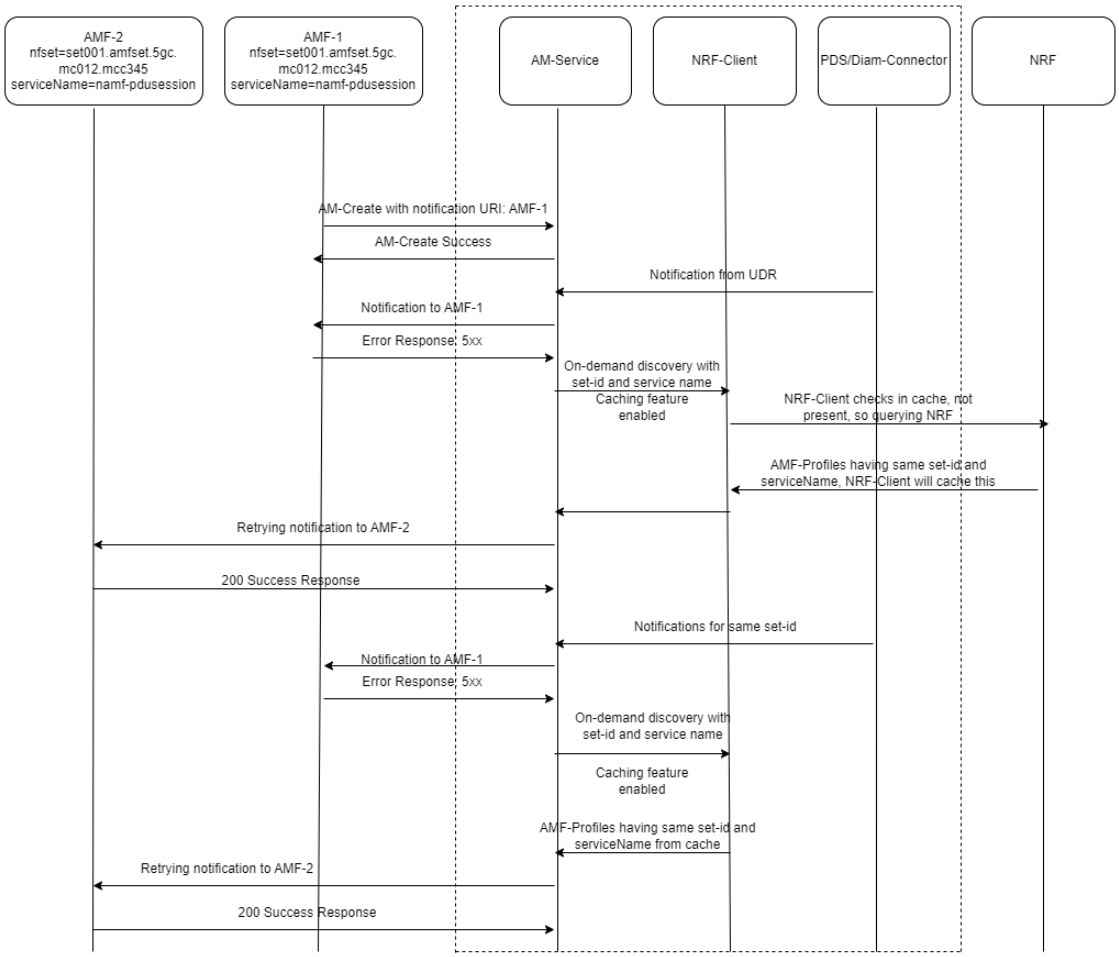
1. SMF1 sends an SM Create request to SM service.
2. After the successful creation, SM service responds to SMF1 with a successful message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Whenever there is a notification from UDR regarding any change in the user profile, PDS forwards the notification to SM service.
4. SM service forwards the notification to SMF1 and receives a 5xx error.
5. If the caching feature is enabled, SM service initiates an on-demand discovery caching with the given set ID and Service name and sends the request to NRF client.
6. As this is the first request and the data is not yet cached, NRF client sends the request to NRF to fetch the SMF profile information.
7. NRF responds with the SMF profile information for the given setID and service name.
8. NRF client caches these details in the database and sends the details to SM service.
9. SM service forwards the details to SMF2, which in turn responds with a 200 ok successful message.
10. Whenever PDS forwards an update notification from UDR to SM service.
11. SM service forwards the notification to SMF1 and receives an error in response.
12. SM service sends an on-demand discovery request to NRF client.
13. Now that the data is already cached for the given setID and service name, NRF client fetches the SMF Profiles from the cache and responds to SM service.
14. SM service sends the notification to SMF2 and receives a 200 ok successful message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-127 AMF Notification for AM Policy (NFSetid based discovery for retry on Notification Request failure)

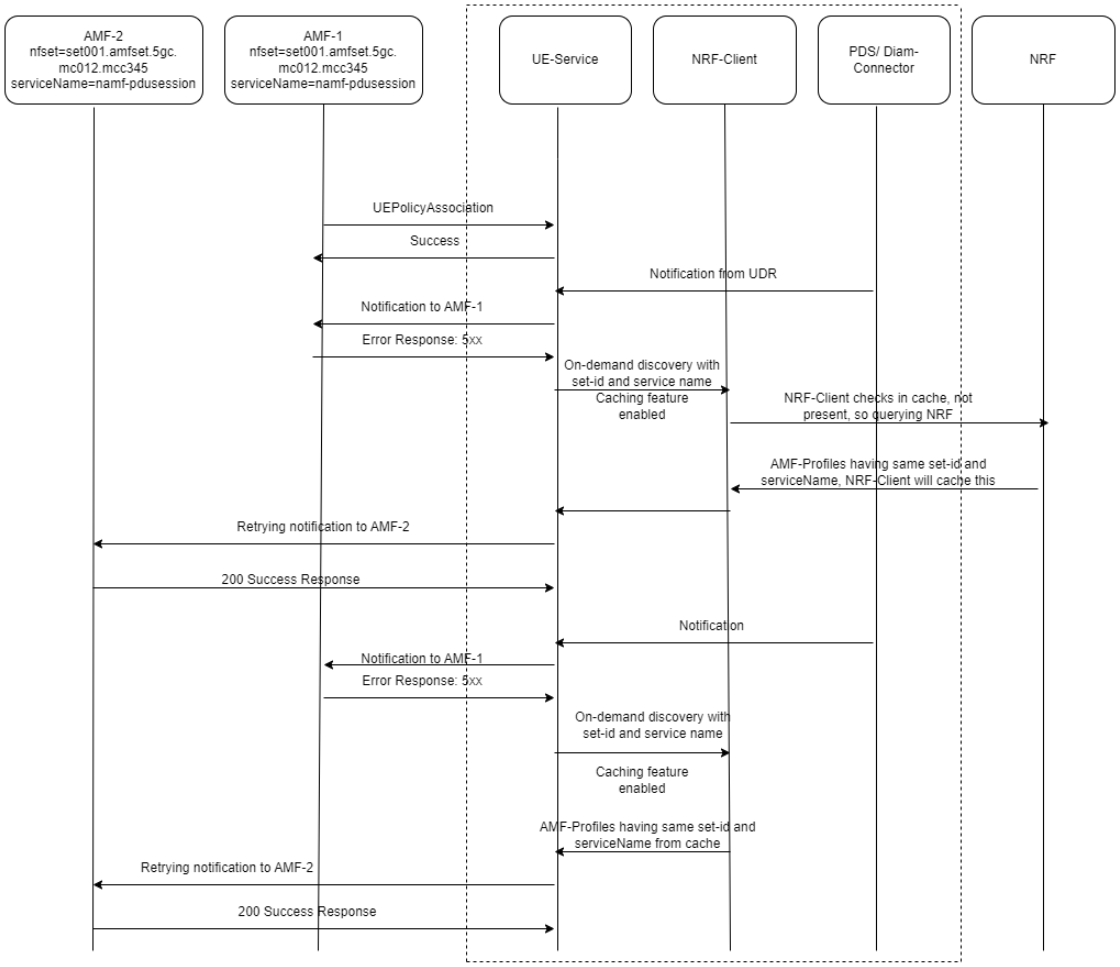


1. AMF1 sends an AM Create request to AM service.
2. After the successful creation, AM service responds to AMF1 with a successful message.
3. Whenever there is a notification from UDR regarding any change in the user profile, PDS forwards the notification to AM service.
4. AM service forwards the notification to AMF1 and receives a 5xx error.
5. If the caching feature is enabled, AM service initiates an on-demand discovery caching with the given set ID and Service name and sends the request to NRF client.
6. As this is the first request and the data is not yet cached, NRF client sends the request to NRF to fetch the AMF profile information for the give set ID and Service name.
7. NRF responds with the AMF profile information for the given setID and service name.
8. NRF client caches these details in the database and sends the details to AM service.
9. AM service forwards the details to AMF2, which in turn responds with a 200 ok successful message.
10. Whenever PDS forwards an update notification from UDR to AM service.
11. AM service forwards the notification to AMF1 and receives an error in response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

12. AM service sends an on-demand discovery request to NRF client.
13. Now that the data is already cached for the given setID and service name, NRF client fetches the AMF profile information from the cache and responds to AM service.
14. AM service sends the notification to AMF2 and receives a 200 ok successful message.

Figure 4-128 AMF Notification for UE Policy (NFSetid based discovery for retry on Notification Request failure)

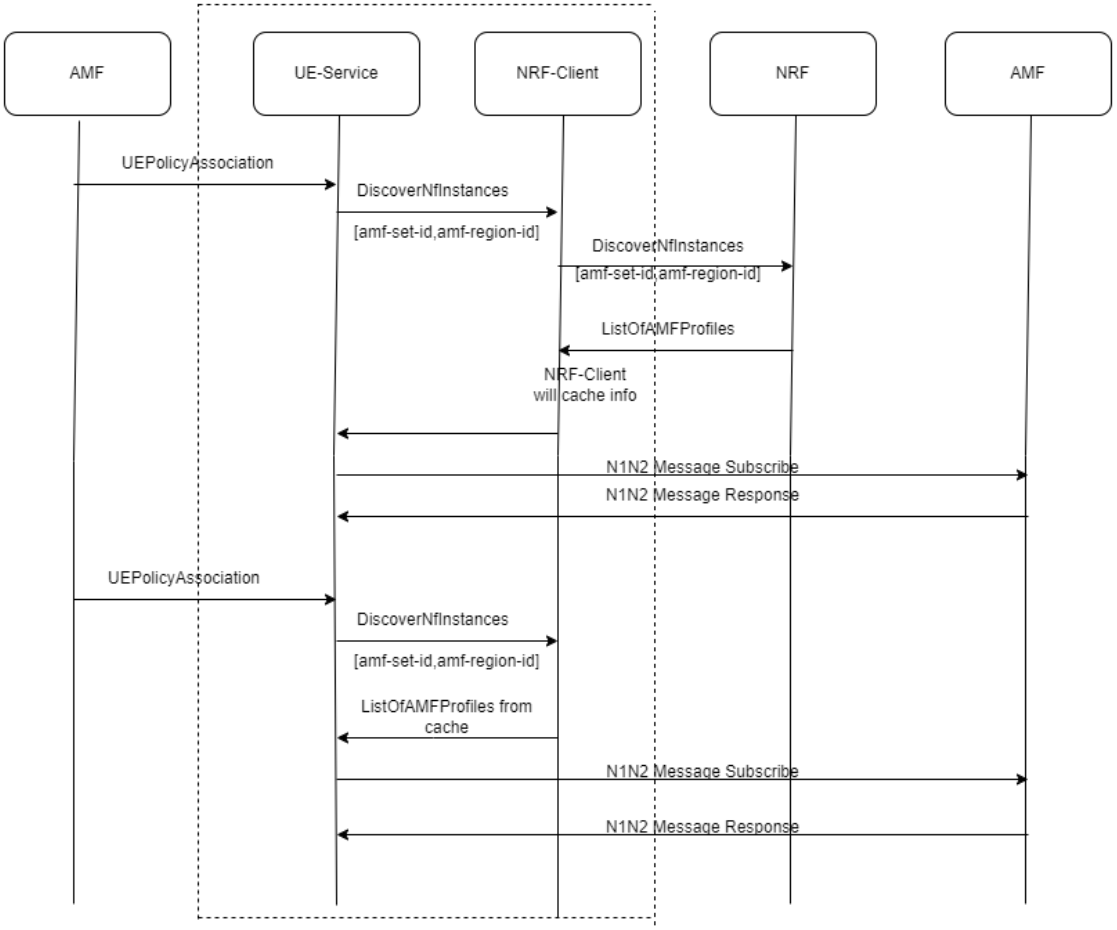


1. AMF1 sends an UE Create request to UE Policy service.
2. After the successful creation, UE Policy service responds to AMF1 with a successful message.
3. Whenever there is a notification from UDR regarding any change in the user profile, PDS forwards the notification to UE Policy service.
4. UE Policy service forwards the notification to AMF1 and receives a 5xx error.
5. If the caching feature is enabled, UE Policy service initiates an on-demand discovery caching with the given set ID and Service name and sends the request to NRF client.
6. As this is the first request and the data is not yet cached, NRF client sends the request to NRF to fetch the AMF profile information for the give set ID and Service name.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7. NRF responds with the AMF profile information for the given setID and service name.
8. NRF client caches these details in the database and sends the details to UE Policy service.
9. UE Policy service forwards the details to AMF2, which in turn responds with a 200 ok successful message.
10. Whenever PDS forwards an update notification from UDR to UE Policy service.
11. UE Policy service forwards the notification to AMF1 and receives an error in response.
12. UE Policy service sends an on-demand discovery request to NRF client.
13. Now that the data is already cached for the given setID and service name, NRF client fetches the AMF profile information from the cache and responds to UE Policy service.
14. UE Policy service sends the notification to AMF2 and receives a 200 ok successful message.

Figure 4-129 AMF Discovery/ Re-Discovery

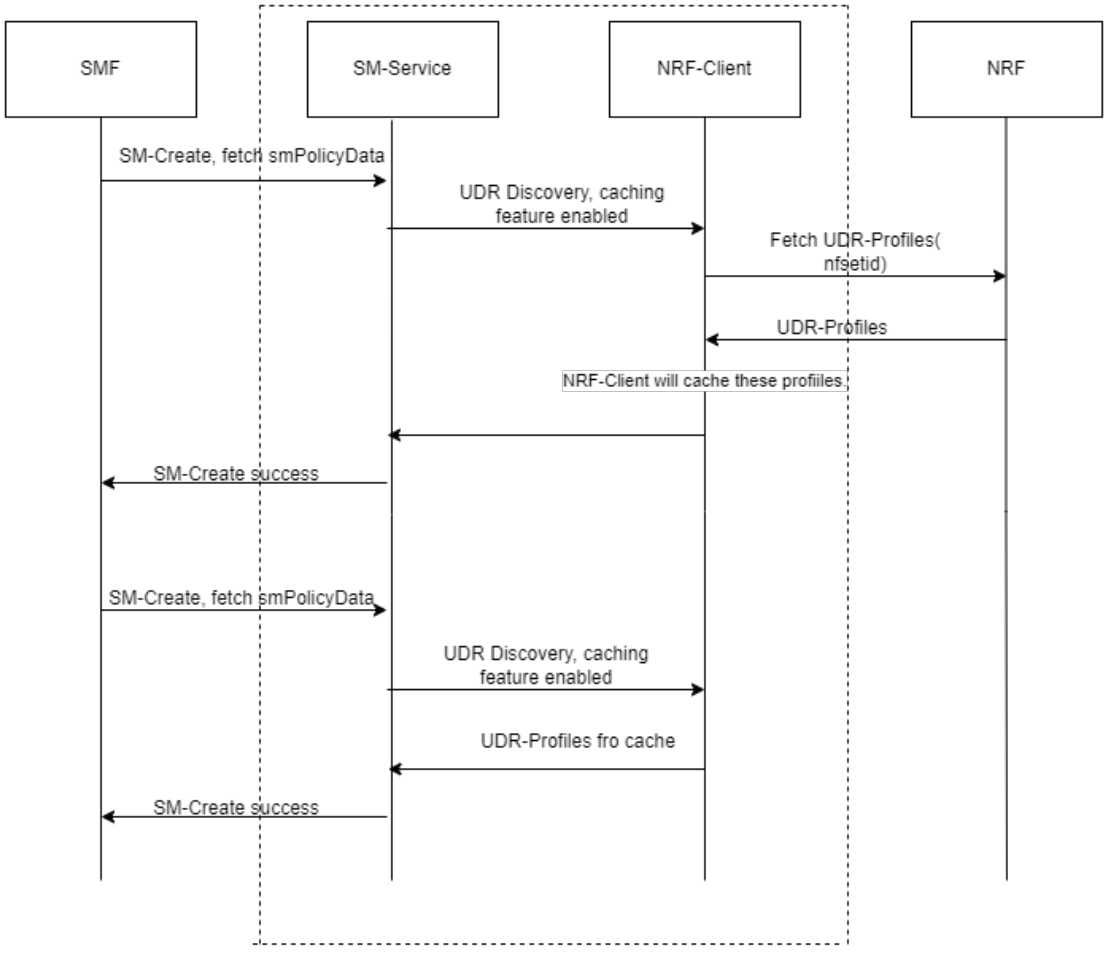


1. AMF Sends a UEPolicyAssociation request to UE Policy service.
2. UE Policy service sends a request to NRF Client to discover the NF instances using amf-set-id and amf-region-id.
3. NRF client forwards the request to NRF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. NRF responds to NRF client with the list of AMF Profiles matching the given amf-set-id and amf-region-id.
5. NRF Client caches these AMF Profiles and then responds to UE Policy service.
6. UE Policy service sends a N1N2 message subscription request to the AMF matching the amf-set-id and amf-region-id and receives a successful response.
7. When UE Policy service receives the next UEPolicyAssociation create request for the same amf-set-id and amf-region-id, it sends a request to NRF client to fetch the AMF profiles.
8. As the data is already cached, NRF client fetches the AMF profiles from its cache and responds to UE Policy service.
9. UE Policy service sends the N1N2 message subscription request to the required AMF and receives a successful response.

Figure 4-130 Non-SUPI based on-demand discovery caching for User Service



1. SMF sends an SM Create request to SM service.
2. SM service sends a request to NRF client to fetch the UDR profiles details.
3. NRF client sends the request to NRF and receives the list of UDR profiles matching the given nfsetID.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. If the caching feature is enabled, NRF client caches these UDR profiles and then forwards the details to SM service.
5. After the successful creation of SMPolicyAssociation, SM service responds to SMF.
6. Whenever SMF sends another SM Create request to SM service, SM service sends a request to NRF client to fetch the UDR profiles.
7. As the data is already cached, NRF client fetches the UDR profiles with the matching nfsetID from its cache and responds to SM service.
8. After the successful creation of SMPolicyAssociation, SM service responds to SMF.

Managing the Feature

Enable

By default, this feature is disabled. You can enable caching of the NF Profiles at NRF client using CNC Console or REST API for Policy.

Enable using CNC Console:

To enable the feature using CNC Console configure:

- **Force Discovery** parameter under **On Demand Discovery Caching** section on **NF Communication Profile** page. The **NF Communication Profile** page is available under **Common Data** for **Service Configurations**.
- **Enable Caching** parameter under **On Demand Discovery Caching** section on **NRF Agent** page, The **NRF Agent** page is available under **Service Configurations**.

For more information about enabling the feature through CNC Console, see NF Communication Profiles.

Enable using REST API:

You can enable the feature using:

- NF Communication Profiles API by configuring the value of `forceDiscovery` parameter under `onDemandDiscoveryCaching` section to 0.
- NRF Agent Service API by configuring the value of `enableFeature` parameter under `onDemandDiscoveryCaching` section to `true`.

For more information about enabling the feature through REST API, see *NF Communication Profiles* in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure this feature using the CNC Console or REST API for Policy.

Configure using CNC Console

- To configure caching of the NF profiles at NRF client at global level, perform the following configurations under **On Demand Discovery Caching** section on **NRF Agent** page, The **NRF Agent** page is available under **Service Configurations**. For more information, see NRF Agent.
- To configure the retention period of the cached data, perform the following configurations under **On Demand Discovery Caching** section on **NF Communication Profile** page. The **NF Communication Profile** page is available under **Common Data** for **Service Configurations**. For more information, see NF Communication Profiles.

Configure using REST API

Copyright © 2019, 2026, Oracle and/or its affiliates.

You can configure this feature using NF Communication Profiles and NRF Agent Service APIs.

For more information, see *NF Communication Profiles* and *NRF Agent* sections in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics

The following NRF Client metrics are used for this feature:

- occnp_nrfclient_discovery_cache_support_force_discovery_total
- occnp_nrfclient_discovery_cache_support_cache_hit_total
- occnp_nrfclient_discovery_cache_support_about_to_expire_total
- occnp_nrfclient_discovery_cache_support_expired_total
- occnp_nrfclient_discovery_cache_support_failover
- occnp_nrfclient_discovery_cache_support_cache_non_cache_total
- occnp_nrfclient_discovery_cache_support_empty_response_total
- occnp_nrfclient_discovery_cache_support_cache_lookup_seconds
- occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_bucket
- occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_count
- occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_max
- occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_sum
- occnp_nrfclient_discovery_cache_support_backend_response_seconds
- occnp_nrfclient_discovery_cache_support_backend_response_seconds_bucket
- occnp_nrfclient_discovery_cache_support_backend_response_seconds_count
- occnp_nrfclient_discovery_cache_support_backend_response_seconds_max
- occnp_nrfclient_discovery_cache_support_backend_response_seconds_sum
- occnp_nrfclient_discovery_cache_support_profiles_bucket
- occnp_nrfclient_discovery_cache_support_profiles_count
- occnp_nrfclient_discovery_cache_support_profiles_max
- occnp_nrfclient_discovery_cache_support_profiles_sum

For more information, see NRF Client Metrics.

Logging

PCF services

```
AM-Service:
{"instant":
{"epochSecond":1687351821,"nanoOfSecond":727462057},"thread":"HttpLoggingJetty
HttpClient@4be14ed1-134","level":"DEBUG","loggerName":"ocpm.pcf.service.am.ret
ry.AlternateRoutingHelper","message":"nfcommunication profile attached in
settings NFCommProfile{nfCommunicationProfileName='nfcp_rtp_sameLoc',
policyNfCommunicationModel=MODEL_C(3),
nfDiscoverySettings=NFDiscoverySettings{discoveryParameters=[ocpm.pcf.resource
.common.model.DiscoveryParamCfg@33ee9d8b], sendDiscoveryHeaderInitMsg=false,
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

sendDiscoveryHeaderSubsequentMsg=false, sendTargetApiRootHeaderInitMsg=true,
onDemandDiscoverySettings=OnDemandDiscoveryCaching{forceDiscovery=1,
retentionPeriod=null}},
nfBindingSettings=NFBindingSettings{cfgBindingLevel=NF_SET(1),
sendBindingHeader=true, sendRoutingBindingHeader=true,
sendCallbackHeader=true},
nfServerSettings=NFServerSettings{sendServerHeader=false,
serverHeaderErrorCodes=null},
retryAndAlternateRoutingSettings=ocpm.pcf.resource.common.model.RetryAndAltern
ateRoutingSettings@4a752f56,
nfCorrelationSettings=null}","endOfBatch":false,"loggerFqcn":"org.apache.loggi
ng.slf4j.Log4jLogger","threadId":134,"threadPriority":5,"messageTimestamp":"20
23-06-21T12:50:21.727+0000"}
{"instant":
{"epochSecond":1687351821,"nanoOfSecond":727672162},"thread":"HttpLoggingJetty
HttpClient@4be14ed1-134","level":"DEBUG","loggerName":"ocpm.pcf.service.am.ret
ry.AlternateRoutingHelper","message":"ocForcedRediscovery is 1 and retention
Period is
null","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","
threadId":134,"threadPriority":5,"messageTimestamp":"2023-06-21T12:50:21.727+0
000"}
SM-Service:

{"instant":
{"epochSecond":1694159028,"nanoOfSecond":405961795},"thread":"boundedElastic-4
","level":"DEBUG","loggerName":"ocpm.pcf.service.sm.domain.component.retry.pro
files.AlternateRoutingHelper","message":" ocForcedRediscovery is 1 and
retentionPeriod is 5000
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":210,"threadPriority":5,"messageTimestamp":"2023-09-08T07:43:48.405+0000"
}

UE-Service:
{"instant":
{"epochSecond":1694169865,"nanoOfSecond":366771034},"thread":"pool-3-
thread-10","level":"DEBUG","loggerName":"ocpm.pcf.service.uepolicy.routing.Alt
ernateRoutingHelper","message":"NF Communication Profile attached in service
configuration is NFCommProfile{nfCommunicationProfileName='nfcp_rtp',
policyNfCommunicationModel=MODEL_C(3),
nfDiscoverySettings=NFDiscoverySettings{discoveryParameters=[ocpm.pcf.resource
.common.model.DiscoveryParamCfg@5d2c8a02], sendDiscoveryHeaderInitMsg=false,
sendDiscoveryHeaderSubsequentMsg=false, sendTargetApiRootHeaderInitMsg=true},
onDemandDiscoveryCaching=OnDemandDiscoveryCaching{forceDiscovery=1,
retentionPeriod=5000},
nfBindingSettings=NFBindingSettings{cfgBindingLevel=NF_SET(1),
sendBindingHeader=true, sendRoutingBindingHeader=true,
sendCallbackHeader=true, sendServiceName=false},
nfServerSettings=NFServerSettings{sendServerHeader=false,
serverHeaderErrorCodes=null},
retryAndAlternateRoutingSettings=ocpm.pcf.resource.common.model.RetryAndAltern
ateRoutingSettings@468b7e0a,
nfCorrelationSettings=null}","endOfBatch":false,"loggerFqcn":"org.apache.loggi
ng.slf4j.Log4jLogger","threadId":890,"threadPriority":5,"messageTimestamp":"20
23-09-08T10:44:25.366+0000"}
{"instant":
{"epochSecond":1694169865,"nanoOfSecond":366943366},"thread":"pool-3-

Copyright © 2019, 2026, Oracle and/or its affiliates.

thread-10","level":"DEBUG","loggerName":"ocpm.pcf.service.uepolicy.routing.Alt
ernateRoutingHelper","message":" ocForcedRediscovery is 1 and retentionPeriod
is 5000
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":890,"threadPriority":5,"messageTimestamp":"2023-09-08T10:44:25.366+0000"
}

User-Service:

{"instant":
{"epochSecond":1694170047,"nanoOfSecond":943574493},"thread":"UserService_Thre
adPool_16","level":"DEBUG","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.Alter
nateRouteServiceHelper","message":"NF-Communication Profile is
NFCommProfile{nfCommunicationProfileName='nfcp_rtp_diffSet_sameLoc',
policyNfCommunicationModel=MODEL_C(3),
nfDiscoverySettings=NFDiscoverySettings{discoveryParameters=[ocpm.pcf.resource
.common.model.DiscoveryParamCfg@75f2f60d], sendDiscoveryHeaderInitMsg=false,
sendDiscoveryHeaderSubsequentMsg=false, sendTargetApiRootHeaderInitMsg=true},
onDemandDiscoveryCaching=OnDemandDiscoveryCaching{forceDiscovery=1,
retentionPeriod=5000},
nfBindingSettings=NFBindingSettings{cfgBindingLevel=NF_SET(1),
sendBindingHeader=true, sendRoutingBindingHeader=true,
sendCallbackHeader=true, sendServiceName=false},
nfServerSettings=NFServerSettings{sendServerHeader=false,
serverHeaderErrorCodes=null},
retryAndAlternateRoutingSettings=ocpm.pcf.resource.common.model.RetryAndAltern
ateRoutingSettings@3b6541ce, nfCorrelationSettings=null}, oc-forced-discovery
is 1 and retention period is
5000","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","
threadId":276,"threadPriority":5,"messageTimestamp":"2023-09-08T10:47:27.943+0
000"}
{"instant":
{"epochSecond":1694170047,"nanoOfSecond":943677402},"thread":"UserService_Thre
adPool_16","level":"DEBUG","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.Alter
nateRouteServiceHelper","message":" OC-Forced-Rediscovery is
1","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thr
eadId":276,"threadPriority":5,"messageTimestamp":"2023-09-08T10:47:27.943+0000
"}

NRF Client

For SM Service:

{"instant":
{"epochSecond":1702446905,"nanoOfSecond":450166996},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Checking if cache applies for a discovery
request (DiscoveryCache feature enabled: true, OC-Force-Rediscovery
requested:
false)","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.450+
0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":507483619},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Query Parameters validation. IsFullyMatch ->"

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
true, Params from request -> [target-nf-type, requester-nf-type, service-
names, target-nf-set-id], Params from config -> [target-nf-type, requester-nf-
type, service-names, target-nf-set-
id]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.507+000
0"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":507762621},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrul
es.DiscoveryRule","message":"DiscoveryCache is enabled and queryParameters
matched. Proceeding with DiscoveryResponse retrieval from
memory","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.507+
0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":508175763},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryEvaluator","message":"Rule applied:
CacheRule","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.5
08+0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":508393875},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.CacheRule","message":"Applying Cache Rule, grabbing NRF response from
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.508+0
000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":813463474},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Unsuccessful retrieval of
Discovery Response from Cache/DB, proceeding retrieval from NRF and saving
response in Cache/
DB","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th
readId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.813+0000
"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":813770323},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"SearchData :
{\"targetNfType\":\"SMF\",\"serviceNames\":[\"nsmf-
pdusession\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serv
iceInfoParamsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSet
Id\":\"set001.smfset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryPa
rameters\":\"target-nf-type=SMF&requester-nf-type=PCF&target-nf-set-
id=set001.smfset.5gc.mnc012.mcc345&service-names=nsmf-
pdusession\",\"forceRediscoveryEnabled\":false}","endOfBatch":false,"loggerFqc
n":"org.apache.logging.slf4j.Log4jLogger","threadId":90,"threadPriority":5,"me
ssageTimestamp":"2023-12-13T05:55:05.813+0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":814870367},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Entering sendOnDemandNfDiscoverRequest
function","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.8
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

14+0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":819222220},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Send NfDiscover request with searchData:
{\"targetNfType\":\"SMF\",\"serviceNames\":[\"nsmf-
pdusession\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serv
iceInfoParamsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSet
Id\":\"set001.smfset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryPa
rameters\":\"target-nf-type=SMF&requester-nf-type=PCF&target-nf-set-
id=set001.smfset.5gc.mnc012.mcc345&service-names=nsmf-
pdusession\",\"forceRediscoveryEnabled\":false}","endOfBatch":false,"loggerFqc
n":"org.apache.logging.slf4j.Log4jLogger","threadId":101,"threadPriority":5,"m
essageTimestamp":"2023-12-13T05:55:05.819+0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":819761612},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"sendRequestToNrf nrfRequest : NRFRequest [scheme=http,
rootURI=nf1stub.gi-dina.svc:8080, resourcePath=/nnrf-disc/v1/nf-instances,
method=GET, body=null, headers=[],
searchData={\"targetNfType\":\"SMF\",\"serviceNames\":[\"nsmf-
pdusession\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serv
iceInfoParamsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSet
Id\":\"set001.smfset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryPa
rameters\":\"target-nf-type=SMF&requester-nf-type=PCF&target-nf-set-
id=set001.smfset.5gc.mnc012.mcc345&service-names=nsmf-
pdusession\",\"forceRediscoveryEnabled\":false}, routeCount=0,
requestType=NFDISCOVER]","endOfBatch":false,"loggerFqcn":"org.apache.logging.s
lf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-1
2-13T05:55:05.819+0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":823597913},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,
nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
05:55:05.823+0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":824455718},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"Sending request to NRF nf1stub.gi-dina.svc:8080, routeCount=0,
attempt=0","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.
824+0000"}
{"instant":
{"epochSecond":1702446905,"nanoOfSecond":824609434},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"trigger","endOfBatch":false,"loggerFqcn":"org.apache.logging.sl
f4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12
-13T05:55:05.824+0000"}
{"instant":

Copyright © 2019, 2026, Oracle and/or its affiliates.

{"epochSecond":1702446905,"nanoOfSecond":824752596},"thread":"pool-10-thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientApi","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig [serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0, nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1, errorReasonsForFailure=[503, 504, 500, SocketTimeoutException, JsonProcessingException, UnknownHostException, NoRouteToHostException], gatewayErrorCodes=[503], requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.824+0000"}
{"instant":{"epochSecond":1702446905,"nanoOfSecond":928605343},"thread":"pool-10-thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientApi","message":"Request returned response with status code : 200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:05.928+0000"}
{"instant":{"epochSecond":1702446906,"nanoOfSecond":28211509},"thread":"pool-10-thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientApi","message":"Successful Response code received","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T05:55:06.028+0000"}
{"instant":{"epochSecond":1702446906,"nanoOfSecond":28712480},"thread":"pool-10-thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientApi","message":"sendOnDemandNfDiscoverRequest with searchData: {\"targetNfType\":\"SMF\",\"serviceNames\":[\"nsmf-pdusession\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoParamsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"set001.smfset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"...

AM Service:

Discovery of AMF for the first time:

{"instant":{"epochSecond":1702447453,"nanoOfSecond":267776264},"thread":"XNIO-1 task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrules.DiscoveryRule","message":"Checking if cache applies for a discovery request (DiscoveryCache feature enabled: true, OC-Force-Rediscovery requested: false)","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.267+0000"}
{"instant":{"epochSecond":1702447453,"nanoOfSecond":267885332},"thread":"XNIO-1 task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrules.DiscoveryRule","message":"Query Parameters validation. IsFullyMatch -> true, Params from request -> [target-nf-type, requester-nf-type, target-nf-set-id], Params from config -> [target-nf-type, requester-nf-type, service-names, target-nf-set-id]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
hreadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.267+000
0"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":268118684},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrul
es.DiscoveryRule","message":"DiscoveryCache is enabled and queryParameters
matched. Proceeding with DiscoveryResponse retrieval from
memory","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.268+
0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":268173836},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryEvaluator","message":"Rule applied:
CacheRule","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.2
68+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":268214963},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.CacheRule","message":"Applying Cache Rule, grabbing NRF response from
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.268+0
000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":279713217},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Unsuccessful retrieval of
Discovery Response from Cache/DB, proceeding retrieval from NRF and saving
response in Cache/
DB","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th
readId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.279+0000
"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":279876856},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"SearchData :
{\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":
false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enableF5\":false,
\"targetNfSetId\":\"set001.region01.amfset.5gc.mnc012.mcc345\",\"retentionPeri
od\":3000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region01.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals
e}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th
readId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.279+0000
"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":280256953},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Entering sendOnDemandNfDiscoverRequest
function","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.2
80+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":282059938},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

i","message":"Send NfDiscover request with searchData:
{\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":
false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enableF5\":false,
\"targetNfSetId\":\"set001.region01.amfset.5gc.mnc012.mcc345\",\"retentionPeri
od\":3000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region01.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals
e}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th
readId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.282+000
0"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":282199870},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"sendRequestToNrf nrfRequest : NRFRequest [scheme=http,
rootURI=nf1stub.gi-dina.svc:8080, resourcePath=/nnrf-disc/v1/nf-instances,
method=GET, body=null, headers=[],
searchData={\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParam
sPresent\":false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enable
F5\":false,\"targetNfSetId\":\"set001.region01.amfset.5gc.mnc012.mcc345\",\"re
tentionPeriod\":3000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region01.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals
e}, routeCount=0,
requestType=NFDISCOVER]","endOfBatch":false,"loggerFqcn":"org.apache.logging.s
lf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-1
2-13T06:04:13.282+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":282424344},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,
nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:04:13.282+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":282532830},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"Sending request to NRF nf1stub.gi-dina.svc:8080, routeCount=0,
attempt=0","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.
282+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":282579698},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"trigger","endOfBatch":false,"loggerFqcn":"org.apache.logging.sl
f4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12
-13T06:04:13.282+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":282628294},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,

Copyright © 2019, 2026, Oracle and/or its affiliates.

nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:04:13.282+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":306471240},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Request returned response with status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.306+00
00"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":311674972},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Successful Response code
received","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.3
11+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":311771862},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"sendOnDemandNfDiscoverRequest with searchData:
{\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":
false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enableF5\":false,
\"targetNfSetId\":\"set001.region01.amfset.5gc.mnc012.mcc345\",\"retentionPeri
od\":3000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region01.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals
e} returned status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.311+00
00"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":311992401},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"Received Discovery Result. Code:
200, Body (SearchResult): {\"validityPeriod\": 300, \"nfInstances\":
[{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797faaaf\",
\"nfSetIdList\": [\"set001.region01.amfset.5gc.mnc012.mcc345\"],
\"allowedNfTypes\": [\"PCF\", \"SMF\"], \"nfType\": \"AMF\", \"plmnList\":
[{\"mcc\": \"450\", \"mnc\": \"05\"}], \"nfStatus\": \"REGISTERED\",
\"fqdn\": \"nf2stub.gi-dina.svc\", \"priority\": 1, \"capacity\": 100,
\"load\": 50, \"locality\": \"1\", \"amfInfo\": {\"amfRegionId\": \"01\",
\"amfSetId\": \"001\", \"guamiList\": [{\"plmnId\": {\"mcc\": \"450\",
\"mnc\": \"05\"}, \"amfId\": \"010041\"}]}, \"nfServices\":
[{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\", \"serviceName\": \"namf-
comm\", \"versions\": [{\"apiVersionInUri\": \"v1\", \"apiFullVersion\":
\"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\": [{\"ipv4Address\":
null, \"ipv6Address\": null, \"transport\": \"TCP\", \"port\": 8080}],
\"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}]}]},
{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797fbbbf\", \"nfSetIdList\":
[\"set001.region01.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",

Copyright © 2019, 2026, Oracle and/or its affiliates.

\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf21stub.gi-dina.svc\",
\"priority\": 2, \"capacity\": 100, \"load\": 50, \"locality\": \"1\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}]}]},
{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797fcccf\", \"nfSetIdList\":
[\"set001.region01.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",
\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf3stub.gi-dina.svc\",
\"priority\": 4, \"capacity\": 100, \"load\": 60, \"locality\": \"2\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}]}]},
{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797fdddf\", \"nfSetIdList\":
[\"set001.region01.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",
\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf31stub.gi-dina.svc\",
\"priority\": 2, \"capacity\": 100, \"load\": 50, \"locality\": \"2\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}]}]},
{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797feeef\", \"nfSetIdList\":
[\"set001.region01.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",
\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf32stub.gi-dina.svc\",
\"priority\": 5, \"capacity\": 100, \"load\": 60, \"locality\": \"2\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}]}]}]}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4j
Logger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:
13.311+0000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":313001061},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf

Copyright © 2019, 2026, Oracle and/or its affiliates.

.GetNrfDiscoveryResponseUseCase","message":"Dynamic discovery cache enabled :
false","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:13.313+0
000"}
{"instant":
{"epochSecond":1702447453,"nanoOfSecond":353052224},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response fetched :
DiscoverySearchResult{queryParams='target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-id=set001.region01.amfset.5gc.mnc012.mcc345',
searchResult={\"validityPeriod\":300,\"nfInstances\":
[{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797faaaf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf2stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":1,\"capacity\":100,\"load\":50,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797fbbbf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf21stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":50,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797fcccf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf3stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":4,\"capacity\":100,\"load\":60,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797fdddf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf31stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":50,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":

Copyright © 2019, 2026, Oracle and/or its affiliates.

{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797feeef\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf32stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":5,\"capacity\":100,\"load\":60,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]}],\"nrfSupportedFeatures\":\"72\"},
sourceType=NRF}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log
4jLogger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:0
4:13.353+0000"}

Discovery of AMF for the second time

{"instant":
{"epochSecond":1702447495,"nanoOfSecond":560602127},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Checking if cache applies for a discovery
request (DiscoveryCache feature enabled: true, OC-Force-Rediscovery
requested:
false)","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.560+
0000"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":560665276},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Query Parameters validation. IsFullyMatch ->
true, Params from request -> [target-nf-type, requester-nf-type, target-nf-
set-id], Params from config -> [target-nf-type, requester-nf-type, service-
names, target-nf-set-
id]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.560+000
0"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":560736605},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrul
es.DiscoveryRule","message":"DiscoveryCache is enabled and queryParameters
matched. Proceeding with DiscoveryResponse retrieval from
memory","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.560+

Copyright © 2019, 2026, Oracle and/or its affiliates.

0000"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":560773857},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryEvaluator","message":"Rule applied:
CacheRule","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.5
60+0000"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":560806304},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.CacheRule","message":"Applying Cache Rule, grabbing NRF response from
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.560+0
000"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":578396526},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Successful retrieval of
Discovery Response stored in Cache/DB, proceeding with
validation","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog
ger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.
578+0000"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":578450087},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response retrieved
from Cache/DB isAboutToExpire value : false
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.578+0000"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":578490288},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response retrieved
from Cache/DB is expired value : false
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:04:55.578+0000"}
{"instant":
{"epochSecond":1702447495,"nanoOfSecond":589440279},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response fetched :
DiscoverySearchResult{queryParams='target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-id=set001.region01.amfset.5gc.mnc012.mcc345',
searchResult={\"validityPeriod\":300,\"nfInstances\":
[{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797faaaf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf2stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":1,\"capacity\":100,\"load\":50,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\

Copyright © 2019, 2026, Oracle and/or its affiliates.

"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797fbbbf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf21stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":50,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797fcccf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf3stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":4,\"capacity\":100,\"load\":60,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797fdddf\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf31stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":50,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797feeef\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf32stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":5,\"capacity\":100,\"load\":60,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region01.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}]}]}],\"nrfSupportedFeatures\":\"72\"},
sourceType=CACHE}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.L

Copyright © 2019, 2026, Oracle and/or its affiliates.

og4jLogger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06
:04:55.589+0000"}

UE Policy Service:

Discovery of AMF for UE policy Association for the first time:

{"instant":
{"epochSecond":1702447646,"nanoOfSecond":16500495},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Checking if cache applies for a discovery
request (DiscoveryCache feature enabled: true, OC-Force-Rediscovery
requested:
false)","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.016+
0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":16566854},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Query Parameters validation. IsFullyMatch ->
true, Params from request -> [target-nf-type, requester-nf-type, target-nf-
set-id], Params from config -> [target-nf-type, requester-nf-type, target-nf-
set-
id]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.016+000
0"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":16634530},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrul
es.DiscoveryRule","message":"DiscoveryCache is enabled and queryParameters
matched. Proceeding with DiscoveryResponse retrieval from
memory","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.016+
0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":16668622},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryEvaluator","message":"Rule applied:
CacheRule","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.0
16+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":16697142},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.CacheRule","message":"Applying Cache Rule, grabbing NRF response from
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.016+0
000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":26184667},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Unsuccessful retrieval of
Discovery Response from Cache/DB, proceeding retrieval from NRF and saving
response in Cache/
DB","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th

Copyright © 2019, 2026, Oracle and/or its affiliates.

readId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.026+0000
"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":26250918},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"SearchData :
{\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":
false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enableF5\":false,
\"targetNfSetId\":\"set001.region48.amfset.5gc.mnc012.mcc345\",\"retentionPeri
od\":5000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region48.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals
e}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th
readId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.026+0000
"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":26465561},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Entering sendOnDemandNfDiscoverRequest
function","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.0
26+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":27251963},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Send NfDiscover request with searchData:
{\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":
false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enableF5\":false,
\"targetNfSetId\":\"set001.region48.amfset.5gc.mnc012.mcc345\",\"retentionPeri
od\":5000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region48.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals
e}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th
readId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.027+000
0"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":27393966},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"sendRequestToNrf nrfRequest : NRFRequest [scheme=http,
rootURI=nf1stub.gi-dina.svc:8080, resourcePath=/nnrf-disc/v1/nf-instances,
method=GET, body=null, headers=[],
searchData={\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParam
sPresent\":false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enable
F5\":false,\"targetNfSetId\":\"set001.region48.amfset.5gc.mnc012.mcc345\",\"re
tentionPeriod\":5000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region48.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals
e}, routeCount=0,
requestType=NFDISCOVER]","endOfBatch":false,"loggerFqcn":"org.apache.logging.s
lf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-1
2-13T06:07:26.027+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":27518993},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,

Copyright © 2019, 2026, Oracle and/or its affiliates.

nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:07:26.027+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":27597244},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"Sending request to NRF nf1stub.gi-dina.svc:8080, routeCount=0,
attempt=0","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.
027+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":27630106},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"trigger","endOfBatch":false,"loggerFqcn":"org.apache.logging.sl
f4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12
-13T06:07:26.027+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":27663824},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,
nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:07:26.027+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":60172668},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Request returned response with status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.060+00
00"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":65762172},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Successful Response code
received","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.0
65+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":65848611},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"sendOnDemandNfDiscoverRequest with searchData:
{\"targetNfType\":\"AMF\",\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":
false,\"serviceInfoParamsPresent\":false,\"enableF3\":true,\"enableF5\":false,
\"targetNfSetId\":\"set001.region48.amfset.5gc.mnc012.mcc345\",\"retentionPeri
od\":5000,\"rawQueryParameters\":\"target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-
id=set001.region48.amfset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":fals

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
e} returned status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.065+00
00"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":66116142},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"Received Discovery Result. Code:
200, Body (SearchResult): {\"validityPeriod\": 1800, \"nfInstances\":
[{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797f111a\",
\"nfSetIdList\": [\"set001.region48.amfset.5gc.mnc012.mcc345\"],
\"allowedNfTypes\": [\"PCF\", \"SMF\"], \"nfType\": \"AMF\", \"plmnList\":
[{\"mcc\": \"450\", \"mnc\": \"05\"}], \"nfStatus\": \"REGISTERED\",
\"fqdn\": \"nf1stub.gi-dina.svc\", \"priority\": 1, \"capacity\": 100,
\"load\": 80, \"locality\": \"2\", \"amfInfo\": {\"amfRegionId\": \"01\",
\"amfSetId\": \"001\", \"guamiList\": [{\"plmnId\": {\"mcc\": \"450\",
\"mnc\": \"05\"}, \"amfId\": \"010041\"}]}, \"nfServices\":
[{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\", \"serviceName\": \"namf-
comm\", \"versions\": [{\"apiVersionInUri\": \"v1\", \"apiFullVersion\":
\"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\": [{\"ipv4Address\":
null, \"ipv6Address\": null, \"transport\": \"TCP\", \"port\": 8080}],
\"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}], \"priority\": 2,
\"capacity\": 100, \"load\": 80, \"locality\": \"2\"}]}, {\"nfInstanceId\":
\"13515195-c537-4645-9b97-96ec797f1111\", \"nfSetIdList\":
[\"set001.region48.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",
\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf12stub.gi-dina.svc\",
\"priority\": 2, \"capacity\": 100, \"load\": 80, \"locality\": \"2\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}],
\"priority\": 2, \"capacity\": 100, \"load\": 80, \"locality\": \"2\"}]},
{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797f2222\", \"nfSetIdList\":
[\"set001.region48.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",
\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf2stub.gi-dina.svc\",
\"priority\": 1, \"capacity\": 100, \"load\": 80, \"locality\": \"1\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}],
\"priority\": 1, \"capacity\": 100, \"load\": 80, \"locality\": \"1\"}]},
{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797f3333\", \"nfSetIdList\":
[\"set001.region48.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",
\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf22stub.gi-dina.svc\",
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

\"priority\": 2, \"capacity\": 100, \"load\": 80, \"locality\": \"1\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}],
\"priority\": 2, \"capacity\": 100, \"load\": 80, \"locality\": \"1\"}]},
{\"nfInstanceId\": \"13515195-c537-4645-9b97-96ec797f4444\", \"nfSetIdList\":
[\"set001.region48.amfset.5gc.mnc012.mcc345\"], \"allowedNfTypes\": [\"PCF\",
\"SMF\"], \"nfType\": \"AMF\", \"plmnList\": [{\"mcc\": \"450\", \"mnc\":
\"05\"}], \"nfStatus\": \"REGISTERED\", \"fqdn\": \"nf21stub.gi-dina.svc\",
\"priority\": 5, \"capacity\": 100, \"load\": 80, \"locality\": \"1\",
\"amfInfo\": {\"amfRegionId\": \"01\", \"amfSetId\": \"001\", \"guamiList\":
[{\"plmnId\": {\"mcc\": \"450\", \"mnc\": \"05\"}, \"amfId\": \"010041\"}]},
\"nfServices\": [{\"serviceInstanceId\": \"aaaa-bbbb-cccc-dddd\",
\"serviceName\": \"namf-comm\", \"versions\": [{\"apiVersionInUri\": \"v1\",
\"apiFullVersion\": \"1.1.0\", \"expiry\": \"2020-07-30T12:09:55.65Z\"}],
\"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"ipEndPoints\":
[{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\",
\"port\": 8080}], \"allowedPlmns\": [{\"mcc\": \"450\", \"mnc\": \"05\"}],
\"priority\": 5, \"capacity\": 100, \"load\": 80, \"locality\":
\"1\"}]}]}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog
ger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.
066+0000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":67989020},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"Dynamic discovery cache enabled :
false","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:07:26.067+0
000"}
{"instant":
{"epochSecond":1702447646,"nanoOfSecond":124766789},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response fetched :
DiscoverySearchResult{queryParams='target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-id=set001.region48.amfset.5gc.mnc012.mcc345',
searchResult={\"validityPeriod\":1800,\"nfInstances\":
[{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f111a\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf1stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":1,\"capacity\":100,\"load\":80,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":2,\"capacity\":100,\"load\":80
,\"locality\":\"2\"}]},{\"nfInstanceId\":\"13515195-

Copyright © 2019, 2026, Oracle and/or its affiliates.

c537-4645-9b97-96ec797f1111\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf12stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":80,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":2,\"capacity\":100,\"load\":80
,\"locality\":\"2\"}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f2222\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf2stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":1,\"capacity\":100,\"load\":80,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":1,\"capacity\":100,\"load\":80
,\"locality\":\"1\"}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f3333\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf22stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":80,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":2,\"capacity\":100,\"load\":80
,\"locality\":\"1\"}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f4444\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf21stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":5,\"capacity\":100,\"load\":80,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":5,\"capacity\":100,\"load\":80
,\"locality\":\"1\"}]}],\"nrfSupportedFeatures\":\"72\"},

Copyright © 2019, 2026, Oracle and/or its affiliates.

sourceType=NRF}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log
4jLogger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:0
7:26.124+0000"}

Discovery of AMF for UE policy association for the second time:

{"instant":
{"epochSecond":1702447706,"nanoOfSecond":365554062},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Checking if cache applies for a discovery
request (DiscoveryCache feature enabled: true, OC-Force-Rediscovery
requested:
false)","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.365+
0000"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":365614917},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Query Parameters validation. IsFullyMatch ->
true, Params from request -> [target-nf-type, requester-nf-type, target-nf-
set-id], Params from config -> [target-nf-type, requester-nf-type, target-nf-
set-
id]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.365+000
0"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":365677878},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrul
es.DiscoveryRule","message":"DiscoveryCache is enabled and queryParameters
matched. Proceeding with DiscoveryResponse retrieval from
memory","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.365+
0000"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":365705820},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryEvaluator","message":"Rule applied:
CacheRule","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.3
65+0000"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":365727980},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.CacheRule","message":"Applying Cache Rule, grabbing NRF response from
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.365+0
000"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":370207433},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Successful retrieval of
Discovery Response stored in Cache/DB, proceeding with
validation","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog
ger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
370+0000"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":370252164},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response retrieved
from Cache/DB isAboutToExpire value : false
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.370+0000"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":370285114},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response retrieved
from Cache/DB is expired value : false
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:08:26.370+0000"}
{"instant":
{"epochSecond":1702447706,"nanoOfSecond":378912228},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response fetched :
DiscoverySearchResult{queryParams='target-nf-type=AMF&requester-nf-
type=PCF&target-nf-set-id=set001.region48.amfset.5gc.mnc012.mcc345',
searchResult={\"validityPeriod\":1800,\"nfInstances\":
[{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f111a\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf1stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":1,\"capacity\":100,\"load\":80,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":2,\"capacity\":100,\"load\":80
,\"locality\":\"2\"}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f1111\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf12stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":80,\"locality\":\"2
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":2,\"capacity\":100,\"load\":80
,\"locality\":\"2\"}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f2222\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf2stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":1,\"capacity\":100,\"load\":80,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":1,\"capacity\":100,\"load\":80
,\"locality\":\"1\"}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f3333\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf22stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":2,\"capacity\":100,\"load\":80,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":2,\"capacity\":100,\"load\":80
,\"locality\":\"1\"}]},{\"nfInstanceId\":\"13515195-
c537-4645-9b97-96ec797f4444\",\"nfType\":\"AMF\",\"nfStatus\":\"REGISTERED\",\
"plmnList\":[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"fqdn\":\"nf21stub.gi-
dina.svc\",\"allowedNfTypes\":
[\"PCF\",\"SMF\"],\"priority\":5,\"capacity\":100,\"load\":80,\"locality\":\"1
\",\"nfSetIdList\":[\"set001.region48.amfset.5gc.mnc012.mcc345\"],\"amfInfo\":
{\"amfSetId\":\"001\",\"amfRegionId\":\"01\",\"guamiList\":[{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"}]},\"nfServices\":
[{\"serviceInstanceId\":\"aaaa-bbbb-cccc-dddd\",\"serviceName\":\"namf-
comm\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.1.0\",\"expiry\":\"2020-07
-30T12:09:55.650Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\",\
"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedPlmns\":
[{\"mcc\":\"450\",\"mnc\":\"05\"}],\"priority\":5,\"capacity\":100,\"load\":80
,\"locality\":\"1\"}]}],\"nrfSupportedFeatures\":\"72\"},
sourceType=CACHE}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.L
og4jLogger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06
:08:26.378+0000"}

UDR:

Discovery of UDR for th first time:

{"instant":
{"epochSecond":1702447911,"nanoOfSecond":703559369},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Checking if cache applies for a discovery

Copyright © 2019, 2026, Oracle and/or its affiliates.

request (DiscoveryCache feature enabled: true, OC-Force-Rediscovery
requested:
false)","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.703+
0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":703624658},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Query Parameters validation. IsFullyMatch ->
true, Params from request -> [target-nf-type, requester-nf-type, service-
names, target-nf-set-id], Params from config -> [target-nf-type, requester-nf-
type, service-names, target-nf-set-
id]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.703+000
0"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":703677942},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrul
es.DiscoveryRule","message":"DiscoveryCache is enabled and queryParameters
matched. Proceeding with DiscoveryResponse retrieval from
memory","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.703+
0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":703715314},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryEvaluator","message":"Rule applied:
CacheRule","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.7
03+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":703735621},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.CacheRule","message":"Applying Cache Rule, grabbing NRF response from
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.703+0
000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":711068647},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Unsuccessful retrieval of
Discovery Response from Cache/DB, proceeding retrieval from NRF and saving
response in Cache/
DB","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","th
readId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.711+0000
"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":711135709},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"SearchData :
{\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-
dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-

Copyright © 2019, 2026, Oracle and/or its affiliates.

id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false}","endO
fBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":9
0,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.711+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":711380511},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Entering sendOnDemandNfDiscoverRequest
function","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.7
11+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":712130386},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Send NfDiscover request with searchData:
{\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-
dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-
id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false}","endO
fBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":1
01,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.712+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":712257461},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"sendRequestToNrf nrfRequest : NRFRequest [scheme=http,
rootURI=nf1stub.gi-dina.svc:8080, resourcePath=/nnrf-disc/v1/nf-instances,
method=GET, body=null, headers=[],
searchData={\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-
dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false},
routeCount=0,
requestType=NFDISCOVER]","endOfBatch":false,"loggerFqcn":"org.apache.logging.s
lf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-1
2-13T06:11:51.712+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":712395565},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,
nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:11:51.712+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":712450944},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"Sending request to NRF nf1stub.gi-dina.svc:8080, routeCount=0,
attempt=0","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg

Copyright © 2019, 2026, Oracle and/or its affiliates.

er","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.
712+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":712478555},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"trigger","endOfBatch":false,"loggerFqcn":"org.apache.logging.sl
f4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12
-13T06:11:51.712+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":712505815},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,
nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:11:51.712+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":731529927},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Request returned response with status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.731+00
00"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":736236543},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Successful Response code
received","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.7
36+0000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":736285120},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"sendOnDemandNfDiscoverRequest with searchData:
{\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-
dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false}
returned status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.736+00
00"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":736499801},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"Received Discovery Result. Code:
200, Body (SearchResult): {\"validityPeriod\": 100, \"nfInstances\":
[{\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555550000000\",
\"nfSetIdList\": [\"set001.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\",
\"nfStatus\": \"REGISTERED\", \"plmnList\": null, \"nsiList\": null,

Copyright © 2019, 2026, Oracle and/or its affiliates.

\"fqdn\": \"nf2stub.gi-dina.svc\", \"interPlmnFqdn\": null,
\"ipv4Addresses\": null, \"ipv6Addresses\": null, \"priority\": 1,
\"capacity\": 50, \"load\": 10, \"locality\": \"1\", \"pcfInfo\": null,
\"udmInfo\": null, \"ausfInfo\": null, \"amfInfo\": null, \"smfInfo\": null,
\"upfInfo\": null, \"groupId\": \"udr1\", \"udrInfo\": {\"supiRanges\":
[{\"start\": \"450081000000000\", \"end\": \"450081002000000\"}],
\"gpsiRanges\": [{\"start\": \"13100000000\", \"end\": \"13102000000\"}],
\"supportedDataSets\": [\"POLICY\"]}, \"bsfInfo\": null, \"customInfo\":
null, \"recoveryTime\": null, \"nfServices\": [{\"serviceInstanceId\":
\"94d8d19a-b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\",
\"versions\": [{\"apiVersionInUri\": \"v1\", \"apiFullVersion\":
\"1.15.1.0\", \"expiry\": \"2019-08-03T18:55:08.871+0000\"}], \"scheme\":
\"http\", \"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null,
\"interPlmnFqdn\": null, \"ipEndPoints\": [{\"ipv4Address\": null,
\"ipv6Address\": null, \"transport\": \"TCP\", \"port\": 8080}],
\"apiPrefix\": null, \"defaultNotificationSubscriptions\": null,
\"allowedPlmns\": null, \"allowedNfTypes\": [\"CHF\", \"PCF\"],
\"allowedNfDomains\": null, \"allowedNssais\": null, \"priority\": 1,
\"capacity\": 100, \"load\": 50, \"locality\": \"1\", \"recoveryTime\":
1542876663222, \"supportedFeatures\": null}]}, {\"nfInstanceId\":
\"fe7d992b-0541-4c7d-ab84-555551111111\", \"nfSetIdList\":
[\"set001.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\":
\"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\":
\"nf21stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null,
\"ipv6Addresses\": null, \"priority\": 2, \"capacity\": 50, \"load\": 20,
\"locality\": \"2\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\":
null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\":
\"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\",
\"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\",
\"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]},
\"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null,
\"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\":
[{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\":
\"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null,
\"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null,
\"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null,
\"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null,
\"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null,
\"allowedNssais\": null, \"priority\": 2, \"capacity\": 50, \"load\": 20,
\"recoveryTime\": 1542876663222, \"supportedFeatures\": null}]},
{\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555553333333\", \"nfSetIdList\":
[\"set001.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\":
\"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\":
\"nf11stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null,
\"ipv6Addresses\": null, \"priority\": 4, \"capacity\": 50, \"load\": 10,
\"locality\": \"1\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\":
null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\":
\"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\",
\"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\",
\"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]},
\"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null,
\"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\":
[{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\":

Copyright © 2019, 2026, Oracle and/or its affiliates.

\"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null,
\"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null,
\"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null,
\"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null,
\"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null,
\"allowedNssais\": null, \"priority\": 4, \"capacity\": 50, \"load\": 10,
\"recoveryTime\": 1542876663222, \"supportedFeatures\": null}]},
{\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555554444444\", \"nfSetIdList\":
[\"set002.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\":
\"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\":
\"nf12stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null,
\"ipv6Addresses\": null, \"priority\": 5, \"capacity\": 50, \"load\": 40,
\"locality\": \"2\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\":
null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\":
\"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\",
\"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\",
\"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]},
\"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null,
\"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\":
[{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\":
\"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null,
\"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null,
\"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null,
\"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null,
\"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null,
\"allowedNssais\": null, \"priority\": 5, \"capacity\": 50, \"load\": 40,
\"recoveryTime\": 1542876663222, \"supportedFeatures\": null}]},
{\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555552222222\", \"nfSetIdList\":
[\"set002.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\":
\"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\":
\"nf22stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null,
\"ipv6Addresses\": null, \"priority\": 3, \"capacity\": 50, \"load\": 30,
\"locality\": \"1\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\":
null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\":
\"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\",
\"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\",
\"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]},
\"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null,
\"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\":
[{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\":
\"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null,
\"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null,
\"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null,
\"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null,
\"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null,
\"allowedNssais\": null, \"priority\": 3, \"capacity\": 50, \"load\": 30,
\"recoveryTime\": 1542876663222, \"supportedFeatures\":
null}]}]}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.7
36+0000"}
{"instant":

Copyright © 2019, 2026, Oracle and/or its affiliates.

{"epochSecond":1702447911,"nanoOfSecond":737221498},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"Dynamic discovery cache enabled :
false","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:11:51.737+0
000"}
{"instant":
{"epochSecond":1702447911,"nanoOfSecond":770303926},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response fetched :
DiscoverySearchResult{queryParams='target-nf-type=UDR&requester-nf-
type=PCF&service-names=nudr-dr&target-nf-set-
id=set001.udrset.5gc.mnc012.mcc345',
searchResult={\"validityPeriod\":100,\"nfInstances\":
[{\"nfInstanceId\":\"fe7d992b-0541-4c7d-
ab84-555550000000\",\"nfType\":\"UDR\",\"nfStatus\":\"REGISTERED\",\"fqdn\":\"
nf2stub.gi-
dina.svc\",\"priority\":1,\"capacity\":50,\"load\":10,\"locality\":\"1\",\"nfS
etIdList\":[\"set001.udrset.5gc.mnc012.mcc345\"],\"udrInfo\":{\"supiRanges\":
[{\"start\":\"450081000000000\",\"end\":\"450081002000000\"}],\"gpsiRanges\":
[{\"start\":\"13100000000\",\"end\":\"13102000000\"}],\"supportedDataSets\":
[\"POLICY\"]},\"nfServices\":[{\"serviceInstanceId\":\"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\",\"serviceName\":\"nudr-dr\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.15.1.0\",\"expiry\":\"2019
-08-03T18:55:08.871Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\
",\"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedNfTypes\":
[\"CHF\",\"PCF\"],\"priority\":1,\"capacity\":100,\"load\":50,\"recoveryTime\"
:\"2018-11-22T08:51:03.222Z\",\"locality\":\"1\"}],\"groupId\":\"udr1\"},
{\"nfInstanceId\":\"fe7d992b-0541-4c7d-
ab84-555551111111\",\"nfType\":\"UDR\",\"nfStatus\":\"REGISTERED\",\"fqdn\":\"
nf21stub.gi-
dina.svc\",\"priority\":2,\"capacity\":50,\"load\":20,\"locality\":\"2\",\"nfS
etIdList\":[\"set001.udrset.5gc.mnc012.mcc345\"],\"udrInfo\":{\"supiRanges\":
[{\"start\":\"450081000000000\",\"end\":\"450081002000000\"}],\"gpsiRanges\":
[{\"start\":\"13100000000\",\"end\":\"13102000000\"}],\"supportedDataSets\":
[\"POLICY\"]},\"nfServices\":[{\"serviceInstanceId\":\"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\",\"serviceName\":\"nudr-dr\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.15.1.0\",\"expiry\":\"2019
-08-03T18:55:08.871Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\
",\"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedNfTypes\":
[\"CHF\",\"PCF\"],\"priority\":2,\"capacity\":50,\"load\":20,\"recoveryTime\":
\"2018-11-22T08:51:03.222Z\"}],\"groupId\":\"udr1\"},
{\"nfInstanceId\":\"fe7d992b-0541-4c7d-
ab84-555553333333\",\"nfType\":\"UDR\",\"nfStatus\":\"REGISTERED\",\"fqdn\":\"
nf11stub.gi-
dina.svc\",\"priority\":4,\"capacity\":50,\"load\":10,\"locality\":\"1\",\"nfS
etIdList\":[\"set001.udrset.5gc.mnc012.mcc345\"],\"udrInfo\":{\"supiRanges\":
[{\"start\":\"450081000000000\",\"end\":\"450081002000000\"}],\"gpsiRanges\":
[{\"start\":\"13100000000\",\"end\":\"13102000000\"}],\"supportedDataSets\":
[\"POLICY\"]},\"nfServices\":[{\"serviceInstanceId\":\"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\",\"serviceName\":\"nudr-dr\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.15.1.0\",\"expiry\":\"2019
-08-03T18:55:08.871Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\
",\"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedNfTypes\":
[\"CHF\",\"PCF\"],\"priority\":4,\"capacity\":50,\"load\":10,\"recoveryTime\":
\"2018-11-22T08:51:03.222Z\"}],\"groupId\":\"udr1\"},

Copyright © 2019, 2026, Oracle and/or its affiliates.

{\"nfInstanceId\":\"fe7d992b-0541-4c7d-
ab84-555554444444\",\"nfType\":\"UDR\",\"nfStatus\":\"REGISTERED\",\"fqdn\":\"
nf12stub.gi-
dina.svc\",\"priority\":5,\"capacity\":50,\"load\":40,\"locality\":\"2\",\"nfS
etIdList\":[\"set002.udrset.5gc.mnc012.mcc345\"],\"udrInfo\":{\"supiRanges\":
[{\"start\":\"450081000000000\",\"end\":\"450081002000000\"}],\"gpsiRanges\":
[{\"start\":\"13100000000\",\"end\":\"13102000000\"}],\"supportedDataSets\":
[\"POLICY\"]},\"nfServices\":[{\"serviceInstanceId\":\"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\",\"serviceName\":\"nudr-dr\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.15.1.0\",\"expiry\":\"2019
-08-03T18:55:08.871Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\
",\"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedNfTypes\":
[\"CHF\",\"PCF\"],\"priority\":5,\"capacity\":50,\"load\":40,\"recoveryTime\":
\"2018-11-22T08:51:03.222Z\"}],\"groupId\":\"udr1\"},
{\"nfInstanceId\":\"fe7d992b-0541-4c7d-
ab84-555552222222\",\"nfType\":\"UDR\",\"nfStatus\":\"REGISTERED\",\"fqdn\":\"
nf22stub.gi-
dina.svc\",\"priority\":3,\"capacity\":50,\"load\":30,\"locality\":\"1\",\"nfS
etIdList\":[\"set002.udrset.5gc.mnc012.mcc345\"],\"udrInfo\":{\"supiRanges\":
[{\"start\":\"450081000000000\",\"end\":\"450081002000000\"}],\"gpsiRanges\":
[{\"start\":\"13100000000\",\"end\":\"13102000000\"}],\"supportedDataSets\":
[\"POLICY\"]},\"nfServices\":[{\"serviceInstanceId\":\"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\",\"serviceName\":\"nudr-dr\",\"versions\":
[{\"apiVersionInUri\":\"v1\",\"apiFullVersion\":\"1.15.1.0\",\"expiry\":\"2019
-08-03T18:55:08.871Z\"}],\"scheme\":\"http\",\"nfServiceStatus\":\"REGISTERED\
",\"ipEndPoints\":[{\"transport\":\"TCP\",\"port\":8080}],\"allowedNfTypes\":
[\"CHF\",\"PCF\"],\"priority\":3,\"capacity\":50,\"load\":30,\"recoveryTime\":
\"2018-11-22T08:51:03.222Z\"}],\"groupId\":\"udr1\"}],\"nrfSupportedFeatures\"
:\"72\"},
sourceType=NRF}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log
4jLogger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:1
1:51.770+0000"}

Discovery of UDR for the second time:

{"instant":
{"epochSecond":1702448069,"nanoOfSecond":173667948},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Checking if cache applies for a discovery
request (DiscoveryCache feature enabled: true, OC-Force-Rediscovery
requested:
false)","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.173+
0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":173707825},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryRule","message":"Query Parameters validation. IsFullyMatch ->
true, Params from request -> [target-nf-type, requester-nf-type, service-
names, target-nf-set-id], Params from config -> [target-nf-type, requester-nf-
type, service-names, target-nf-set-
id]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.173+000
0"}
{"instant":

Copyright © 2019, 2026, Oracle and/or its affiliates.

{"epochSecond":1702448069,"nanoOfSecond":173763918},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryrul
es.DiscoveryRule","message":"DiscoveryCache is enabled and queryParameters
matched. Proceeding with DiscoveryResponse retrieval from
memory","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger"
,"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.173+
0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":173787036},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.DiscoveryEvaluator","message":"Rule applied:
CacheRule","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.1
73+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":173803555},"thread":"XNIO-1
task-2","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.core.discoveryru
les.CacheRule","message":"Applying Cache Rule, grabbing NRF response from
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.173+0
000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":178149415},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Successful retrieval of
Discovery Response stored in Cache/DB, proceeding with
validation","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog
ger","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.
178+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":178179123},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response retrieved
from Cache/DB isAboutToExpire value : false
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.178+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":178199339},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response retrieved
from Cache/DB is expired value : true
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.178+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":178405635},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.cac
he.GetCacheDiscoveryResponseUseCase","message":"Discovery Response has
expired, updating and retrieving from NRF to
Cache","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.178+0
000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":178450502},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"SearchData :
{\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-

Copyright © 2019, 2026, Oracle and/or its affiliates.

dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-
id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false}","endO
fBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":9
0,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.178+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":178601367},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Entering sendOnDemandNfDiscoverRequest
function","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.1
78+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":179243376},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Send NfDiscover request with searchData:
{\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-
dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-
id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false}","endO
fBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":1
01,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.179+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":179374539},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"sendRequestToNrf nrfRequest : NRFRequest [scheme=http,
rootURI=nf1stub.gi-dina.svc:8080, resourcePath=/nnrf-disc/v1/nf-instances,
method=GET, body=null, headers=[],
searchData={\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-
dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false},
routeCount=0,
requestType=NFDISCOVER]","endOfBatch":false,"loggerFqcn":"org.apache.logging.s
lf4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-1
2-13T06:14:29.179+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":179497176},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,
nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:14:29.179+0000"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

{"instant":
{"epochSecond":1702448069,"nanoOfSecond":179552046},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"Sending request to NRF nf1stub.gi-dina.svc:8080, routeCount=0,
attempt=0","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.
179+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":179577169},"thread":"pool-10-
thread-1","level":"DEBUG","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientA
pi","message":"trigger","endOfBatch":false,"loggerFqcn":"org.apache.logging.sl
f4j.Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12
-13T06:14:29.179+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":179601014},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Returning retryConfig for ALL_REQUESTS NRFRetryConfig
[serviceRequestType=ALL_REQUESTS, primaryNRFRetryCount=0,
nonPrimaryNRFRetryCount=0, alternateNRFRetryCount=-1,
errorReasonsForFailure=[503, 504, 500, SocketTimeoutException,
JsonProcessingException, UnknownHostException, NoRouteToHostException],
gatewayErrorCodes=[503],
requestTimeout=10]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.
Log4jLogger","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T
06:14:29.179+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":197764440},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Request returned response with status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.197+00
00"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":203073867},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"Successful Response code
received","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.2
03+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":203133658},"thread":"pool-10-
thread-1","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.api.NRFClientAp
i","message":"sendOnDemandNfDiscoverRequest with searchData:
{\"targetNfType\":\"UDR\",\"serviceNames\":[\"nudr-
dr\"],\"requesterNfType\":\"PCF\",\"nfInfoParamsPresent\":false,\"serviceInfoP
aramsPresent\":true,\"enableF3\":true,\"enableF5\":false,\"targetNfSetId\":\"s
et001.udrset.5gc.mnc012.mcc345\",\"retentionPeriod\":5000,\"rawQueryParameters
\":\"target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&target-nf-
set-id=set001.udrset.5gc.mnc012.mcc345\",\"forceRediscoveryEnabled\":false}
returned status code :
200","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":101,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.203+00
00"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":203337703},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf

Copyright © 2019, 2026, Oracle and/or its affiliates.

.GetNrfDiscoveryResponseUseCase","message":"Received Discovery Result. Code: 200, Body (SearchResult): {\"validityPeriod\": 100, \"nfInstances\": [{\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555550000000\", \"nfSetIdList\": [\"set001.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\": \"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\": \"nf2stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null, \"ipv6Addresses\": null, \"priority\": 1, \"capacity\": 50, \"load\": 10, \"locality\": \"1\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\": null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\": \"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\", \"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\", \"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]}, \"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null, \"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\": [{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\": \"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null, \"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null, \"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null, \"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null, \"allowedNssais\": null, \"priority\": 1, \"capacity\": 100, \"load\": 50, \"locality\": \"1\", \"recoveryTime\": 1542876663222, \"supportedFeatures\": null}]}, {\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555551111111\", \"nfSetIdList\": [\"set001.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\": \"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\": \"nf21stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null, \"ipv6Addresses\": null, \"priority\": 2, \"capacity\": 50, \"load\": 20, \"locality\": \"2\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\": null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\": \"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\", \"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\", \"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]}, \"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null, \"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\": [{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\": \"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\", \"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null, \"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null, \"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null, \"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null, \"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null, \"allowedNssais\": null, \"priority\": 2, \"capacity\": 50, \"load\": 20, \"recoveryTime\": 1542876663222, \"supportedFeatures\": null}]}, {\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555553333333\", \"nfSetIdList\": [\"set001.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\": \"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\": \"nf11stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null, \"ipv6Addresses\": null, \"priority\": 4, \"capacity\": 50, \"load\": 10, \"locality\": \"1\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\": null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\": \"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\", \"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\",

Copyright © 2019, 2026, Oracle and/or its affiliates.

\"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]},
\"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null,
\"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\":
[{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\":
\"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null,
\"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null,
\"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null,
\"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null,
\"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null,
\"allowedNssais\": null, \"priority\": 4, \"capacity\": 50, \"load\": 10,
\"recoveryTime\": 1542876663222, \"supportedFeatures\": null}]},
{\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555554444444\", \"nfSetIdList\":
[\"set002.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\":
\"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\":
\"nf12stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null,
\"ipv6Addresses\": null, \"priority\": 5, \"capacity\": 50, \"load\": 40,
\"locality\": \"2\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\":
null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\":
\"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\",
\"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\",
\"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]},
\"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null,
\"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\":
[{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\":
\"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null,
\"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null,
\"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null,
\"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null,
\"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null,
\"allowedNssais\": null, \"priority\": 5, \"capacity\": 50, \"load\": 40,
\"recoveryTime\": 1542876663222, \"supportedFeatures\": null}]},
{\"nfInstanceId\": \"fe7d992b-0541-4c7d-ab84-555552222222\", \"nfSetIdList\":
[\"set002.udrset.5gc.mnc012.mcc345\"], \"nfType\": \"UDR\", \"nfStatus\":
\"REGISTERED\", \"plmnList\": null, \"nsiList\": null, \"fqdn\":
\"nf22stub.gi-dina.svc\", \"interPlmnFqdn\": null, \"ipv4Addresses\": null,
\"ipv6Addresses\": null, \"priority\": 3, \"capacity\": 50, \"load\": 30,
\"locality\": \"1\", \"pcfInfo\": null, \"udmInfo\": null, \"ausfInfo\":
null, \"amfInfo\": null, \"smfInfo\": null, \"upfInfo\": null, \"groupId\":
\"udr1\", \"udrInfo\": {\"supiRanges\": [{\"start\": \"450081000000000\",
\"end\": \"450081002000000\"}], \"gpsiRanges\": [{\"start\": \"13100000000\",
\"end\": \"13102000000\"}], \"supportedDataSets\": [\"POLICY\"]},
\"bsfInfo\": null, \"customInfo\": null, \"recoveryTime\": null,
\"nfServices\": [{\"serviceInstanceId\": \"94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\", \"serviceName\": \"nudr-dr\", \"versions\":
[{\"apiVersionInUri\": \"v1\", \"apiFullVersion\": \"1.15.1.0\", \"expiry\":
\"2019-08-03T18:55:08.871+0000\"}], \"scheme\": \"http\",
\"nfServiceStatus\": \"REGISTERED\", \"fqdn\": null, \"interPlmnFqdn\": null,
\"ipEndPoints\": [{\"ipv4Address\": null, \"ipv6Address\": null,
\"transport\": \"TCP\", \"port\": 8080}], \"apiPrefix\": null,
\"defaultNotificationSubscriptions\": null, \"allowedPlmns\": null,
\"allowedNfTypes\": [\"CHF\", \"PCF\"], \"allowedNfDomains\": null,
\"allowedNssais\": null, \"priority\": 3, \"capacity\": 50, \"load\": 30,

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
\"recoveryTime\": 1542876663222, \"supportedFeatures\":
null}]}]}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogg
er","threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.2
03+0000"}
{"instant":
{"epochSecond":1702448069,"nanoOfSecond":203984193},"thread":"XNIO-1
task-2","level":"INFO","loggerName":"com.oracle.cgbu.cnc.nrf.core.usecases.nrf
.GetNrfDiscoveryResponseUseCase","message":"Dynamic discovery cache enabled :
false","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":90,"threadPriority":5,"messageTimestamp":"2023-12-13T06:14:29.203+0
000"}
```


4.58 Handling Race Condition Between Gx and Sy Sessions in two sites

Policy supports handling race condition between Gx and Sy sessions in two sites that result in Sy stale sessions in PDS.

Race condition between Gx and Sy sessions

A sample race condition is when the PGW opens two different sessions (such as data and voice or data and data sessions) with two different PCRF Core instances on site1 and site2, termination request for both the sessions are sent to different sites.

While the session create Diameter Credit-Control-Request (CCR)-I appears to come in a sequence succession, first data and then voice, the terminate request for both voice and data are received at the same time in two different sites, while the device disconnects from the network.

As this is happening at the same time, both sites Site 1 and Site 2 in their local database find that there is another Gx session open. Both sites close their own Gx sessions, but as they both (at this time) see a remaining Gx session at the other site, they keep the Sy session as open.

As the Session Termination Request (Sy-STR) is missing, the session remains active in OCS resulting in stale Sy session.

> **Note**
>
> Currently, Policy only supports minimizing the number of stale sessions, but cannot completely avoid the race condition.
>
> Also, Policy does not support error handling for this feature.

Handling Stale Sy sessions

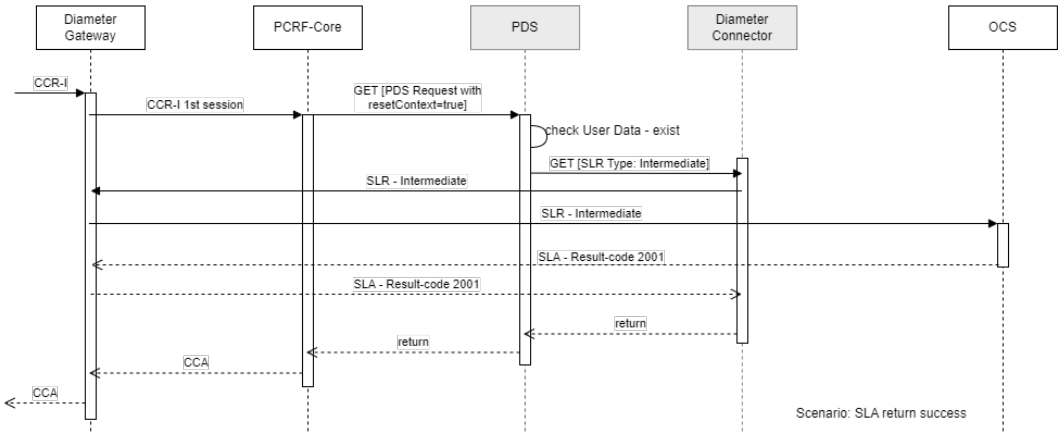
Revalidating the Sy session to ensure that the Sy session is still valid by polling OCS (ResetContext)

1. Upon establishment of the first Gx session for the subscriber, if the Sy data is present on PDS, PDS sends an Sy Spending-Limit-Request (SLR)-Intermediate to OCS requesting all the policy counters.
2. If PDS receives a success response from OCS, it indicates that PDS is in sync with OCS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

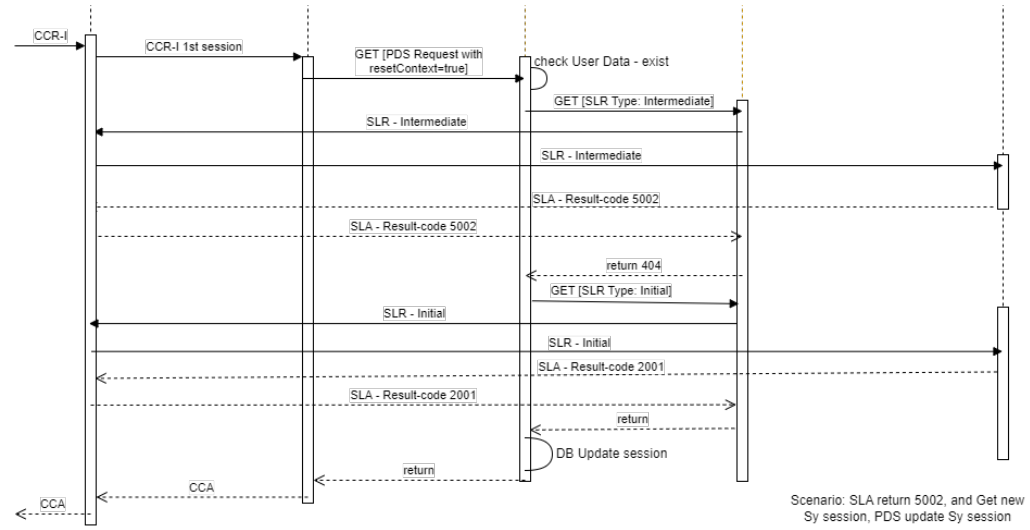
3. If PDS receives UNKNOWN_SESSION_ID error, PDS deletes the old Sy session and creates a new one.

Figure 4-131 SLA Returns Success



1. PCRF Core receives a CCR-I for first session through Diameter Gateway.
2. PCRF Core sends a Get request to PDS with `resetContext` flag set to `true`.
3. PDS searches for the corresponding user data in its database.
4. If the data exists, PDS sends an Sy SLR-Intermediate request to OCS to fetch all the policy counters. PDS sends this request through Diameter Connector routed through Diameter Gateway.
5. OCS responds with Spending Limit Answer (SLA) with success result code 2001. The response is sent from OCS to Diameter Connector routed through Diameter Gateway.
6. Diameter Connectors returns the success response to PDS.
7. PDS updates the details in its database and returns the response to PCRF Core.
8. PCRF Core responds to the CCR-I request for session 1 with Diameter Credit-Control-Request (CCA).

Figure 4-132 SLA Returns 5002, Get New Sy Session, PDS Update Sy Session



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. PCRF Core receives a CCR-I for first session through Diameter Gateway.
2. PCRF Core sends a Get request to PDS with `resetContext` flag set to `true`.
3. PDS searches for the corresponding user data in its database.
4. If the data exists, PDS sends an Sy SLR-Intermediate request to OCS to fetch all the policy counters. PDS sends this request through Diameter Connector routed through Diameter Gateway.
5. OCS responds with Spending Limit Answer (SLA) with success result code 5002 indicating Diameter Unknown Session Id. The response is sent from OCS to Diameter Connector routed through Diameter Gateway.
6. Diameter Connector sends a 404 error to PDS.
7. PDS sends a GET request with SLR Type: Initial to Diameter Connector to get the new Sy session.
8. Diameter Connector forwards the SLR - Initial request to OCS through Diameter Gateway.
9. OCS sends SLA with Result-Code 2001 to Diameter Connector through Diameter Gateway indicating Diameter Success.
10. Diameter Connector returns the success response to PDS.
11. PDS updates its database and returns the response to PCRF Core.
12. PCRF Core responds to the CCR-I request for session 1 with Diameter Credit-Control-Request (CCA).

> **Note**
>
> For any unsuccessful response other than 5002 (404) the existing record will be deleted.

Handling stale Sy sessions by limiting the number of Gx sessions that can be associated with an Sy session for a specific APN

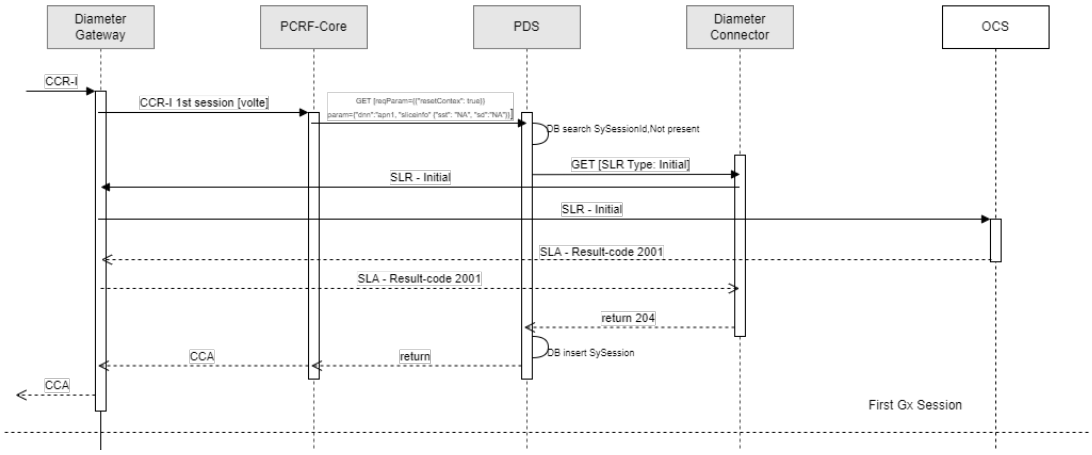
1. PCRF provides **Max Sessions Count** to specify how many Gx sessions can be associated with an Sy session for a specific APN.
2. If **Max Sessions Count** exceeds the limit, PCRF revalidates the Sy session with OCS.

This method protects against cases where Gx CCR-T are not sent by the PGW/received by the PCRF for a specific APN.

Here is an example call flow with **Max Sessions Count**=1. The request for the first Gx session results with a success response, while the second request is revalidated.

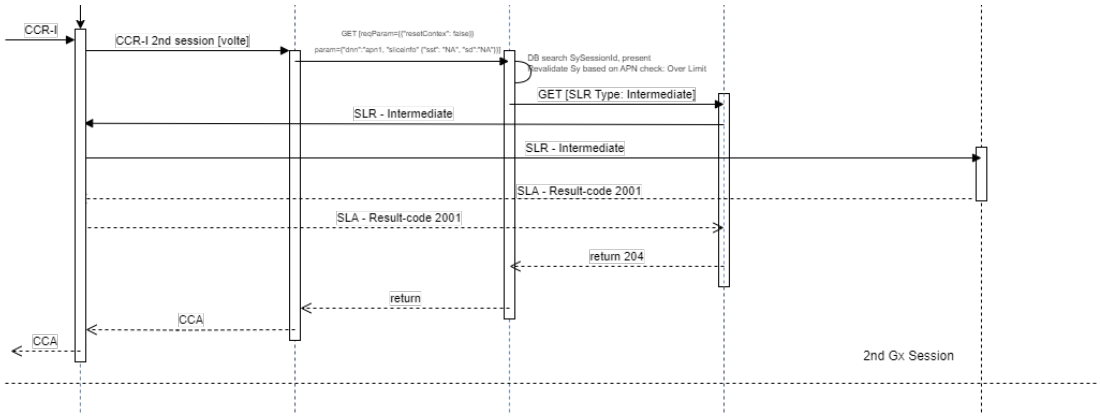
Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-133 First Gx Session



1. PCRF Core receives a CCR-I for first session through Diameter Gateway.
2. PCRF Core sends a Get request to PDS with `resetContext` flag set to `true` along with other parameters such as DNN (with Data Network Name), SST (with Slice or Service Type) and SD (with Slice Differentiator Name).
3. PDS searches for the data in its database.
4. If the data does not exist for the given Sy SessionId, PDS sends an Sy SLR-Intermediate request to OCS to fetch all the policy counters. PDS sends this request through Diameter Connector routed through Diameter Gateway.
5. OCS responds with Spending Limit Answer (SLA) with success result code 2001. The response is sent from OCS to Diameter Connector routed through Diameter Gateway.
6. Diameter Connectors returns the success response to PDS.
7. PDS updates the details in its database and returns the response to PCRF Core.
8. PCRF Core responds to the CCR-I request for session 1 with Diameter Credit-Control-Request (CCA).

Figure 4-134 Second Gx Session

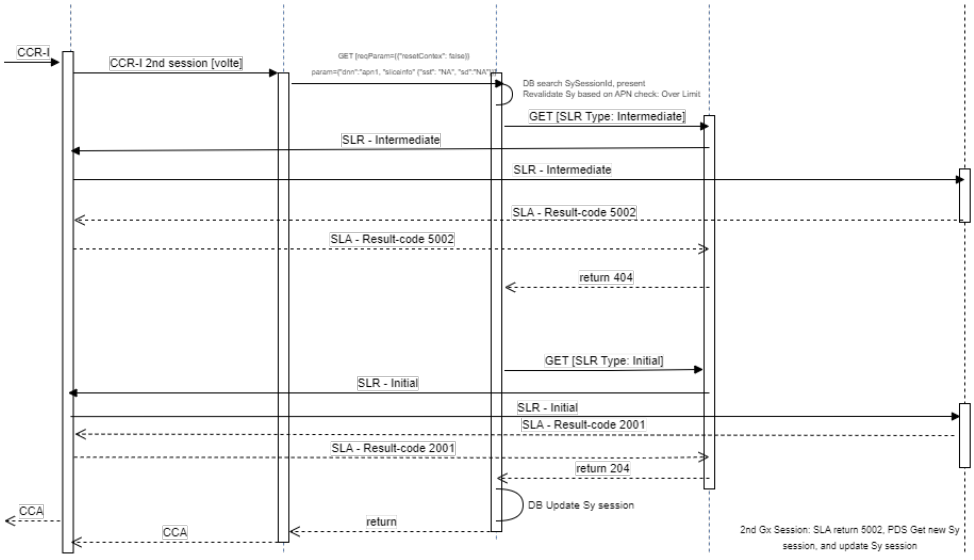


1. PCRF Core receives a CCR-I for second session through Diameter Gateway.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. PCRF Core sends a Get request to PDS with `resetContext` flag set to `false` along with other parameters such as DNN (with Data Network Name), SST (with Slice or Service Type) and SD (with Slice Differentiator Name).
3. PDS searches for the data in its database.
4. If the data exists for the given Sy SessionId, PDS sends an Sy SLR-Intermediate request to OCS to fetch all the policy counters. PDS sends this request through Diameter Connector routed through Diameter Gateway.
5. OCS responds with Spending Limit Answer (SLA) with success result code 2001. The response is sent from OCS to Diameter Connector routed through Diameter Gateway.
6. Diameter Connectors returns 204 no data response to PDS.
7. PDS updates the details in its database and returns the response to PCRF Core.
8. PCRF Core responds to the CCR-I request for session 2 with Diameter Credit-Control-Request (CCA).

Figure 4-135 Second Gx Session: SLA Returns 5002, Get New Sy Session, PDS Update Sy Session



1. PCRF Core receives a CCR-I for second session through Diameter Gateway.
2. PCRF Core sends a Get request to PDS with `resetContext` flag set to `false` along with other parameters such as DNN (with Data Network Name), SST (with Slice or Service Type) and SD (with Slice Differentiator Name).
3. PDS searches for the data in its database.
4. If the data exists for the given Sy SessionId, PDS sends an Sy SLR-Intermediate request to OCS to fetch all the policy counters. PDS sends this request through Diameter Connector routed through Diameter Gateway.
5. OCS responds with Spending Limit Answer (SLA) with success result code 5002. The response is sent from OCS to Diameter Connector routed through Diameter Gateway.
6. Diameter Connectors returns 404 error to PDS.
7. PDS sends a GET request with SLR Type: Initial to Diameter Connector to get the new Sy session.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8. Diameter Connector forwards the SLR - Initial request to OCS through Diameter Gateway.
9. OCS sends SLA with Result-Code 2001 to Diameter Connector through Diameter Gateway indicating Diameter Success.
10. Diameter Connector returns the 204 response to PDS.
11. PDS updates its database and returns the response to PCRF Core.
12. PCRF Core responds to the CCR-I request for session 1 with Diameter Credit-Control-Request (CCA).

Managing Handling Race Condition Between Gx and Sy Sessions over two sites

Enable

To enable the PDS revalidation functionality:

You can enable the PDS revalidation functionality using the CNC Console or REST API for Policy.

- **Enable using CNC Console**:
  To enable revalidation of the Sy stale sessions, set the value of `USER.ocsSpendingLimit.resetContextOnGxCreate` key under **Advanced Settings** in **Settings** page for **PCRF Core** to `true`.

  For more details, see Settings.
- **Enable using REST API**:
  To enable the revalidation functionality, configure the advanced settings keys in the `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcrfcore/settings` REST API.

  For more details, see *Policy REST Specifications* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the revalidation functionality to handle the stale Sy sessions using CNC Console or REST API for Policy.

- **Configure using CNC Console**:
  For revalidating Sy sessions, configure **Enable Fetch and Resubscribe** and **Session Count per DNN/APN List Settings** under **Settings** page for **PDS**.

  For more information, see PDS Settings.
- **Configure using REST API**: Policy provides {apiRoot}/oc-cnpolicy-configuration/v1/services/pds/pdsSettings REST API to configure the PDS revalidation functionality.

Observability

Metrics

The following PDS metrics are used to revalidate the Sy sessions:

- revalidation_request
- revalidation_response

For more details on these metrics, see Policy DS Metrics.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.59 Support for Policy Action to Send the Notify Terminate

PCF provide policy rules to network functions SMF/AMF. It integrates with AMF for Access and Mobility Policy Control and User Equipment (UE) related policies and with SMF for session management policies. To provide updated Policies, PCF initiates an `update` notification request toward SMF/AMF. On receiving SMF/AMF response, the PCF either decides to update the Policies or sends request to terminate the policy association.

The PCF policy engine evaluates configured Policies that are triggered by events received from SMF, AMF, CHF, and UDR. The PCF receives policy triggers during the following cases:

- UDR notifies the PCF about a Policy subscription changes
- CHF notifies PCF of Policy counter status changes
- AMF notifies PCF for AM and UE Policy updates
- SMF notifies PCF for session and PCC updates

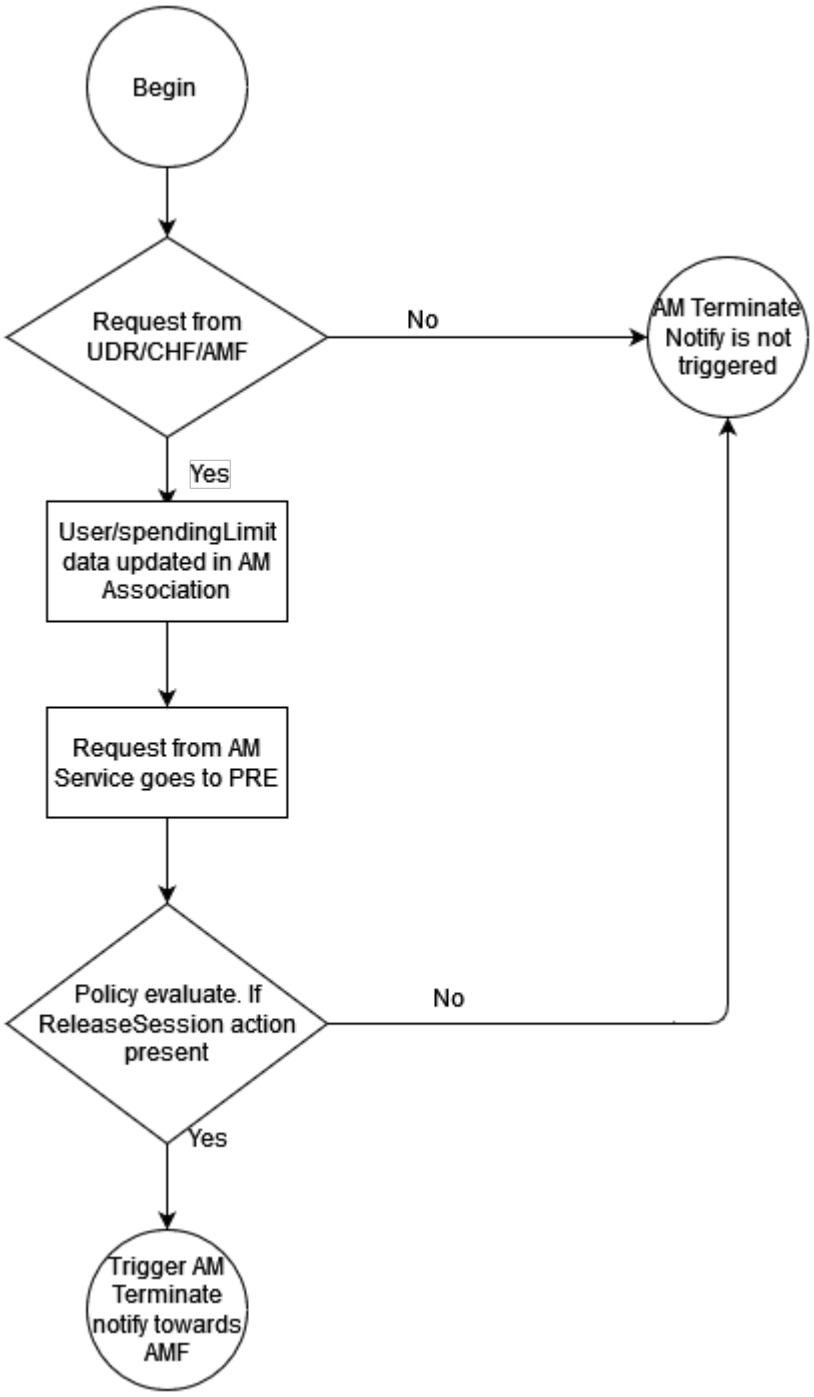
On receiving policy trigger information from PCF, the Policy Runtime Engine (PRE) evaluates the Policies and makes the requested policy decision. Based on the policy decision that is made after evaluating the Policies, the PCF may decide to send an `update` or `terminate` request toward AMF/SMF. PCF applies these policy decision by interacting with AMF/SMF.

PCF Triggering AM UpdateNotify Terminate

The following flowchart illustrates the flow of PCF triggering AM terminateNotify request toward AMF for termination of the Policy association.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-136 PCF Triggering AM UpdateNotify Terminate



1: Start

2: If notifications requests are coming from either UDR or CHF or AMF, go to step 3, if not, go to step 7.

3: User/Spending limit data updated in AM association.

4: Request from AM service goes to PRE.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5: PRE evaluates the policies. If ReleaseSession action (with or without cause) is present go to step 6, if not, go to step 7.

6: Trigger AM terminate notify toward AMF.

7: AM Terminate notify is not triggered.

Policy blockly `Release Session with cause` holds the PCF cause for termination of AM policy association. The cause for termination is configurable by the user and the default cause value is `UE_SUBSCRIPTION`.

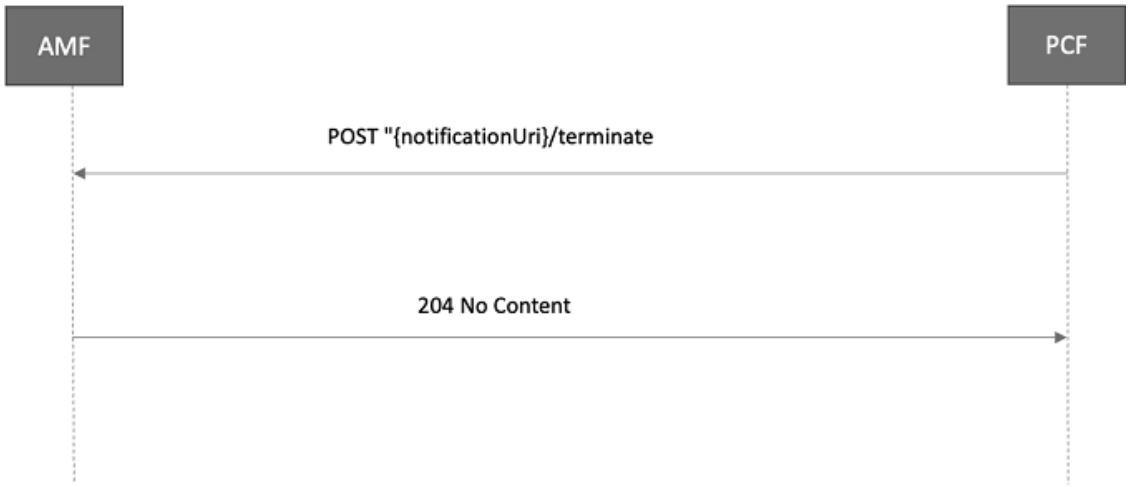
PCF request for Termination of AM/SM/UE Policy Association

If PCF requests the termination of AM/SM Policy association, it sends an HTTP Post request with "{notificationUri}/terminate" as URI (where the notification URI was previously supplied by the AMF). The request body of termination notification includes:

- the policy association Id encoded as "polAssoId" attribute; and
- the cause as to why PCF requests the termination of the policy association encoded as "cause" attribute

The following figure, illustrates the request for termination of the policy association from PCF.

Figure 4-137 Deletion of Policy Association



Termination of AM/UE Policy Association

For termination of AM/UE Policy associations, PCF invokes `Npcf_AMPolicyControl_UpdateNotify` and `Npcf_UEPolicyControl_UpdateNotify` respective service operation towards AMF.

PCF termination notification request toward SMF is made with `TerminationNotification` data type.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-118 Definition of Type TerminationNotification

Attribute Name	Data Type	Description
resourceUri	Uri	The resource URI of each AM/UE policy association related to the notification.
cause	PolicyAssociationReleaseCause	The cause for PCF requesting for AM Policy association termination.

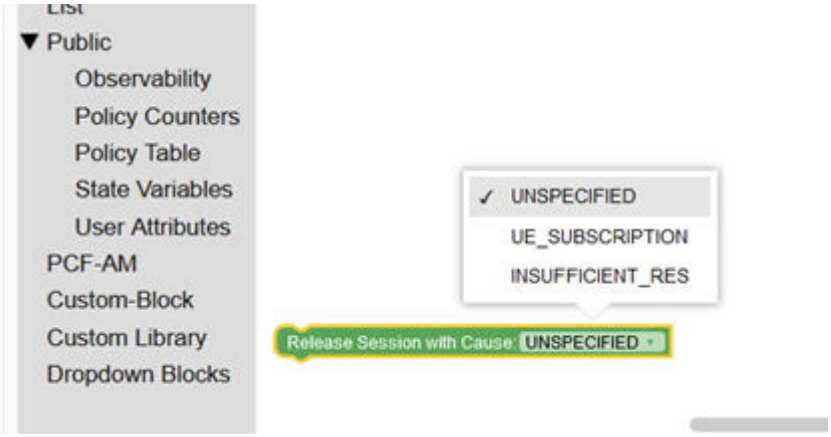
The user can set the `cause` in `TerminationNotification`. The default cause is set to "UE_SUBSCRIPTION". The user shall be able to customize the termination causes as per need to other 3gpp defined causes. The enumeration `PolicyAssociationReleaseCause` represents the cause for PCF requests for AM policy association termination.

Table 4-119 Enumeration PolicyAssociationReleaseCause

Enumeration value	Description
UNSPECIFIED	This value is used for unspecified reasons.
UE_SUBSCRIPTION	This value indicates that the policy association needs to be terminated because the subscription of UE has changed such as removal of a subscription.
INSUFFICIENT_RES	This value indicates that the server is overloaded and needs to terminate the policy association.

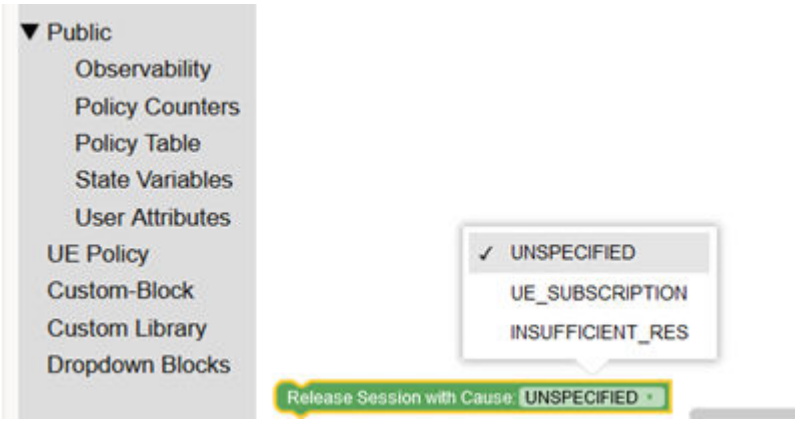
Policy blockly `Release Session with cause` holds the PCF cause for termination of AM/UE policy association.

Figure 4-138 Release Session with cause for PCF-AM



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-139 Release Session with cause for PCF-UE



Termination of SM Policy Association

For termination of SM Policy association, PCF invokes `Npcf_SMPolicyControl_UpdateNotify` service operation to the SMF. PCF termination notification request toward SMF is made with `TerminationNotification` data type.

Table 4-120 Definition of Type TerminationNotification

Attribute Name	Data Type	Description
resourceUri	Uri	The resource URI of each SM policy association related to the notification.
cause	SMPolicyAssociationReleaseCause	The cause for PCF requesting for SM Policy association termination.

The user can set the `cause` in `TerminationNotification`. The default cause is set to "UNSPECIFIED". The user shall be able to customize the termination causes as per need to other 3gpp defined causes. The enumeration `SmPolicyAssociationReleaseCause` represents the cause for PCF requests for SM policy association termination.

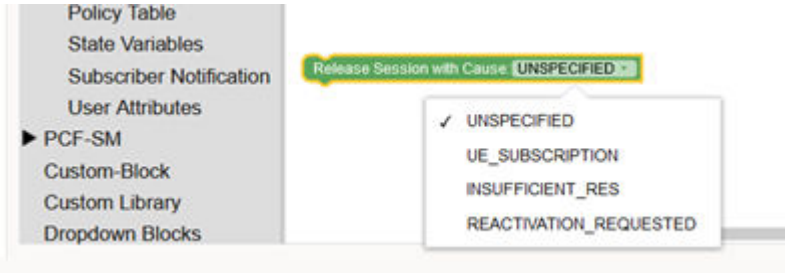
Table 4-121 Enumeration SMPolicyAssociationReleaseCause

Enumeration value	Description
UNSPECIFIED	This value is used for unspecified reasons.
UE_SUBSCRIPTION	This value indicates that the policy association needs to be terminated because the subscription of UE has changed such as removal of a subscription.
INSUFFICIENT_RES	This value indicates that the server is overloaded and needs to terminate the policy association.
REACTIVATION_REQUESTED	This value indicates that policy association needs to be terminated, since PCF is not able to maintain the existing PDU session and requests for PDU session reactivation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Policy blockly `Release Session with cause` holds the PCF cause for termination of SM policy association.

Figure 4-140 Release Session with cause for PCF-SM



AMF/SMF on receiving post request for termination from PCF, either sends a *204 No Content* response for the successful processing or an appropriate failure response. After successful processing of PCF request, AMF/SMF invokes `Npcf_AMPolicyControl_Delete` or `Npcf_SMPolicyControl_Delete` or `Npcf_UEPolicyControl_Delete` service operation to terminate the policy associations respectively. Upon receiving the delete request, PCF deletes the Policy association and its associated sessions in UDR. It sends either a `204 No Content` response indicating the success of the deletion or an appropriate failure response.

When PCF does not receive the delete request from AMF/SMF, the Policy association is not deleted in Policy and thus its associated resources with the external NFs are not deleted.

When PCF receives an error response from AMF/SMF, it handles the error as defined in "Error Handling" feature.

PCF Decision Not to Terminate AM/SM Policy Association

In case of the PCF decision, to keep the Policy associations and not to terminate it, the default policy is used and data is not fetched from the UDR.

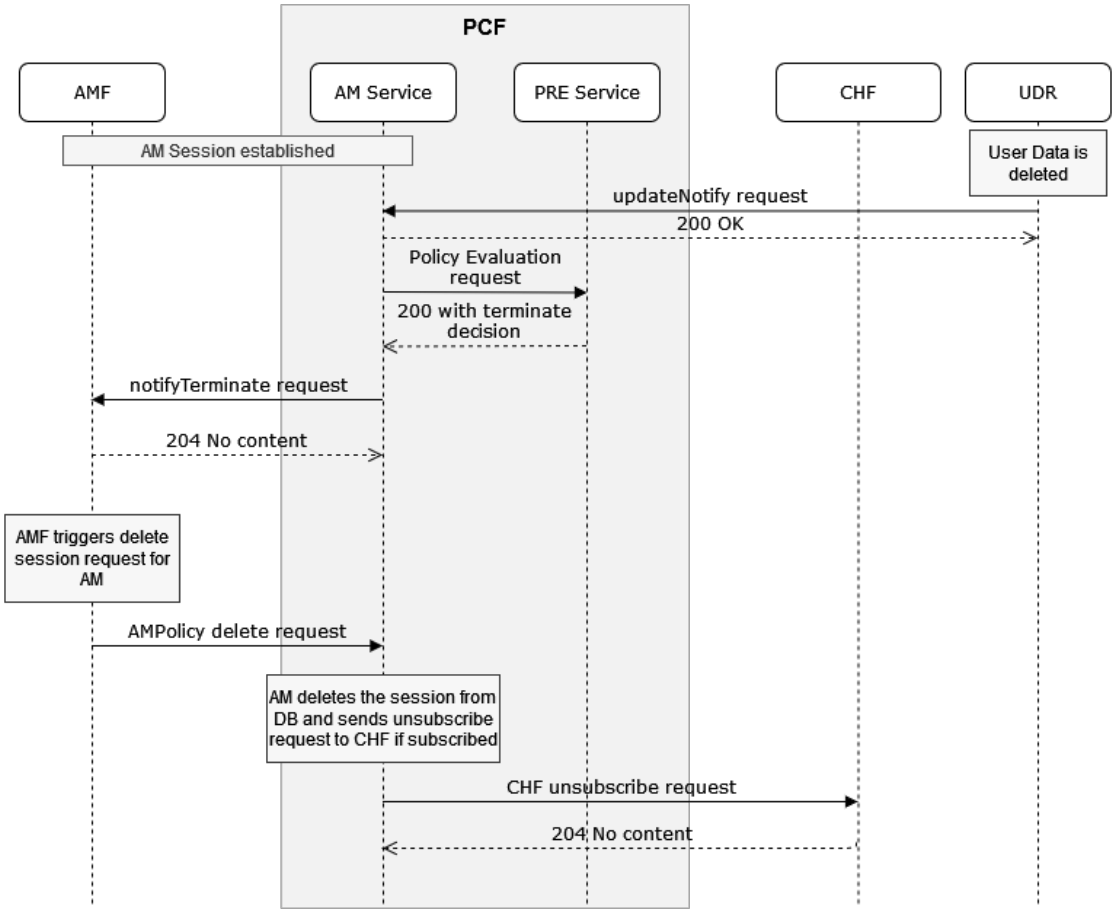
If PCF decides to keep the Policy associations, the default policy is used and not the data from UDR. PCF invokes UpdateNotify service operation toward AMF/SMF to update the AM/SM Policy control information. PCF updates the local database as ampolicydata/smpolicydata. Since the data from UDR is not present for the subscriber, UDR should not have any subscription for this subscriber.

When PCF receives update of a Policy association from the AMF/SMF for this session, it performs UDR query request based on configurations from `am-data/sm-data`. If UDR sends an error response due to USER_NOT_FOUND, then PCF takes actions according to "Error handling feature for AM/SM Policy" feature.

Copyright © 2019, 2026, Oracle and/or its affiliates.

AM Session Termination Call Flows

Figure 4-141 Call Flow for AM Terminate for UDR updateNotify with delResources

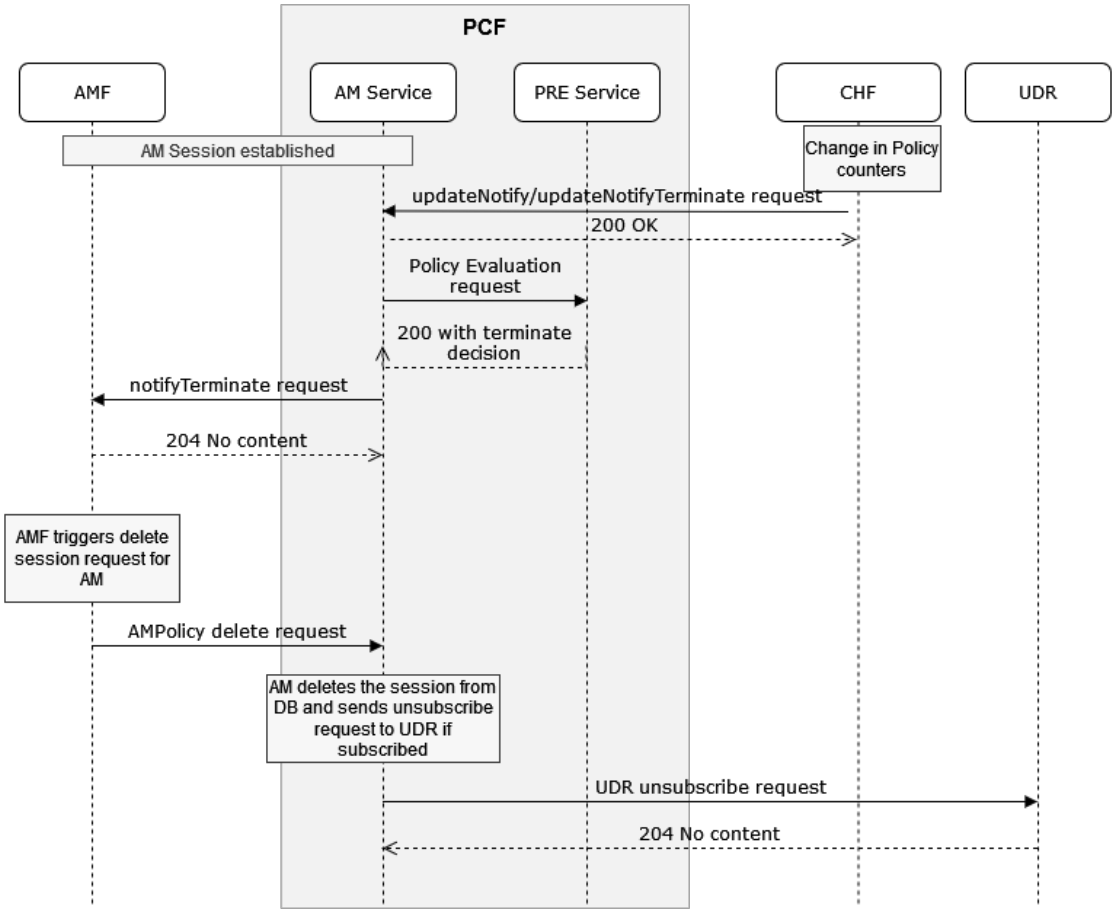


1. AMF sends a UE session established message to AM Policy service.
2. At UDR when a user data is deleted then, UDR sends an *updateNotify* request to AM service. The updateNotify request includes the `delResources` property containing the path of the resource that was deleted.
3. AM Policy service forwards the `200 OK` message to UDR.
4. AM Policy service sends a *Policy evaluation* request to PRE to evaluate the details.
5. Depending on the evaluation, PRE includes `Release Session` action in its response to AM Policy service.
6. In case of termination, AM Policy service sends a *terminateNotify* request to AMF.
7. AMF sends a `204 No Content` response to AM Policy service indicating that the request was successful.
8. AMF triggers a delete session requests and sends *AM Policy delete* request to AM Policy service.
9. AM Policy service deletes the AMPolicyAssociation from the database and sends an *unsubscribe* request to CHF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

10. CHF removes the subscription and responds to AM Policy service with `204 No Content` message.

Figure 4-142 Call Flow for AM Terminate for CHF updateNotify or TerminateNotify



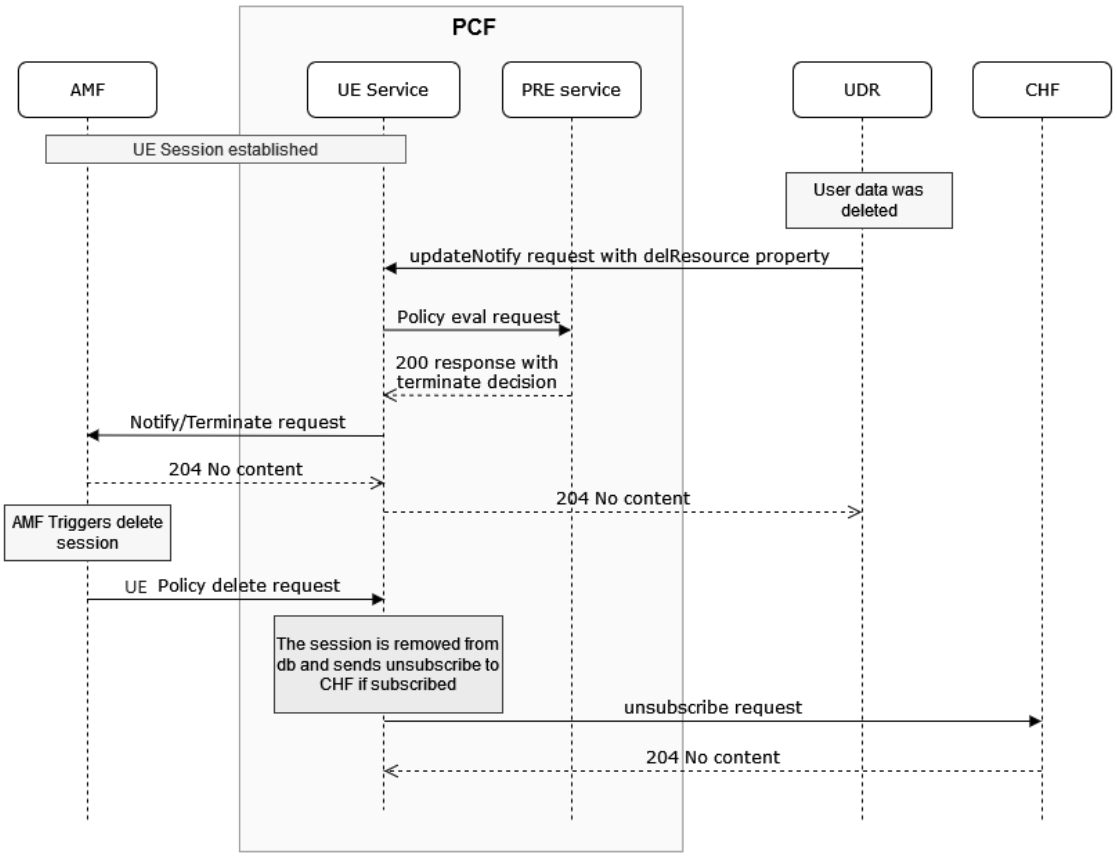
1. AMF sends an AM session established message to AM Policy service.
2. When the Policy Counters for a subscriber is deleted in CHF, it sends an *updateNotify* or*terminateNotify* request to AM Policy service.
3. AM Policy service forwards the `200 OK` message to CHF.
4. AM Policy service sends a *Policy evaluation* request to PRE to evaluate the details.
5. Depending on the evaluation, PRE includes *Release Session* action in its response to AM Policy service.
6. AM Policy service sends a *notifyTerminate* request to AMF.
7. AMF sends a `204 No Content` response to AM Policy service indicating that the request was successful.
8. AMF triggers a delete session request and sends a AMPolicy delete request to AM Policy service.
9. AM Policy service deletes the AMPolicyAssociation from the database and sends an *unsubscribe* request to UDR, if subscribed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

10. UDR removes the subscription and responds to AM Policy service with `204 No Content` message.

UE Session Termination Call Flows

Figure 4-143 Call Flow for UE Terminate for UDR updateNotify with delResources

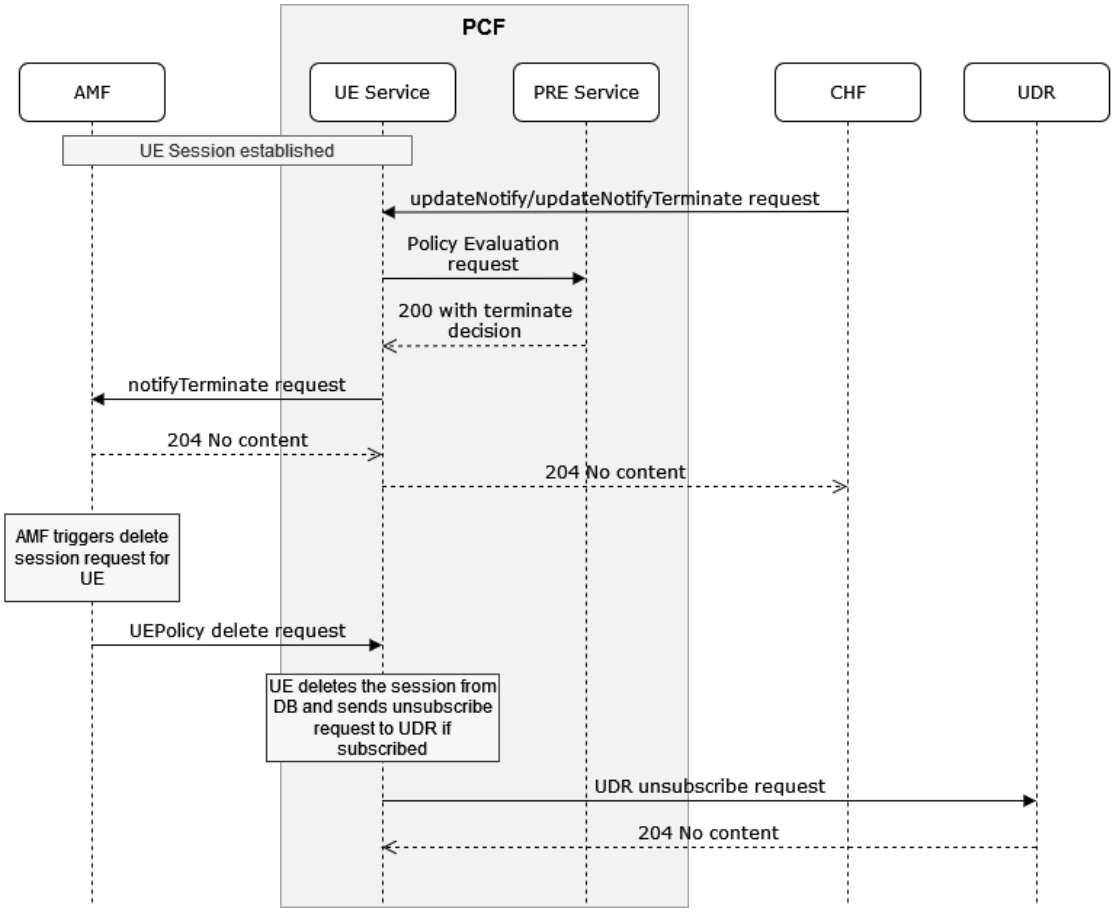


1. AMF sends a UE Session established message to UE Policy service.
2. When a user data is deleted in UDR, UDR sends an *updateNotify* request to UE Policy service. The updateNotify request includes the *delResources* property, containing the path of the resource that was deleted.
3. UE Policy service sends a *Policy evaluation* request to PRE to evaluate the details.
4. Depending on the evaluation, PRE includes *Release Session* action in its response to UE Policy service.
5. UE Policy service sends a *notifyTerminate* request to AMF.
6. AMF sends a `204 No Content` response to UE Policy service indicating that the request was successful.
7. UE Policy service forwards the `204 No Content` message to UDR.
8. AMF triggers a delete session request and sends a UEPolicy delete request to UE Policy service.
9. UE Policy service deletes the UEPolicyAssociation from the database and sends an `unsubscribe` request to CHF, if subscribed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

10. CHF removes the subscription and responds to UE Policy service with `204 No Content` message.

Figure 4-144 Call Flow for UE Terminate for CHF updateNotify or updateNotifyTerminate



1. AMF sends a UE Session established message to UE Policy service.
2. When the Policy Counters for a subscriber is deleted in CHF, CHF sends an *updateNotify* or *updateNotify Terminate* request to UE Policy service.
3. UE Policy service sends a *Policy evaluation* request to PRE to evaluate the details.
4. Depending on the evaluation, PRE includes *Release Session* action in its response to UE Policy service.
5. UE Policy service sends a *notifyTerminate* request to AMF.
6. AMF sends a `204 No Content` response to UE Policy service indicating that the request was successful.
7. UE Policy service forwards the `204 No Content` message to CHF.
8. AMF triggers a delete session request and sends a UEPolicy delete request to UE Policy service.
9. UE Policy service deletes the UEPolicyAssociation from the database and sends an *unsubscribe* request to UDR, if subscribed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

10. UDR removes the subscription and responds to UE Policy service with `204 No Content` message.

Support for ReleaseToReactivate in SM Service

The `ReleaseToReactivate` feature indicates that the PCF can request the SMF for reactivation of a PDU session based on an SM Policy association release cause, `REACTIVATION_REQUESTED`. This happens with supported features negotiation through the "suppFeat" field. When a session is terminated with `REACTIVATION_REQUESTED` termination cause, then SMF informs UE and AMF, that the UE should reactivate its PDU session.

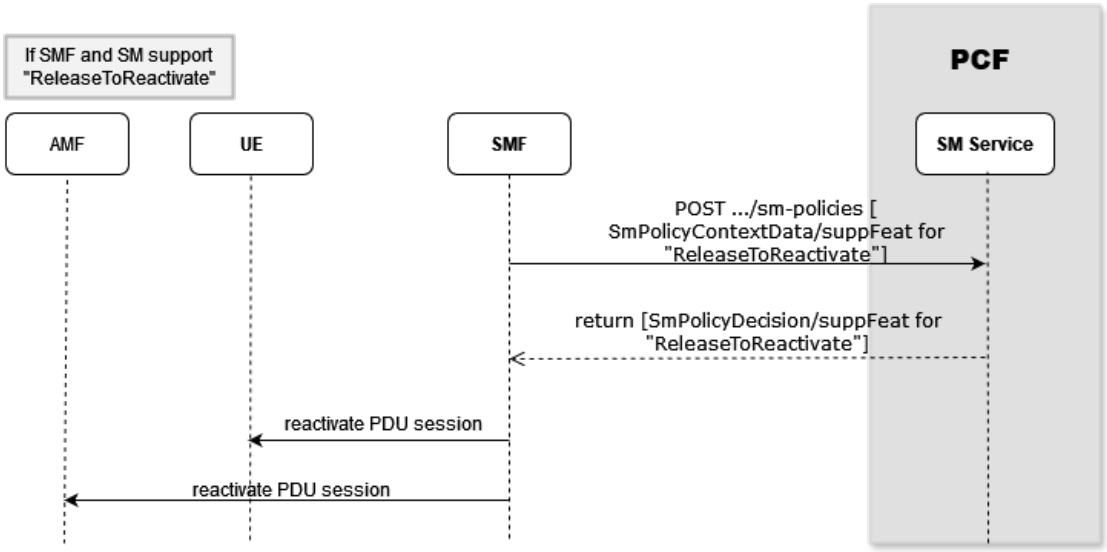
To support this feature in PCF during a SM session creation, a configuration **ReleaseToReactivate** value is added to the **Override Supported Features** field in PCF-SM service in CNC Console. This configuration can be either enabled or disabled by the operator by considering the following requirements:

- If SMF supports `ReleaseToReactivate` feature, and `ReleaseToReactivate` configuration is selected in **Override Supported Features** in SM configurations, then SM service returns this update as part of `suppFeat` attribute in its response message towards SMF.
- If SMF supports `ReleaseToReactivate` feature, and `ReleaseToReactivate` configuration is not selected in **Override Supported Features** in SM configurations, then SM service returns `suppFeat` attribute without any updates in its response message towards SMF. Also, it does not send "REACTIVATION_REQUESTED" in `SmPolicyAssociationReleaseCause`, instead it sends "UNSPECIFIED" as the termination cause.
- If SMF does not support `ReleaseToReactivate` feature, and `ReleaseToReactivate` configuration is selected in **Override Supported Features** in SM Configuration, then SM service returns `suppFeat` attribute without any updates in its response message towards SMF.

Policy blockly `Release Session with cause` holds the PCF causes for termination of SM/AM/UE policy association.

This flow represents the feature negotiation for `ReleaseToReactivate` **only** if both SMF and SM support for the feature `ReleaseToReactivate`.

Figure 4-145 SM and SMF support for ReleaseToReactivate Feature

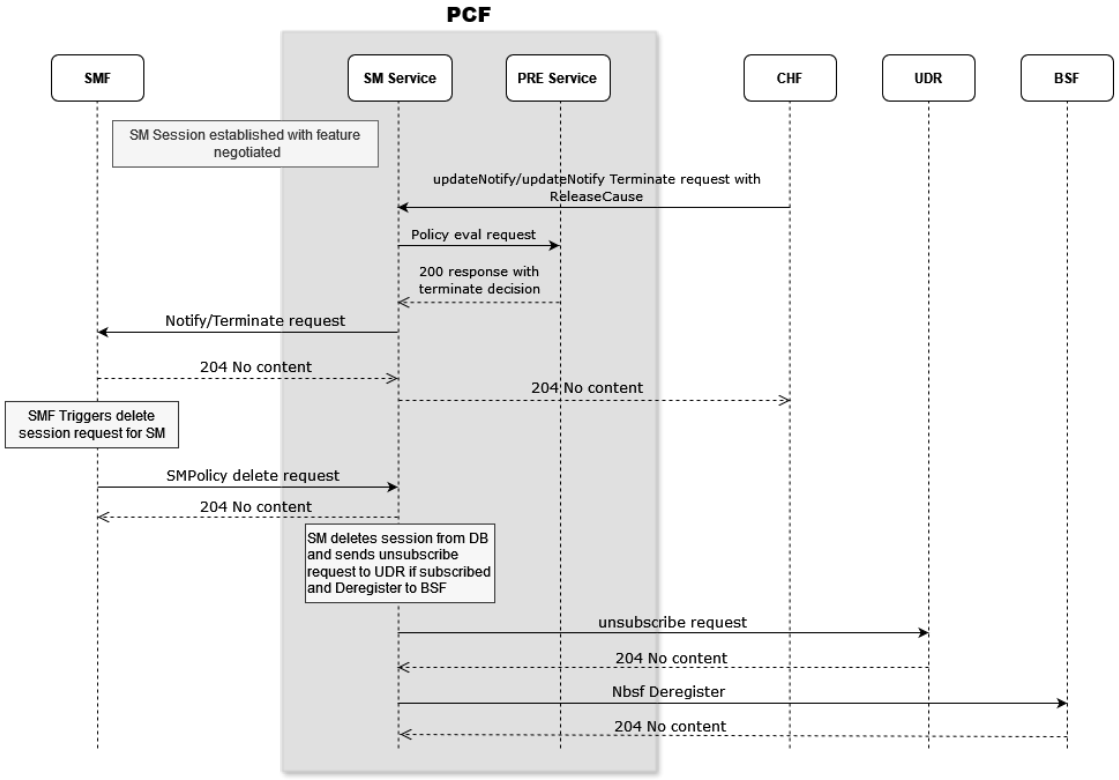


Copyright © 2019, 2026, Oracle and/or its affiliates.

1. SMF sends POST request for SM Policy creation toward SM service.
2. SM service responds with SmPolicyDecision along with `ReleaseToReactivate` added to the list of supported features.
3. SMF initiates a reactivate PDU session request toward UE service.
4. SMF initiates a reactivate PDU session request toward AMF.

ReleaseToReactivate in SM Service Call Flows

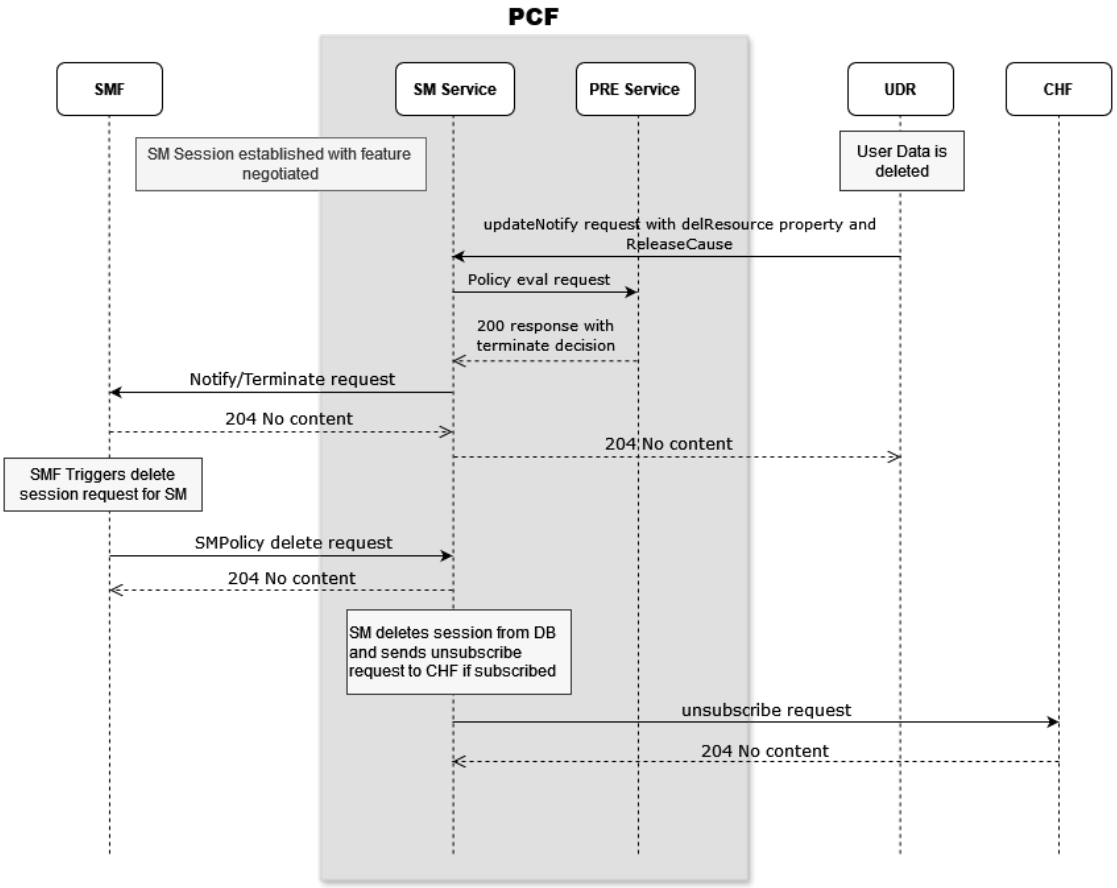
Figure 4-146 SM Terminate for CHF updateNotify or updateNotifyTerminate:



1. CHF triggers updateNotify/UpdateNotify Termination request toward along with release cause to SM service.
2. On receiving the CHF request, SM service sends request to PRE for Policy evaluation.
3. PRE responds to SM service with `200 OK` SM session termination.
4. SM service sends Notify/Terminate request to SMF.
5. SMF responds with `204 No Content` message to SM service.
6. SM service sends `204 No Content` message to CHF.
7. SMF triggers SMPolicy delete request to SM service.
8. SM service sends `204 No Content` toward SMF.
9. SM service initiates SM delete session from the database, sends `unsubscribe` request to UDR and `deregister` request to BSF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-147 SM Terminate for UDR updateNotify with (or without) delResources:



1. On user data deletion at UDR, it triggers an updateNotify request toward along with delResource and release cause properties to SM service.
2. On receiving the UDR request, SM service sends request to PRE for Policy evaluation.
3. PRE responds to SM service with `200 OK` SM session termination.
4. SM service sends Notify/Terminate request to SMF.
5. SMF responds with `204 No Content` message to SM service.
6. SM service sends `204 No Content` toward UDR.
7. SMF triggers session delete request to SM service.
8. SM service sends `204 No Content` toward SMF.
9. SM service initiates SM delete session from the database, sends `unsubscribe` request to CHF.

Managing Support of Policy Action to Send the Notify Terminate

This section explains the procedure to enable and configure the feature.

Enable

This forms Policy applications core feature functionality. You do not need to enable or disable this feature.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Configure Using Blockly

New blocks `UDR delResources contains`, `Release Session with cause` and `Release session` without cause are introduced in AM/UE/SM services. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Observability

Metrics:

The following AM service metrics are used for this feature:

- `ocpm_egress_request_total`
- `ocpm_egress_response_total`

The following SM and UE metrics are used for this feature:

- `http_in_conn_request`
- `http_out_conn_response`

UDR service uses `ocpm_userservice_inbound_count_total` metric for this feature.

Maintain
If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support for more information on how to raise a service request.

4.60 Support for UDR Discovery Using Group ID

PCF interfaces with UDR to receive subscriber related data for the UE (uePolicySet) AM (amPolicyData) and SM (smPolicyData) information. On PCF receiving requests from AMF or SMF, it performs UDR discovery using NRF.

With user equipment existing in millions, thousands of UDR discovery requests are sent to NRF. Many UE's subscription data will be associated to a single UDR in form of UDR groups. PCF, by performing UDR discovery using the UDR group id reduces the number of discovery requests to NRF for the same UDR. The **UDR Group ID** refers to one or more UDR instances managing a specific set of SUPI's.

SMF/AMF makes following PCF `GET` and initial `POST` requests with UDR group id `oc-policy-udr-group-id-list` to receive Policy associations associated with the user or SUPI.

- AMF for AM Policy association, POST ../npcf-am-policy-control/v./policies/ (PolicyAssociationRequest)
- AMF for UE Policy association,POST ../npcf-ue-policy-control/v./policies/ (PolicyAssociationRequest)
- SMF for SM Policy association,POST ../npcf-smpolicycontrol/v./sm-policies (SmPolicyContextData)

Core services (SM/ AM/UE) accepts requests containing `oc-policy-udr-group-id-list` header from NF consumer and forwards it to PDS. PDS forwards it to UDR connector. Based on the discovery parameters and the NF communication profile configurations received in the

Copyright © 2019, 2026, Oracle and/or its affiliates.

request, UDR connector selects query parameters and forms a request toward NRF client for UDR discovery or rediscovery.

For example the request toward NRF:

```
GET ../nnrf-disc/v./nf-instances?target-nf-type=UDR&requester-nf-type=PCF&group-id-list=<Value from XXX-UDR-Group-Id>&data-set=POLICY
```

Based on query parameters for UDR discovery or rediscovery and configurations, NRF client supports either non-SUPI or SUPI based caching.

Customizing Header Name Containing udr-group-id-list

PCF receives the service requests with header that contain UDR Group Id associated with the user/SUPI. Default custom header name is `oc-policy-udr-group-id-list`. The user shall be able to customize the header name as per their requirements at `routesConfig` in PCF custom_values.yaml file. Adding header for the following routes:

- SMF for SM Policy association - `sm_create_session_route`
- AMF for UE Policy association - `ue_create_session_route`
- AMF for AM Policy association - `am_create_session_route`

An example of default header structure in the custom_values.yaml file:

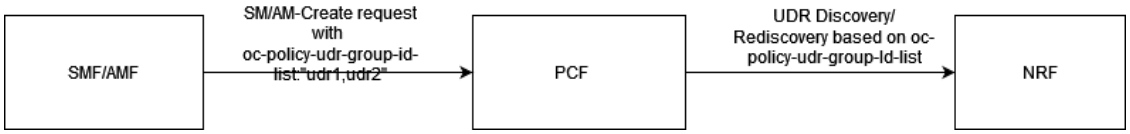
```
routesConfig:
    - id: sm_create_session_route
      uri: http://{{ .Release.Name }}-occnp-pcf-sm:
{{ .Values.global.servicePorts.pcfSmServiceHttp }}
      path: /npcf-smpolicycontrol/*/sm-policies
      order: 1
      method: POST
      readBodyForLog: true
      filters:
        subLog: true,CREATE,SM
        customReqHeaderEntryFilter:
          headers:
            - methods:
              - POST
              headersList:
                - headerName: 3gpp-Sbi-Message-Priority
                  defaultVal: 24
                  source: incomingReq
                  sourceHeader: 3gpp-Sbi-Message-Priority
                  override: false
                - headerName: oc-policy-udr-group-id-list
                  source: incomingReq
                  sourceHeader: oc-policy-udr-group-id-list
                  override: false
```

UDR Discovery in Model B and Model C Communications

SMF/AMF sends SM/AM Policy association requests with `oc-policy-udr-group-id-list` to PCF. And then PCF performs UDR discovery/rediscovery based on `oc-policy-udr-group-id-list` request header to NRF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-148 UDR Discovery with oc-policy-udr-group-id-list Header to NRF



During the GET and initial POST requests, PCF along with existing query parameters, `target-nf-set-id, data-set, preferred-locality, dnn, snssais, guami` for a NF communication profile, now will also have the following parameters for UDR discovery.

- group-id-list
- supi

The following table shows the query parameters (supi, group-id-list) that go from UDR connector to NRF Client for UDR discovery.

Table 4-122 Query Parameters

Query Parameters Selected to Sent from UDR Connector to NRF Client	Discovery Parameters Received by UDR Connector from PDS	Query Parameters Sent to NRF Client for UDR Discovery
group-id-list	group-id-list, supi	group-id-list
group-id-list	supi	supi
supi	group-id-list, supi	supi
supi	supi	supi
supi and group-id-list	group-id-list, supi	group-id-list, supi
supi and group-id-list	supi	supi
NF Communication Profile is not configured	supi	supi
NF Communication Profile is not configured	Group-Id-List, SUPI	SUPI

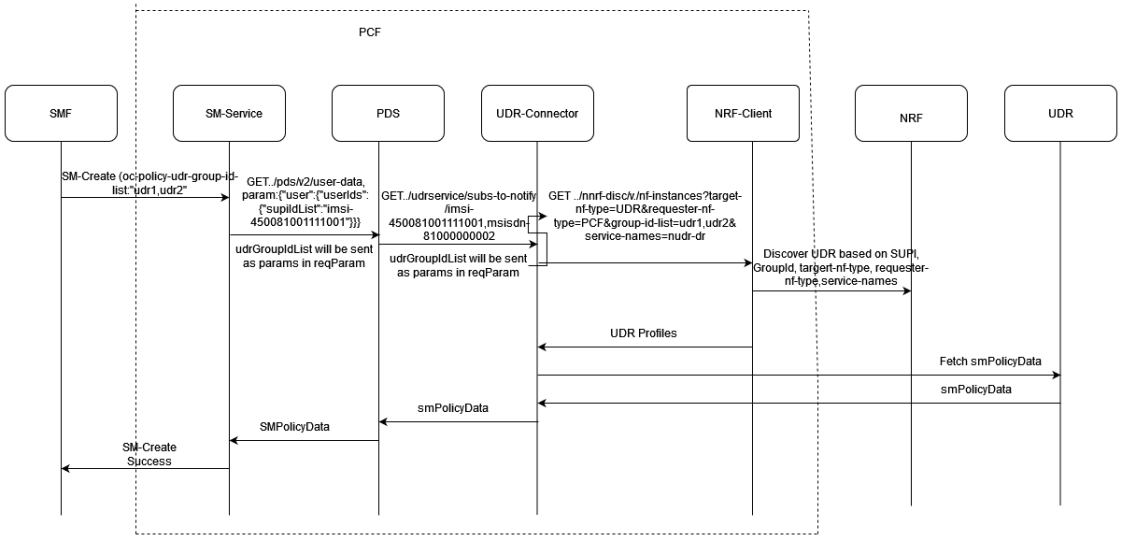
Note

- UE Policy uses the UDR selected for the UE during AM Policy association. When UDR_RELATED_RESOURCE for `amPolicyData` and `UEPolicySet` are enabled, PCF does not perform UDR discovery again during UE Policy association for the UE for which AM Policy association is already established
- UE Policy gets NFProfiles again from NRF if the same UDR that sent amPolicyData during AM Policy association is giving error and when the UDR_RELATED_RESOURCE for `amPolicyData` and `UEPolicySet` are enabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flows

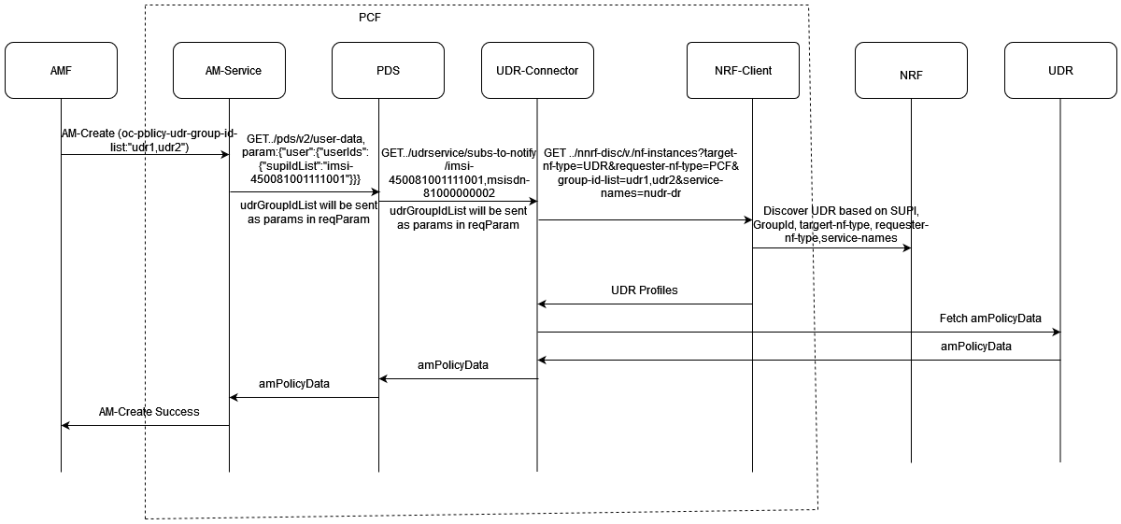
Figure 4-149 SMF sends SM Policy Association Request with oc-policy-udr-group-id



1. SMF sends SM Create request with `oc-policy-udr-group-id-list:"udr1,udr2"` to SM service.
2. SM service sends a GET request along with udr group id lists as request parameters to PDS.
3. PDS sends a GET request along with udr group id lists as request parameters to UDR Connector
4. UDR Connector sends a GET request along with udr group id lists as request parameters to NRF Client.
5. NRF Client sends UDR discovery request along with SUPI, GroupId, target-nf-type,requester-nf-type, and service-name request parameters to UDR via NRF.
6. NRF Client sends the UDR profiles to UDR Connector.
7. UDR responds back with `smpolicydata` to UDR Connector.
8. UDR connector forwards the response to SM service via PDS.
9. With successful creation of SM Policy association, SM service responds back to SMF with SM Create success.

Copyright © 2019, 2026, Oracle and/or its affiliates.

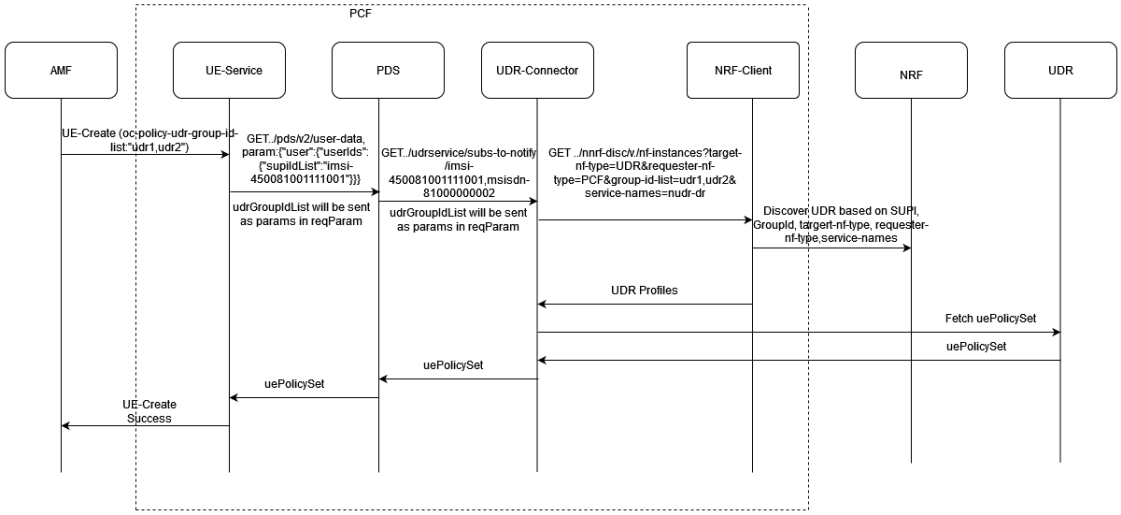
Figure 4-150 AMF sends AM Policy Association Request with oc-policy-udr-group-id



1. AMF sends AM Create request with `oc-policy-udr-group-id-list:"udr1,udr2"` to AM service.
2. AM service sends a GET request along with udr group id lists as request parameters to PDS.
3. PDS sends a GET request along with udr group id lists as request parameters to UDR Connector
4. UDR Connector sends a GET request along with udr group id lists as request parameters to NRF Client.
5. NRF Client sends UDR discovery request along with SUPI, GroupId, target-nf-type,requester-nf-type, and service-name request parameters to UDR via NRF.
6. NRF Client sends the UDR profiles to UDR Connector.
7. UDR responds back with `ampolicydata` to UDR Connector.
8. UDR connector forwards the response to AM service via PDS.
9. With successful creation of AM Policy association, AM service responds back to AMF with AM Create success.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-151 AMF sends UE Policy Association Request with oc-policy-udr-group-id



1. AMF sends UE Create request with `oc-policy-udr-group-id-list:"udr1,udr2"` to UE service.
2. UE service sends a GET request along with udr group id lists as request parameters to PDS.
3. PDS sends a GET request along with udr group id lists as request parameters to UDR Connector
4. UDR Connector sends a GET request along with udr group id lists as request parameters to NRF Client.
5. NRF Client sends UDR discovery request along with SUPI, GroupId, target-nf-type,requester-nf-type, and service-name request parameters to UDR via NRF.
6. NRF Client sends the UDR profiles to UDR Connector.
7. UDR responds back with `uePolicySet` to UDR Connector.
8. UDR connector forwards the response to UE service via PDS.
9. With successful creation of UE Policy association, UE service responds back to AMF with UE Create success.

Policy Features Impacted due to UDR Discovery using Group-id-list

Impact on Non-SUPI based Caching: When non-SUPI based caching is enabled, UDR discovery/rediscovery is done using `group-id-list`. NRF client cache's the discovered NF profiles along with query parameters. The following table shows if NRF Client cache's the NF profile or not when non-SUPI based caching is enabled:

Table 4-123 NRF Client Caching

NRF Agent Query Parameters Configurations	Query Parameter for UDR Discovery at NRF Client	Caching at NRF Client
group-id-list	group-id-list	True
group-id-list	group-id-list, supi	False
group-id-list	supi	False

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-123 (Cont.) NRF Client Caching

NRF Agent Query Parameters Configurations	Query Parameter for UDR Discovery at NRF Client	Caching at NRF Client
Other than group-id-list	group-id-list	False (as query parameters sent to NRF client and configured should be same)

For more information about non-supi based caching, see the Support for Non-SUPI based On-Demand Discovery Caching of NF Profiles section.

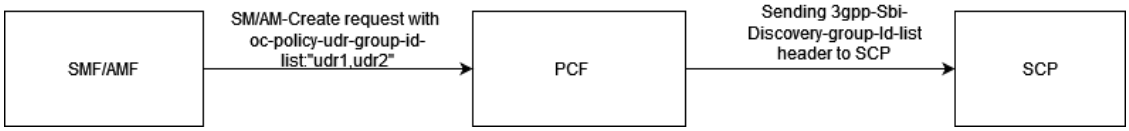
Impact on SUPI-based Caching: When SUPI-based caching is enabled, UDR discovery/rediscovery is done using `SUPI` and `(SUPI,Group-Id-List)`. Enabling the non-SUPI-based caching will not be applicable as the query parameter contains SUPI. For more information, see Support for SUPI based NRF Discovery Optimization and Response Caching from UDR section.

Impact on Session Retry: For `GET` and initial `POST` requests, this feature is not impacted and the UDR discovery happens based on query parameters as configured in NF communication profile. For more information, see Support for Session Retry and Alternate Route Service section.

UDR Discovery in Model D Communication

SMF/AMF sends SM/AM Policy association requests with `oc-policy-udr-group-id-list` to PCF. And then PCF performs UDR discovery using `3gpp-Sbi-Discovery-group-Id-list` request header to SCP.

Figure 4-152 UDR Discovery with 3gpp-Sbi-Discovery-group-Id-list Header to SCP



UDR connector compares NF communication profile configurations, NF discovery settings, Model D configurations and discovery parameters received from PDS and accordingly sends the request header to SCP based on the following table:

Table 4-124 Query Parameters

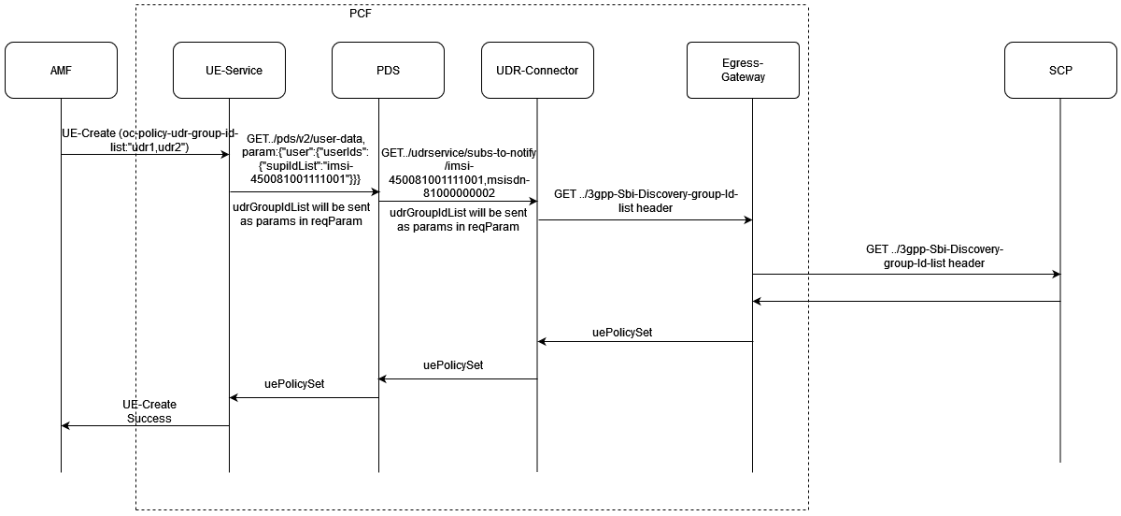
NF Communication Configurations	Values Received by UDR Connector	Header Sent to SCP
udr-group-id-list	udr-group-id-list, supi	3gpp-Sbi-Discovery-group-Id-list
udr-group-id-list	supi	No Header
supi	udr-group-id-list, supi	3gpp-Sbi-Discovery-SUPI
supi	supi	3gpp-Sbi-Discovery-SUPI
udr-group-id-list, supi	udr-group-id-list, supi	3gpp-Sbi-Discovery-group-Id-list, 3gpp-Sbi-Discovery-SUPI
udr-group-Id-list, supi	supi	3gpp-Sbi-Discovery-SUPI

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> If configured, the UDR discovery happens for subsequent sessions for the same subscriber based on udr-group-id-list.

Call Flow

Figure 4-153 Model D, AMF sends UE Policy Association Request with oc-policy-udr-group-id-list



1. AMF sends UE Create request with `oc-policy-udr-group-id-list:"udr1,udr2"` to UE service.
2. UE service sends a GET request along with udr group id lists as request parameters to PDS.
3. PDS sends a GET request along with udr group id lists as request parameters to UDR Connector
4. UDR Connector sends a GET request along with 3gpp-Sbi-Discovery-group-Id-list header to Egress Gateway.
5. Egress Gateways sends a GET request along with 3gpp-Sbi-Discovery-group-Id-list header to SCP.
6. SCP responds with `uePolicySet` to Egress Gateway.
7. Egress Gateways forwards `uePolicySet` to UDR Connector.
8. UDR connector forwards the response to UE service via PDS.
9. With successful creation of UE Policy association, UE service responds back to AMF with UE Create success.

Managing Supports UDR Discovery using Group ID

Enable

This forms Policy applications core feature functionality. You do not need to enable or disable this feature.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Helm

You can customize the custom headers using `headerName` and `sourceHeader` routing parameters for SM/UE/AM service in `custom_values.yaml` file. For more information about routing configurations, see the "Custom Header Name for UDR Group Id" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Configure Using CNC Console

The initial discovery parameters for Model B and C Communication profiles now supports the following parameters:

- `target-nf-set-id`
- `supi`
- `group-id-list`

Model D Communication profile supports the following parameters:

- `target-nf-set-id`
- `supi`
- `data-set`
- `preferred-locality`
- `dnn`
- `snssais`
- `guami`
- `group-id-list`

For more information about these discovery parameters, see the NF Communication Profiles section in the **Common Data** group, under **Service** settings in CNC Console.

The on demand discovery of caching in NRF client supports a new query parameter `group-id-list`. For more information, see the NRF Agent section under **Service** settings in CNC Console.

Maintain
If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support for more information on how to raise a service request.

4.61 Network Policies

Network Policies are an application-centric construct that allows you to specify how a pod communicates with various network entities. It creates pod-level rules to control communication between the cluster's pods and services, and to determine which pods and services can access one another inside a cluster.

Previously, the pods under Policy deployment could be contacted by any other pods in the Kubernetes cluster without any restrictions. Now, Network Policies provide namespace-level isolation, which allows secured communications to and from Policy with rules defined in

Copyright © 2019, 2026, Oracle and/or its affiliates.

respective Network Policies. The Network Policies enforce access restrictions for all the applicable data flows except communication from Kubernetes node to pod for invoking container probe. For example, PCF internal microservices cannot be contacted directly by any other pods.

The key purpose of implementing Network Policies is to support principle of zero trust, the concept that no service or network can be trusted, including in house services and networks.

The following table lists the different access policies to be used by Policy traffic flows.

> **Note**
>
> This list is not exhaustive but tries to represent all the data flows supported by Policy traffic flows.

Microservice	Direction	Client/Server	Port	Access Policy
Configuration Svc	Egress	• Database • K8s API server for K8s secret	3306, K8s API Server Port	K8s Network Policies
Configuration Svc	Egress	• Jaeger Agent	6831	K8s Network Policies
Configuration Svc	Ingress	• Console • Egress Gateway for configuration • Ingress Gateway for configuration • Perf-info for configuration • App-info for configuration • ATS • ARS • NrfClient	8081	K8s Network Policies
Configuration Svc	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Ingress Gateway	Egress	• Jaeger Agent	6831	K8s Network Policies
Ingress Gateway	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
Ingress Gateway	Egress	• Coherence	8000, 7	K8s Network Policies
Ingress Gateway	Ingress	• Perf Info	8000	K8s Network Policies
Ingress Gateway	Ingress	• SBI Peer	80, 443	3GPP-defined Access Policies
Ingress Gateway	Ingress	• Coherence	7, 8000, 8095, 8096	K8s Network Policies

Copyright © 2019, 2026, Oracle and/or its affiliates.

Microservice	Direction	Client/Server	Port	Access Policy
Ingress Gateway	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Egress Gateway	Egress	• Jaeger Agent	6831	No Access Policy due to SBI Egress*
Egress Gateway	Egress	• Database • K8s API Server for K8s Secret	3306	No Access Policy due to SBI Egress*
Egress Gateway	Egress	• Coherence	7, 8000	No Access Policy due to SBI Egress*
Egress Gateway	Egress	• SBI Peer	Decided at run-time	3GPP-defined Access Policies
Egress Gateway	Egress	• ARS	ARS Port	K8s Network Policies
Egress Gateway	Ingress	• Egress Gateway for coherence	7, 8000	K8s Network Policies
Egress Gateway	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Egress Gateway	Ingress	• Coherence	7, 8000	K8s Network Policies
Audit	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Audit	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
App Info	Ingress	• Registration • Subscription • Auditor	8000	K8s Network Policies
App Info	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
App Info	Egress	• DB monitoring port	8080	K8s Network Policies
diam-gateway	Egress	• Jaeger Agent	6831	K8s Network Policies
diam-gateway	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
diam-gateway	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
diam-gateway	Ingress	• Peer	3868	K8s Network Policies

Copyright © 2019, 2026, Oracle and/or its affiliates.

Microservice	Direction	Client/Server	Port	Access Policy
Query-Svc	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Query-Svc	Egress	• Jaeger Agent	6831	K8s Network Policies
User svc	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
User svc	Ingress	• Monitoring	8000, 9443	K8s Network Policies
User svc	Egress	• Jaeger	6831	K8s Network Policies
Policy DS	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Policy DS	Ingress	• Monitoring	8000, 9443	K8s Network Policies
Policy DS	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
Policy DS	Egress	• Jaeger	6831	K8s Network Policies
Notifier	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Notifier	Egress	• Jaeger	6831	K8s Network Policies
Notifier	Egress	• Signaling	8080	K8s Network Policies
Nwdaf-agent	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Nwdaf-agent	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
Nwdaf-agent	Egress	• Jaeger	6831	K8s Network Policies
Bulwark	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Bulwark	Egress	• Signaling	8080	K8s Network Policies
Bulwark	Egress	• Jaeger	6831	K8s Network Policies
Performance	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies

Copyright © 2019, 2026, Oracle and/or its affiliates.

Microservice	Direction	Client/Server	Port	Access Policy
Performance	Egress	• Signaling	8080	K8s Network Policies
alternate route svc	Ingress	• Coherence	7, 8000, 8095, 8096	K8s Network Policies
alternate route svc	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
soap-connector	Egress	• Signaling	8000, 8443	K8s Network Policies
soap-connector	Egress	• Jaeger Agent	6831	K8s Network Policies
soap-connector	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
soap-connector	Ingress	• Monitoring	9000	K8s Network Policies
usage-mon	Egress	• Jaeger Agent	6831	K8s Network Policies
usage-mon	Egress	• Database • K8s API Server for K8s Secret	3306	K8s Network Policies
usage-mon	Egress	• Signaling	8000	K8s Network Policies
usage-mon	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
ldap-gateway	Egress	• Jaeger Agent	6831	K8s Network Policies
ldap-gateway	Egress	• Signaling	8000, 8443	K8s Network Policies
ldap-gateway	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
diam-connector	Egress	• Signaling	8000	K8s Network Policies
diam-connector	Ingress	• Diameter	3868	K8s Network Policies
diam-connector	Ingress	• Monitoring	9000	K8s Network Policies
diam-connector	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Biding	Egress	• Signaling	8000, 9443	K8s Network Policies
Biding	Egress	• Jaeger Agent	6831	K8s Network Policies

Copyright © 2019, 2026, Oracle and/or its affiliates.

Microservice	Direction	Client/Server	Port	Access Policy
Biding	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
Biding	Ingress	• Monitoring	9000	K8s Network Policies
Biding	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
pcrf-core	Egress	• Signaling	8000, 9443	K8s Network Policies
pcrf-core	Egress	• Jaeger Agent	6831	K8s Network Policies
pcrf-core	Ingress	• Diameter	3868	K8s Network Policies
pcrf-core	Ingress	• Monitoring	9000	K8s Network Policies
pcrf-core	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
SM Service	Egress	• Jaeger Agent	6831	K8s Network Policies
SM Service	Egress	• Signaling	8000, 9443	K8s Network Policies
SM Service	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
SM Service	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
SM Service	Ingress	• Monitoring	9000	K8s Network Policies
AM Service	Egress	• Jaeger Agent	6831	K8s Network Policies
AM Service	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
AM Service	Egress	• Signaling	8000, 9443	K8s Network Policies
AM Service	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
AM Service	Ingress	• Monitoring	9000	K8s Network Policies
UE Service	Egress	• Jaeger Agent	6831	K8s Network Policies

Copyright © 2019, 2026, Oracle and/or its affiliates.

Microservice	Direction	Client/Server	Port	Access Policy
UE Service	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
UE Service	Egress	• Signaling	8000, 9443	K8s Network Policies
UE Service	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
UE Service	Ingress	• Monitoring	9000	K8s Network Policies
PRE	Egress	• Jaeger Agent	6831	K8s Network Policies
PRE	Egress	• Signaling	8000	K8s Network Policies
PRE	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
PRE	Ingress	• Monitoring	9000	K8s Network Policies
nrf-client	Egress	• Jaeger Agent	6831	K8s Network Policies
nrf-client	Egress	• Performance • Platform	8000	
nrf-client	Egress	• Cache Service	8095, 8096	
nrf-client	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
nrf-client	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies

As an assumption when deploying Policy, the following labels are set by default:

Table 4-125 Default Labels

Pod	Label
<name_of_the_pod>	np **Note**: This label is only used as long as NRF pods do not use the label app.kubernetes.io/part-of with occnp value.
<name_of_each_service>	app.kubernetes.io/name:

`np` is custom global label that must be added as follows:

1. Open `occnp-custom-values.yaml` file.
2. Add the label under `customExtention-allResources-labels` section.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For example:

```
customExtension:
   # The `factoryLabelTemplates` and `factoryAnnotationTemplates` can
   # accept templates rather than plain text.
   factoryLabelTemplates: {}
   factoryAnnotationTemplates: {}
   allResources:
     labels: {
       "np": "cnpolicy"
     }
```

3. Run the following Helm upgrade command.

```
helm upgrade <helm_name> <build_file.tgz> -f <custom_values.yaml> --
namespace
    <namespace>
```

When the upgrade is complete, the new tag must be observed on all pods.

PCF Security Policies:

- **deny-ingress-all**: To block all ingress traffic of pods present in a PCF deployment.
- **allow-ingress-network-sbi**: To allow traffic on the Ingress Gateway Pods on container ports 8000 and 9443 to allow sbi traffic.
- **allow-ingress-diameter-traffic**: To allow Ingress traffic for diameter gateway, diameter connector, and PCRF Core on port 3868.
- **allow-ingress-local-prometheus**: To allow Ingress traffic for all services on port 9000.
- **allow-ingress-local-policy-flow**: To allow Ingress traffic between pods inside PCF.
- **allow-ingress-network-gui**: To allow ingress traffic on port 8000 for CM Service to access CNC Console.
- **deny-egress-all**: To block all egress traffic for all the pods.
- **allow-egress-network-all-gws**: To allow Egress traffic on all ports for these pods [occnp-egress-gateway, diam-gateway, ldap-gateway, occnp-alternate-route].
- **allow-egress-network-pre**: To allow Egress traffic on all ports for PRE (only use this when PER is enabled).
- **allow-egress-local-database**: To allow Egress traffic on ports 3306 & 8080 for connection with database.
- **allow-egress-local-k8sapi**: To allow Egress traffic on port 6443.
- **allow-egress-local-jaeger**: To allow Egress traffic on port 6831.
- **allow-egress-local-dns**: To allow Egress traffic on port 53.
- **allow-egress-local-flow**: To allow Egress traffic between pods inside PCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> The default Network Policies to be applied for Policy are the recommended even though they are not very granular but they keep operational overhead to the minimum and still achieve access control security.

Managing Network Policies

Enable

To use this feature, Network Policies need to be applied to the namespace wherein Policy is applied.

Configure

You can configure this feature using Helm. For information about configuring network policy for Policy deployment, see *Configuring Network Policy* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Observe

There are no specific metrics and alerts required for the Network Policies feature.

4.62 Support for SUPI based NRF Discovery Optimization and Response Caching from UDR

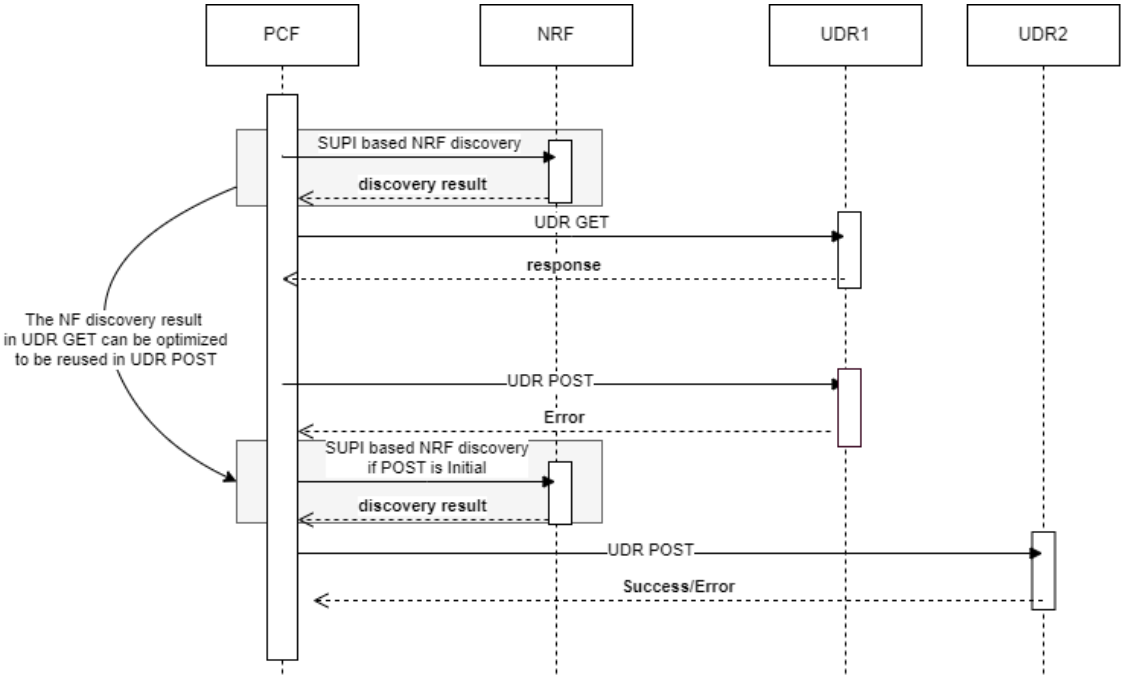
This feature helps in optimizing SUPI based NRF discoveries between the query and subscription (GET and POST) of the policy data request towards UDR.

PCF discovers the NF Profiles from NRF along with the query parameters used in discovery request, which are discovered on demand based on SUPI. SUPI based NRF discovery result for UDR GET request is cached till the POST request is completed. The on demand discovery based on SUPI is currently supported only for UDR discovery. The cache for the discovered UDR profiles expires even if the UDR POST result is success or fail.

The following diagram shows the SUPI based NRF discovery result for UDR GET request is cached till the POST request is completed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-154 UDR GET Discovery Result Reused in UDR POST



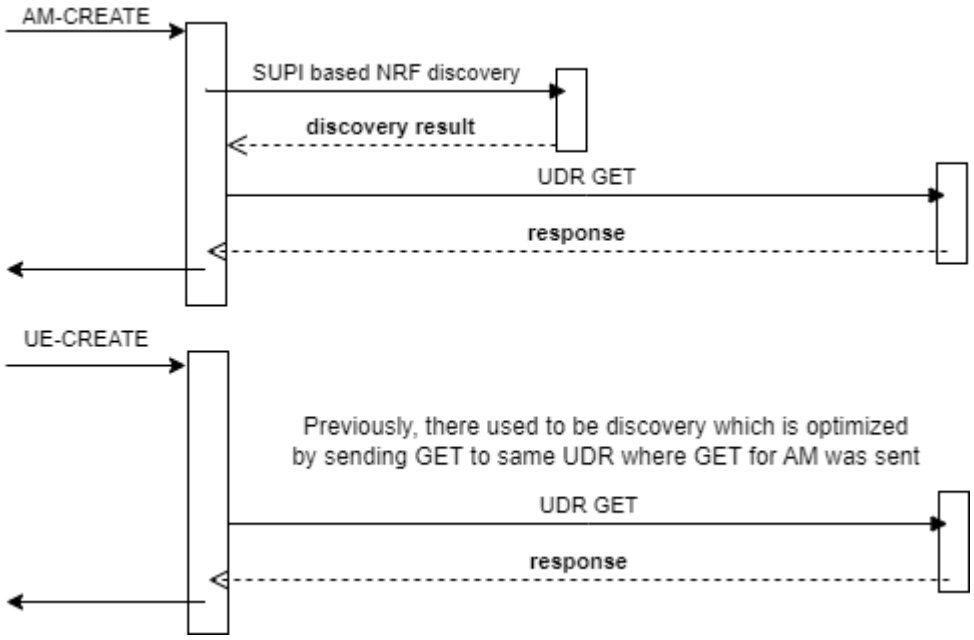
1. PCF sends SUPI based NRF discovery request to NRF.
2. NRF discovers the NF profile using SUPI.
3. PCF sends UDR GET request to UDR1.
4. UDR1 sends response message to PCF.
5. PCF sends UDR POST request to UDR1.
6. UDR 1 responds with an error.
7. PCF does SUPI based NRF discovery if the POST is initial.
8. NRF provides the corresponding discovery result.
9. PCF sends UDR POST to UDR2.
10. UDR2 responds with success or error. If it is successful, cache data is cleared. If it fails and there are no further retry attempts, then POST fails and cache data is cleared.

Instead of doing discovery for amPolicyData and uePolicySet separately, the UDR information used in fetching amPolicyData can be reused in fetching uePolicySet and vice versa. PCF can rediscover the NF profiles for UDR based on the query parameter SUPI, from NRF during POST, if POST fails and uses the discovered profiles from the cache that was cached during GET.

The following diagram shows the reuse of UDR profile for amPolicyData GET in uePolicySet GET.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-155 Reuse of UDR profile for amPolicyData GET in uePolicySet GET



1. For AM-Create request, PCF sends SUPI based NRF discovery request to NRF.
2. NRF discovers the NF profile using SUPI.
3. PCF sends UDR GET request to UDR1.
4. UDR1 sends response message to PCF.
5. For UE-Create request, PCF sends the GET to same UDR where GET for AM was sent.
6. UDR1 sends corresponding response message to PCF.

Managing the Feature

This section explains the procedure to enable and configure the feature.

Enable and Configure

By default, this feature is disabled. You can enable using CNC Console by configuring the following advanced settings:

- Set value of the following keys under the Advanced Settings section on the PDS Settings page:
  - UDR_FETCH_RELATED_RESOURCE
  - UPDATE_SSV_DATASOURCE_INFO_ON_CHANGE

  For information about how to configure for in CNC Console, see PDS Settings.
- Set value of the following keys under the Advanced Settings section on the PCF User Connector page:
  - UDR_NF_PROFILE_COOKIE_ENABLED
  - UDR_NF_PROFILE_COOKIE_COMPRESS
  - UDR_NF_PROFILE_COOKIE_LIMIT
  - UDR_GET_USE_RELATED_RESOURCE

Copyright © 2019, 2026, Oracle and/or its affiliates.

For information about how to configure for in CNC Console, see PCF User Connector.

Observe

The following metrics have been added for this feature:

- Policy DS Metrics
  - occnp_nf_cookie_forwarded_total
  - occnp_nf_cookie_received_total

  For more information, see Policy DS Metrics.
- User Service Metrics
  - occnp_udr_nf_cookie_enabled_total
  - occnp_udr_use_related_resource

  For more information, see User Service Metrics .

4.63 RAA Error Code Handling

RAA error code handling helps in error handling at SM and PA services. The operator should be able to take corrective actions on the receipt of error response from Diameter Connector for initiated update-notify or RAR message.

The operator can configure the corrective action on the error handling configuration page for PA service. Based on this configuration, the PA service receives the error response from Diameter Connector. The Diameter Connector forwards the received diameter error result code in the error header of the response.

Following are the actions that PA service can use:

- Terminate the transaction: To terminate the transaction or call.

  > **Note**
  >
  > If error handling configuration is not done, the default behavior is to terminate the transaction.

- Cleanup session: To delete the corresponding Rx session locally. The PA service initiates the delete request internally that causes the corresponding PCC rule to be removed by SM service by sending Update_Notify request to SMF and also send dependentContextBinding delete request. In this case, no more ASR or STR messages get exchanged.

  > **Note**
  >
  > In case of 5002 DIAMETER_UNKNOWN_SESSION_ID, the default behavior is to cleanup the session. The 'Terminate the transaction' action should be configured only in case of an explicit requirement.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> There is no retry action of update notify http request (RAR) by error handling library at SM/PA service and all the attempts for retry for RAR must be performed as part of diameter session retry at Diameter Gateway.

Managing RAA Error Code Handling

This section explains the procedure to enable and configure the feature.

Enable

To enable RAA error handling, set the value of SYSTEM.PA_ERROR_HANDLER_ENABLED key to true in the Advanced Settings of PA service. For more information, see PCF Policy Authorization.

Configure

Once the service is enabled, you can configure the RAA error handling functionality under **Error Handling** on CNC Console for Policy. For information about how to configure for in CNC Console, see Error Handling.

Observe

The following metrics have been added in PCF Session Management service for this feature:

- error_handler_exec_total
- error_handler_in_total
- error_handler_out_total

For more information, see SM Service Metrics.

4.64 IPv6 Support in Converged Policy Mode

CNC Policy and its microservices can be deployed in a K8s Kubernetes environment that supports the IPv6 addressing. It supports the complete range of IPv6 prefixes as defined in the 3GPP TS 29.571 and 3GPP TS 29.510 specifications.

The protocol configurations can be performed during deployment using the Custom Values YAML file for CNC Policy. For more information about the configurations, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

External Communications

With the support for IPv6 protocol, CNC Policy allows communication with external NFs over the following interfaces:

- The DNS (Domain Name System) for the resolution of FQDNs
- The SBI interface over the HTTP/2 and HTTPS protocols for the following types of connections:
  - Consumer Connections
  - Producer Connections
- Diameter interface for the following types of connections:

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - Connection as a server. For example, connection with PGW
  - Connection as a client. For example, connection to OCS over Sy
- Service IP endpoints
- Provisioning interface for connection with Cloud Native Core Console (CNCC)
- CNC Policy Rest API interface for the REST API Client configurations over IPv6

Internal Communications

CnPolicy supports all the internal communication over IPv6 addresses for PCF, PCRF, and Converged Policy modes.

The internal communications include:

- Inter microservice communication
- Communication with CnDbTier
- Communication with IGW, EGW
- Communication with Diameter Gateway and Diameter connector
- DNS for FQDN resolution
- Integration with common services using IPv6 addressing for observability - logging, monitoring and tracing
- Communication with platform components supporting retrieval of certificates/public/private keys

Managing IPv6 Support in Converged Policy Mode

Deploy and Configure

To deploy Policy in the IPv6 environment:

1. The cnDBTier must have IPv6 enabled. For information about installing cnDBTier, see "Installing cnDBTier" in Oracle Communications cnDBTier Installation Guide.
2. Deploy Policy over the IPv6 supported cnDBTier site. For information about installing and deploying Policy over IPv6, see the Configuration Parameters for Dual Stack and Single Stack IPv4 or IPv6 section in *Oracle Communications Converged Policy Installation and Upgrade Guide*.

4.65 Handling Rx Stale Sessions

Policy Control Function (PCF) supports auditing the Rx session periodically to detect and remove stale sessions. This helps to avoid unlimited system memory utilization growth.

An Rx session is considered as stale when an association exists in PCF, but is not used by Proxy Call Session Control Function (P-CSCF) or Application Function (AF) for a specific time period. The time period after which the session is considered as stale is configurable.

PCF detects an Rx stale session based on:

- Configured Time To Live (TTL)
- Authorization Lifetime using:
  - Support of Rx Subscription Expiry
  - Authorization Lifetime Attribute Value Pair (AVP)

Copyright © 2019, 2026, Oracle and/or its affiliates.

TTL is the time period for which an Rx session can be active. When the TTL of an Rx session reaches its maximum as configured by the user, the Rx session will be considered as stale.

Authorization Lifetime is the maximum lifetime of an Rx session. When the life time of a session reaches its Authorization Life Time, the session is considered as stale and is cleaned up.

> **Note**
>
> Currently, the value of Authorization Lifetime is just echoed back and it is expected to be the same value as configured in TTL under Audit settings in Policy Authorization service (PA service).

The P-CSCF provides Authorization Lifetime AVP and the `Support of Rx Subscription Expiry` feature bit for the Supported-Feature AVP in Rx Authorization Authentication Request Initial (AAR-I).

PCF echoes back the value in Authorization Lifetime AVP in Authorization Authentication Answer (AAA) response to P-CSCF along with the `Support of Rx Subscription Expiry` feature bit in the Supported-Feature AVP.

The P-CSCF sends Authorization Authentication Request Update (AAR-U) according to the Authorization Lifetime AVP.

PCF updates the last access timestamp of the Rx session when it receives AAR-U from P-CSCF.

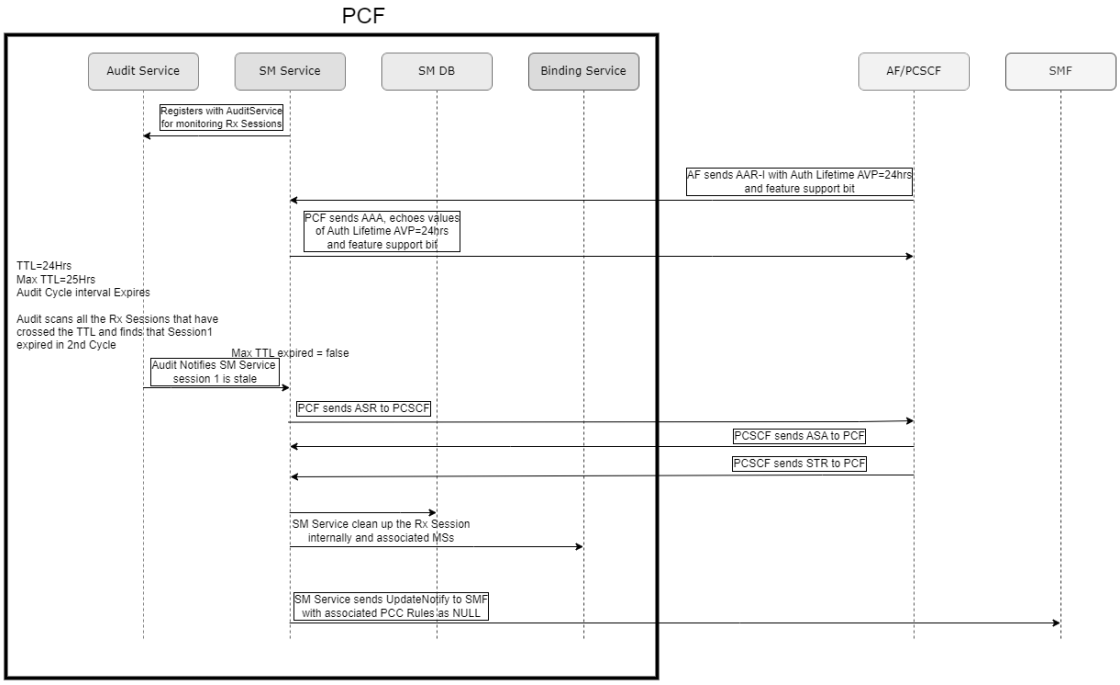
PCF sends abort session request to P-CSCF and removes the stale Rx Session locally along with the related PCC rules in SMF, upon detection.

Detection and removal of stale Rx session generates appropriate alert and log entries.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

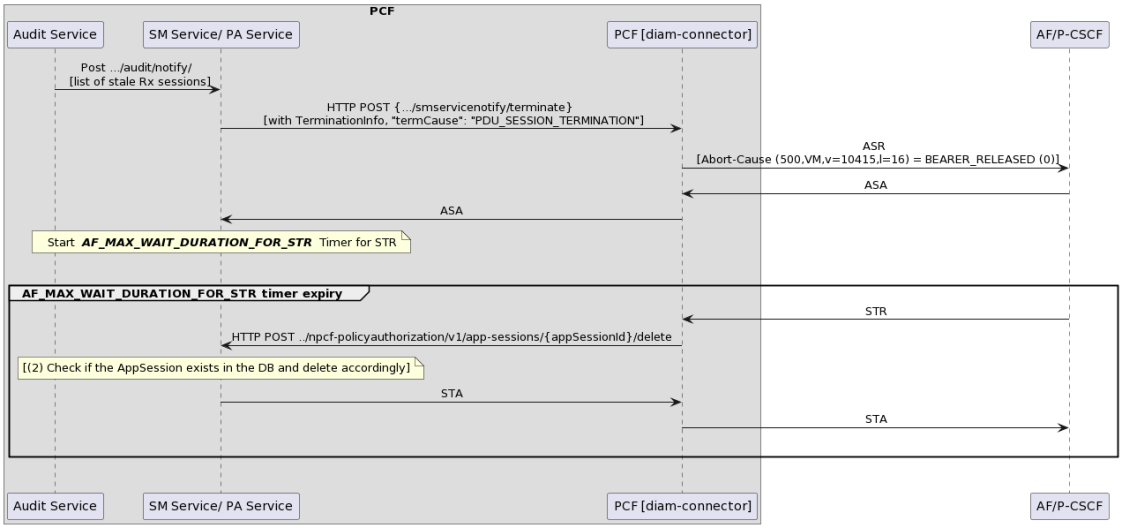
Figure 4-156 Rx Stale Session Detection and Deletion Based on TTL and Authorization-Lifetime



1. If the **Enable Audit** field is enabled under **Audit** group in **PCF Policy Authorization** page for **Service Configurations**, SM service registers with Audit service for monitoring Rx sessions.
2. SM service receives AAR-I message from P-CSCF with `Support of Rx Subscription Expiry` feature bit for the Supported-Feature AVP.
3. If the **Enable Authorization Lifetime** field is enabled under **System** group in **PCF Policy Authorization** page for **Service Configurations**, and the AAR-I message includes Authorization-Lifetime AVP, SM service sends Authorization-Lifetime to P-CSCF in Rx AAA messages. It returns the same value of Authorization-Lifetime AVP to P-CSCF, as the value received from P-CSCF.
4. SM service registers with the Audit service for monitoring the Rx session.
5. Audit service analyzes the EXPIRY_TIMESTAMP and compares it with TTL value. If necessary, it sends a message to SM service as mentioned in the next step.
6. If AAR-U for an Rx session is not received and its TTL expires, Audit service sends a message to SM service with `Max TTL Expired = true`.
7. SM service sends an Abort Session Request (ASR) to P-CSCF for that Rx session.
8. P-CSCF sends a successful Abort Session Answer (ASA) response to SM service.
9. P-CSCF also sends a STR to SM service.
10. SM service responds to P-CSCF with STA message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-157 Rx session cleanup when Audit service detects a stale session



If **Enable Audit** field is enabled, SM service registers with Audit service for auditing Rx sessions. Depending on the value of `EXPIRY_TIMESTAMP` field in `AppSession` database, the Audit service considers that the Max TTL of an Rx session has expired. SM service updates `EXPIRY_TIMESTAMP` after every successful AAR-I and AAR-U messages. In case of georedundancy, the Audit service uses `SITEID` field in `AppSession` database to filter and handle the Rx sessions for multiple sites.

1. When Audit service detects that some of the Rx sessions expired and for any reason these Rx sessions are not deleted after TTL expiry, Audit service sends the list of such Rx sessions to PA service for which the Max TTL has expired.
2. For all the Rx sessions in the list, PA service sends PDU Session Termination request to SM service.
3. SM service sends ASR to P-CSCF and waits for a configured time period to receive a successful Abort Session Answer (ASA) response from P-CSCF.
   - When sending ASR, if SM service receives any response that is not success (except for timeout), it cleans up the session.
     - If ASA times out, SM service checks if AppSession exists for these sessions in Audit service. SM service deletes the Rx Session and the associated resources internally. Also, it deletes the associated PCC Rules from SMF externally, by sending Update Notification to SMF.
     - If SM service receives ASA with error code other than 5002 (for reasons like the ASR request did not go out of PCF), then the Audit service does not delete the AppSession for such sessions. Depending on the configuration, SM service resends the ASR to P-CSCF. If all the retries fail with timeout or any other error, SM service deletes the Rx Session and associated resources internally. Also, it deletes the associated PCC Rules from SMF externally, by sending Update Notification to SMF.
   - If SM service receives a successful ASA from P-CSCF, it waits for receiving a STR from P-CSCF.
4. PCF uses `AF_MAX_WAIT_DURATION_FOR_STR` timer to receive the STR from P-CSCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

If AF_MAX_WAIT_DURATION_FOR_STR timer expires and SM service does not receive STR from P-CSCF, SM service checks if AppSession exists for these sessions. SM service deletes the Rx Session and the associated resources internally. Also, it deletes the associated PCC Rules from SMF externally, by sending Update Notification to SMF.

5. If SM service receives a successful STR from P-CSCF, SM service checks if AppSession exists for these sessions. SM service cleans up these Rx sessions and the associated resources externally and internally. Also, it deletes the associated PCC Rules from SMF externally, by sending Update Notification to SMF.
6. SM service responds to P-CSCF with STA.

- When there are bulk of stale Rx records detected, in order to avoid performance impact on the system, Policy allows to configure:
  - the rate at which ASR is sent to P-CSCF.
  - the rate at which the records are deleted.

Managing Handling Rx Stale Sessions

Enable

By default, this feature is disabled. You can enable stale Rx session audit and deletion using CNC Console or REST API for Policy.

Enable using CNC Console:

To enable the Rx Stale Session detection based on TTL and Authorization-Lifetime:

- To enable auditing by Audit service, configure:
  - **Enable Audit** parameter to `true` under **Audit** group in **PCF Policy Authorization** page for **Service Configurations**.
  - Configure **App Session Age (in minutes)** parameter under **Audit** group in **PCF Policy Authorization** page for **Service Configurations**.
- To enable detection and deletion of stale sessions based on Authorization Lifetime, enable **Enable Authorization Lifetime** parameter under **Systems** group in **PCF Policy Authorization** page for **Service Configurations**.

For more information about enabling the feature through CNC Console, see PCF Policy Authorization.

Enable using REST API

To enable the feature, set the value of `enable` parameter to `true` in `Audit` group in `Policy Authorization Service` API.

For more information about enabling the feature through REST API, see *Policy Authorization Service* in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure this feature using the CNC Console or REST API for Policy.

Configure using CNC Console: Perform the feature configurations under **Audit** group in **PCF Policy Authorization** page for **Service Configurations**. For more information, see PCF Policy Authorization.

Configure using REST API: Configure the parameters under `Audit` group in `Policy Authorization Service` API. For more information about configuring the feature through

Copyright © 2019, 2026, Oracle and/or its affiliates.

REST API, see *Policy Authorization Service* in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

> **Note**
>
> - On upgrade, `SITEID` and `EXPIRY_TIMESTAMP` contains null values in all AppSession records until there is an update on the AppSession.
> - As `SITEID` and `EXPIRY_TIMESTAMP` contains null values, the default value of `Handle NULL As Stale` parameter is set to `false`. You must enable this setting after the desired TTL has passed after site upgrade. This will cleanup all AppSessions for which `SITEID` and `EXPIRY_TIMESTAMP` contains null value. That is, they did not receive an update for the duration after upgrade and now these sessions are considered as stale.

Observability

Metrics

The following SM service metrics are used to differentiate between SM and PA deletions:

- audit_delete_records_max_ttl_count_total
- audit_notifications_sent_totak
- audit_delete_records_count_total
- audit_terminate_notify

For more details on these metrics, see SM Service Metrics.

4.66 Data Compression

Data compression can be used to reduce the data size and hence the storage used by database. It can also be used to improve the communication latency between application and DB when compression is performed at the application level.

Following are the available options for data compression schemes:

- **MySQL_Compressed**: Compression and decompression performed at MySql level
- **Zlib_Compressed**: Compression and decompression performed at application level

Binding and PDS services support this feature only with Zlib_Compressed scheme. PCRF-core and SM service supports this feature only with MySQL_Compressed scheme.

Managing the Feature

Enable
This feature is disabled by default. It can be enabled by choosing the compression scheme from respective service configuration. For more information, see the details of the **Data Compression Scheme** field in PDS, Binding Service, and PCF Session Management in the Configuring Policy Using CNC Console section.

Configure
You can configure this feature using Helm for PCF Session Management and CNC Console for PCF Session Management, PDS, and Binding service as follows:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Helm**: Set the value of the parameter `smDataCompressionScheme` and `paDataCompressionScheme` to 0, 1, or 2 during install or upgrade. For more information, see the Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.
- **CNC Console**: You can configure this feature using the **Data Compression Scheme** field in PDS, Binding Service, and PCF Session Management in the Configuring Policy Using CNC Console section.

Observe
The following metric has been added in PCF Session Management service for this feature:

- occnp_db_overall_processing_time

For more information, see SM Service Metrics.

4.67 Usage Monitoring on Gx Interface

Cloud Native 4G Policy implements Usage Monitoring or Quota Management using the combination of PCRF Core and Usage Monitoring. These two microservices have their respective policy engines and thus separate policy projects. Each of the two microservices (along with their respective policies) has the following functions with respect to Quota Management:

- PCRF Core - Controls PCC and/or Session Rules, and Charging Description.
- Usage Monitoring - Controls the Quota Selection, Accumulation and Grant.

For details on PCRF Core, see PCRF Core Service

For details on Usage Monitoring Service, see Usage Monitoring Service

To achieve end to end use cases of 4G quota, the policies must be split into these two microservice functions.

The configuration of Quota plans can be done at two places:

- CNC Policy - Quota plans that are not per subscriber can be configured directly on CNC Policy and used in Policy Configuration. For more details, see Usage Monitoring Service.
- UDR - Quota plans that need to be assigned per subscriber can be provisioned on the UDR.
  For details on UDR Quota plans, see *Converged Quota Support* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

> **Note**
>
> Quota plans when configured in CNC Policy will avoid duplication of the plan data in UDR for every subscriber.

Quota Management for a Subscriber

Usage Monitoring supports different quota plans for a subscriber such as Basic, Dynamic, Daily, Roaming, Monthly quota based on volume of usage.

Basic Quota
Basic quota specifies restrictions on the amount of data volume, active session time, or service-specific events that a subscriber can consume.

Copyright © 2019, 2026, Oracle and/or its affiliates.

A single quota can express limits on any combination of volume, time, or events. A Basic quota is also referred as a plan. For example, Domestic/Home/ Roaming plan.

Plan
A **plan** describes a subscriber's basic, recurring service. A plan can be a basic plan, or a pass or a top-up.

The quota plan for a subscriber is provisioned at UDR. For details on provisioning quota and dynamic quota for a subscriber, see *Converged Quota Support* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

Plans include policy characteristics such as time and volume limits. These characteristics can be computed automatically or through policy rules. Policy actions grant plans, based on a subscriber's tier provisioned on CnUDR.

The following fields under **Usage Monitoring** page for **Service configurations** can be used to configure the time and volume limits for a plan:

- Minimum Volume Grant (bytes): Minimum grant value (in bytes) that can be approved for volume based usage monitoring.
- Maximum Volume Grant (bytes): Maximum grant value (in bytes) that can be approved for volume based usage monitoring.
- Minimum Time Grant (seconds): Minimum grant value (in seconds) that can be approved for time based usage monitoring.
- Maximum Time Grant (seconds): Maximum grant value (in seconds) that can be approved for time based usage

  monitoring.

The default volume and time grants for the plan can be configured using the fields available under **Default Volume Grant** and **Default Time Grant** sections in **Usage Monitoring** page.

A plan can have associated quota controls, which in turn can be subject to modification or over-ride through Passes, Top-ups, and Roll-overs.

Reset frequency can be:

- Hourly
- Daily
- Weekly
- Monthly
- Yearly
- Never

Postpaid monthly data plans are monthly recurring data plans that have defined **volume/time thresholds associated**. Users are notified about the user’s current usage at various levels. On reaching the threshold, the user’s access is subjected to suspension of service or reduced quality of service.

The default usage levels can be configured using the following fields under **Default Usage Levels** section in **Usage Monitoring** page for **Services Configuration** in CNC Console:

- Minor Usage Level (%): Threshold value in percentage indicating minor usage.
- Major Usage Level (%): Threshold value in percentage indicating major usage.
- Critical Usage Level (%): Threshold value in percentage indicating critical usage.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Exhausted Usage Level (%): Threshold value in percentage indicating usage level has exhausted allowed limit.

Dynamic Quota
Dynamic quotas are one-time changes to a subscriber's service.

There are two types of dynamic quotas:

- Passes
- Top-ups.

Passes
Passes allow the service providers to grant resources outside of a subscriber's normal/default plan.

A pass is a one-time override quota that a subscriber can purchase that temporarily replaces or adds to a subscriber's default plan.

It allows users to access data till a predefined quota (either volume, time or event based) for a specific validity period.

For short time users, there can be different types of data passes:

- Hourly
- Daily
- Weekly
- Monthly
- Yearly
- Never

A subscriber can have multiple passes. An active Pass can modify the QoS controls, charging parameters, or other configurable rules associated with a subscriber's service.

A Pass may:

- be valid for a restricted interval
- start when provisioned, or at a specific time, or upon occurrence of a triggering event within its validity interval
- end at a specific time, or after given duration once activated, or upon a particular event
- apply continuously, or only during certain time periods, or only under certain conditions (such as. when roaming)
- apply to the subscriber's overall usage, or be more limited (such as. applying only to specific applications, flows, traffic types, or pre-defined rules)

Passes are common options for pre-paid subscribers, who frequently have limited or no data access via their basic plan, and may purchase Passes to gain access to such services. They can also be used to allow Casual Use plans for pre- or post-paid subscribers to purchase services on an occasional basis which they would not otherwise subscribe for on an ongoing basis.

Users are notified about the user's current usage at various levels. On reaching the threshold, the user's access is subjected to suspension of service or reduced quality of service.

Pass configuration options can be modified. The dynamic PCC rules are updated based on the changes on the Pass Configuration.

Upon deletion of a pass, the pass is exhausted immediately.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Top-up
A Top-up allows to extend access to services beyond the time or volume limits typically enforced by a plan. A top-up is processed if the default plan is exhausted, or the quota is expired. There can be multiple Top-ups for a subscriber based on time or volume.

> **Note**
>
> Passes cannot not have Top-ups.

Top-up configuration options can be modified. The dynamic PCC rules are updated based on the changes on the Top-up configuration.

Upon deletion of a Top-up, the Top-up is exhausted immediately.

The quota plan for a subscriber is provisioned at UDR. For details on provisioning quota and dynamic quota for a subscriber, see *Converged Quota Support* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

Quota details are configured at UDR based on ueID using the REST API: {apiRoot}/nudr-dr-prov/v1/policy-data/{ueId}. For more details on how to add the quota information, see *Provisioning Operations for PCF Data* section in *Oracle Communications Cloud Native Core, Unified Data Repository REST Specification Guide.*

Whenever there is a change in the subscriber quota information, UDR notifies Policy through updateNotify message.

The order/priority of basic plan, pass or top-ups can be specified using **Selection Order 1**, **Selection Order 2**, and **Selection Order 3** fields under **Data Limit Selection** section in **Usage Monitoring** page for **Service configurations** in CNC Console for Policy. For more information, see Usage Monitoring Service.

Exhaustion (Quota)
Exhaustion occurs when reports indicate that usage of a metered unit has equaled or exceeded the specified quota limit. If a recurring quota is exhausted, typically the subscriber's sessions are subjected to more restrictive policies until the end of the plan period or billing cycle.

Expiration (Quota)

Expiration occurs when a periodic plan reaches the end of the plan period or billing cycle, or when a one-time pass or top-up reaches its established End Time or close to the validity period.

> **Note**
>
> The time-based expiration of a Quota is quite different from the exhaustion of a Quota restricting the active session Time of a subscriber's usage.

A plan (periodic quota) is typically reset at expiration.

Rollover
A rollover allows a subscriber to carry forward unused units from one billing cycle to another.

For example, if a subscriber is allowed 10 GB of data a month and only uses 9 GB, the remaining 1 GB of data can be saved for use in the next month.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Rollover units can accumulate and can be carried across multiple months.

Data units are rolled over based on multiple conditions such as:

- Rollover unused data when it is more than a minimum threshold.
- Total data (base data + rollover data) may not exceed a maximum cap.
- Rollover certain percentage of unused data.
- Data may be rolled over for a fixed number of billing cycles.

When data is rolled over without any restriction, the leftover volume/time can be added to the base volume/time in the next billing cycle.

When data is rolled over with restrictions on duration of usage (for example, a maximum number of rollover periods/cycles), it needs to be tracked as separate rollover definitions (data limits).

The data rollover for a plan can be enabled using **Data Rollover** field under **Usage Monitoring** page for **Service Configurations**.

The data rollover can be configured based on a particular profile. The rollover profiles can be created by configuring the fields in **Data Rollover Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.

You can create multiple profiles and specify profile to be used for the plan using **Data Rollover Profile** field under **Usage Monitoring** page for **Service Configurations**.

Also, you can specify the default rollover profile to be used in **Default Data Rollover Profile** field.

Support for Multiple Passes for a subscriber
Usage Monitoring supports One time passes.

Support for Multiple Top-Ups
Usage Monitoring supports One time top-ups.

Match list for Quota use cases
To identify the geographical location where the data usage is occurring as well as to ensure that the correct quota plan is applied, Policy uses match lists while defining the MCC/MNC allocations, RAT-Type, Service GW IP address, APN Lists.

- IPv4 Subnet - When a Match List is created with a data type of IPv4 subnet, the Items are configured with valid IPv4 subnet addresses in CIDR notation.

  For example, 192.168.10.0/24.

  PRE evaluates if an IPv4 address belongs to one of the subnets configured in the match list.
- IPv6 Subnet - When a Match List is created with a data type of IPv6 subnet, the Items are configured with valid IPv6 subnet addresses in CIDR notation.

  For example, 2001:db8:abcd:0012::0/64.

  PRE evaluates if an IPv6 address or an IPv6 Prefix belongs to one of the subnets configured in the match list.
- Regular Expression - When a Match List is created with a data type of Regular Expression, the Items are configured with valid Regular Expressions, such as ^([a-zA-Z0-9. _-])+$.

  PRE evaluates if a string matches one of the Regular Expressions configured in the match list.

Support for flexible billing day change

Copyright © 2019, 2026, Oracle and/or its affiliates.

Billing day for an active plan can be changed from monthly to yearly, weekly, daily, or hourly. The billing day change can be applied to either the current billing cycle or next billing cycle.

The **Apply Billing Day / Data Plan Change** field under **Usage Monitoring** page for **Service configurations** in CNC Console can be used to indicate whether the billing change should be applied to current billing cycle or to the next billing cycle.

With flexible billing day change, the billing day for plans will also be changed with the same periodicity. But, Policy supports changing the periodicity as well.

The billing date change should take place and determine if the usage should be pro-rated.

- Delayed behavior: Allows the billing day change to take effect on the next billing cycle irrespective of the current usage. Quota will be reset after the current billing cycle end date is reached.
- Immediate behavior: Allows the billing day change to take effect immediately. Quota will also be reset immediately.
- Default behavior: Allows the flexible billing day changes to take place immediately. For a user with no current usage and for a user that has current usage, billing day change will take place after the end of the user's current billing cycle is reached.

The **Enable Pro-rated Data at The Time of Billing Day Change** field under **Usage Monitoring** page for **Service configurations** can be used to indicate whether pro-rated data calculation should be applied to the selected plan at a time of billing day change.

When billing day change is set to current cycle and a billing day change is performed, the **lastresetTime** field in umdata stores the previous billing day and **resettime** field stores the updated billing day.

Usage monitoring support at PCC rule level

Policy supports Usage monitoring either at PCC rule level or at session level.

Usage monitoring can be requested on an individual rule (PCC rule level) or on all rules activated during a IP-CAN session (session level).

- Based on certain custom attributes on CnUDR, quota can be granted for an application like whatsapp or facebook although the pass or a top-up volume been exhausted.
- Differentiate unlimited usage of certain application and not volume accumulate those applications for overall quota monitoring. For example: Plans with Facebook unlimited.

Multiple quotas contain single session-level and multiple PCC-level grants.

Rollover will be applicable for PCC-level grants.

- PCCRule data can be provisioned at UDR or configured at Policy. This can be of type BASE, TOP-UP and PASS.
- PCCRule can also be rollover. All rollover configurations will be applicable for PCCRule data limits.
- PCCRule can also allow excessUsage data.
- PCCRule can be of Type BASE, Top-up and pass.

You can configure the usage monitoring at PCC rule level using the following blocks available under **Policy Projects** in CNC Console.

- PCC Rule Hint: Allows to access the value of PCCRuleHint from Data limit profile and apply the same in UMPolicyDecision in monitoring key.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Active Monitoring Key with PCCRuleHint: Allows to select a monitoring key for the configured PCCRule from usage monitoring policy decision which fulfills the value from active monitoring with PccRuleHint attribute.

For more information on configuring the PCC rules for usage monitoring, see *Usage Monitoring* section in *Oracle Communications Cloud Native Core, Policy Design Guide*.

Pro-Rating of quota limits

Policy supports pro-rating of quota volume. If a subscriber's profile billing day is changed, a shorter than usual period occurs (either from the date of change, or after the next scheduled reset).

For example, if the user has a plan with a monthly quota of 30GB and the plan start date is the 1st of every month, now the plan is activating at the 10th of that month, so rather than allocating the complete 30GB to the user, only 20GB will be allocated to the user as the expected activation date is the 1st of the month, but the plan activates after 10 days, so the remaining data is 20GB for that month.

The following parameters under **Usage Monitoring** page for **Service Configurations** can be used to configure the pro-rating of the quota:

- Enable Pro-rated Data at The Time of Activation: Indicates whether pro-rated data calculation should be applied to the selected plan at a time of activation or not.
- Enable Pro-rated Data at The Time of Billing Day Change: Indicates whether pro-rated data calculation should be applied to the selected plan at a time billing day change .

Pro-rating can be configured per plan to reduce the quota allocation for the short period.

> **Note**
>
> Pro rating is not applicable for one-time plan.

Quota Policy conditions

The Policy supports a number of blocks, actions, and conditions that can be used for constructing Policy rules, such as:

- where the user has greater than number of rollover units of type unit type for plan name and usage type.
- where the user is using greater than 80 percent and less than 100 percent of total volume for Monthly1,Daily1
- where the user is using greater than 100 percent of total volume for Monthly1,Daily1

For more information on the blocks, actions, and conditions available to write Policy rules, see *Usage Monitoring* section in *Oracle Communications Cloud Natvie Core, Policy Design Guide*..

PRE support for Usage Monitoring

Policy uses Policy Runtime Engine (PRE) to enable and manage the following usage monitoring use cases:

- Grant pass or top-ups.
- Enable time of day quota. For example, If time of day is between HH:MM:SS - HH:MM:SS grant x% of volume and Y QoS
- Quota Plans can be activated by Policy Rule Conditions which look for attributes on

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - Gx attributes : MCC-MNC, RAT Type, Serving GW IP address.
  - CnUDR such as **Tier**, **Entitlement**, or **Custom Field(s)***values* provisioned in the Subscriber Profile

PRE performs the Policy evaluation when it receives a notification from UDR regarding quota or state data update.

Possible change of parameters include:

- Reset of Quota, triggers an action to throttle, block, or re-direct user to charging portal
- Billing day change triggers pro-rata calculation
- Subscriber Tier change
- Any customer attribute definition change

Support for profiles based configuration

Data Limit Profiles

When a subscriber is provisioned with multiple quota plans with different priorities, a separate profile can be used to track each plan. For example, if a subscriber is provisioned a daily plan and a monthly plan, one profile is used to track the daily quota limit and another profile is used to track the monthly quota limit.

A unique name and identifier can be assigned to each data limit profile and details such as plan type, profile type, parent plan, priority, usage level, reset period and billing day can be configured for the profile.

Data Limit Profiles can be configured using CNC Console and REST API.

- **Using CNC Console**: Apply the configurations in **Data Limit Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
  For more information, see Data Limit Profiles.
- **Using REST API**: Configure the parameters in UM Data Limit Profile API.
  For more information, see *UM Data Limit Profile* section in *Oracle Communications, Cloud Native Core, REST API Guide*.

Data Limit Selection Profiles

A set of rules can be used to select one or more data plans based on certain conditions.

For example, if a subscriber is provisioned with one monthly limit quota plan and two roaming plans: roam1 and roam2, a selection rule can be used to select a plan based on home zone and roaming zone. Separate selection profiles can be created for each selection rule.

A unique name can be assigned to each selection profile and details such as rule type, rule priority, parameter type (forwarded attribute/Policy decision tag), attribute name, and match list can be configured for the profile.

Data Limit Selection Profiles can be configured using CNC Console and REST API.

- **Using CNC Console**: Apply the configurations in **Data Limit Selection Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
  For more information, see Data Limit Selection Profiles.
- **Using REST API**: Configure the parameters in UM Data Limit Selection Profile API.
  For more information, see *UM Data Limit Selection Profile* section in *Oracle Communications, Cloud Native Core, REST API Guide*.

Data Limit Sorting Profiles

Copyright © 2019, 2026, Oracle and/or its affiliates.

Sorting rule is a set of rules to sort data limits.

When a subscriber is provisioned with multiple quota plans, a sorting rule can be applied to sort the quota plan based on a criteria. For example, if a subscriber is provisioned with two Monthly Limit Quota plan with different priority plan1 - priority1 and plan2 - priority2, a sorting rule can be created to select plan with higher priority. Separate sorting profiles can be created for sorting rules.

The sorting rules can be configured based on order of index, parameter type, attribute name, and order.

If selection rules are configured, sorting rules are applied after applying selection rules and when the output of selection rules results in more than one data limit.

Data Limit Sorting Profiles can be configured using CNC Console and REST API.

- **Using CNC Console**: Apply the configurations in **Data Limit Sorting Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
  For more information, see Data Limit Sorting Profiles.
- **Using REST API**: Configure the parameters in UM Data Limit Sorting Profile API.
  For more information, see *Data Limit Sorting Profile* section in *Oracle Communications, Cloud Native Core, REST API Guide*.

Data Rollover Profiles

When data rollover is enabled, data rollover profile can be used to configure the rollover.

The data rollover profile can be configured with details such as:

- rollover data consumption
- maximum number of rollovers
- data rollover percentage
- maximum rollover threshold
- minimum rollover threshold
- data limit cap

Data Rollover Profiles can be configured using CNC Console and REST API.

- **Using CNC Console**: Apply the configurations in **Data Rollover Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
  For more information, see Data Rollover Profiles.
- **Using REST API**: Configure the parameters in UM Data Limit Sorting Profile API.
  For more information, see *Data Rollover Profile* section in *Oracle Communications, Cloud Native Core, REST API Guide*.

Attribute Forwarding Profiles

Policy supports forwarding the value of attributes such as Serving Gateway MCC MNC / IP Address, and APN from PCRF Core to Usage Monitoring Service. An attribute forwarding profile is used to configure the list of attributes to be forwarded from PCRF Core to Usage Monitoring.

An attribute forwarding profile can be configured with details such as attribute name, attribute source, attribute selection (predefined/custom), request message type (diameter message/ HTTP message), and attribute location.

The attribute forwarding profile name must be specified in PCRF Core settings.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Attribute forwarding profiles can be configured using CNC Console or REST API:

- **Using CNC Console**: Apply the configurations in **Attribute Forwarding Profiles** page under **Common Data** for **Service Configurations**.
  For more information, see Attribute Forwarding Profiles.
- **Using REST API**: Configure the parameters in Attribute Forwarding Profile API.
  For more information, see *Attribute Forwarding Profile* section in *Oracle Communications, Cloud Native Core, REST API Guide*.

Data Compression in Usage Monitoring

In order to handle the growing size of the Usage Monitoring database and the replication volume, Policy supports compressing the Usage Monitoring data.

Usage Monitoring service application is used to reduce the V columns in `UmContext` table for data persisted in the database.

Data Compression Scheme flag available under **Usage Monitoring** page for **Service Configurations** in CNC Console is used to configure the compression status on the V columns in `UmContext` table.

When accessing the data from `UmContext.v`, the application determines the compression status based on the value of `COMPRESSION_SCHEME` and does the decompression accordingly.

The **Data Compression Scheme** flag accepts the following values:

- `Disabled`: Indicates that the data will not be compressed and will be stored in the column in uncompressed format. The value of `COMPRESSION_SCHEME` for that row is set to the default value 0.
- `MySQL Compressed`: Indicates that the data will be compressed using MySQL and will be stored in the column in compressed format. The value of `COMPRESSION_SCHEME` for that row is set to 1.
- `Application Compressed`: Indicates that the data will be compressed using Zlib and will be stored in the column in compressed format. The value of `COMPRESSION_SCHEME` for that row is set to 2.

> **Note**
>
> - The existing data will remain in uncompressed format and their COMPRESSION_SCHEME` is set to default NULL. Once the "Data Compression Scheme" changes to "MySQL Compressed" or "Application Compressed", all future v column data will be in compressed format.
> - Existing session's data will be compressed once we send CCR-U/UDR Notify with compression enabled.

For more information on configuring data compression for Usage Monitoring, see Configuring Usage Monitoring.

Managing the Feature

This section provides information on enabling, configuring, observability and logging for Usage Monitoring on Gx Interface.

Enable

Copyright © 2019, 2026, Oracle and/or its affiliates.

By default, the Usage Monitoring service is disabled.

To enable the service, set the **Enabled** parameter under **Usage Monitoring** group in **PCRF Core Settings** page for **Service Configuration**. to `true` at the time of installing or upgrading Policy.

For information on how to set the parameter value, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

The **Enable PRE** field under **Usage Monitoring** page for **Service configurations** in CNC Console can be used to enable or disable the interaction with PRE for Policy evaluation as per the match list.

Configure

You can configure the Usage Monitoring for Gx interface using CNC Console and REST API.

- **Configure using CNC Console**: To configure Usage Monitoring for Gx interface using CNC Console, perform the configurations as described in the following sections:
  - Configuring Usage Monitoring
  - Settings
  - Attribute Forwarding Profiles
  - Usage Monitoring

  For details on the blocks used to create Policy projects, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.
- **Configure using REST API**: Refer to the *Usage Monitoring* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.67.1 Migrating Subscribers from OCPM to PCRF Deployment

Quota details for both OCPM (4G) and Converged Policy (5G) are configured and provisioned at the individual subscriber level in OCUDR and CnUDR respectively.

For details on how CnUDR provisions and manages the quota information for PCRF, see *Convered Quota Support* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

Using Provisioning Gateway, 4G provisioning system provisions OCPM data over SOAP/XML interface on CnUDR. Provisioning Gateway converts SOAP/XML to REST/JSON and forwards to CnUDR. CnUDR converges the OCPM quota and dynamic quota data to Converged data model and stores in CnUDR.

For details on how CnUDR integreates with the provisioning gateway, see *Cloud Native Core, Provisioning Gateway Interface Specification Guide*.

CnPCRF interacts with CnUDR to access and manage both OCPM and converged quota information. cnPCRF uses the N36 interface toward CnUDR for OCPM call flows.

The OCPM data that CnPCRF receives from CnUDR includes:

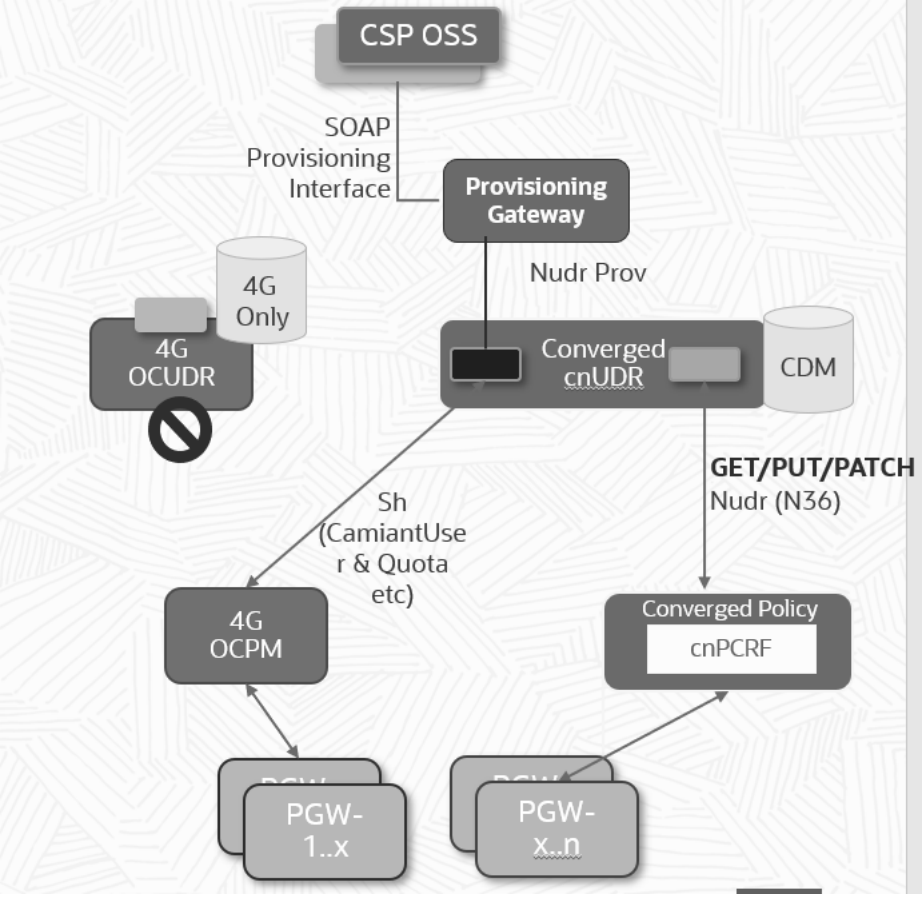
- Quota data: the runtime quota data of a subscriber. That is, the data time and/or volume consumed by that subscriber and the other meta-data. For example, plan activation date, reset date, any roll-over plans and their corresponding usages.
  The remaining quota must be derived based on the consumed data retrieved from 4G UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Dynamic quota data: includes the provisioning data for dynamic plans which are also known as passes and top-ups.

> **Important**
>
> Since the 4G data structures for quota usages and monitoring are not defined by 3GPP standards, there must be a mapping from the proprietary 4G data structures to 3GPP defined 5G Data structures.

The following diagram depicts the connectivity between OCPM and CnUDR which will be swicthed to CnPCRF and CnUDR.



Diverting the subscribers from OCPM deployment to PCRF deployment involves the following procedures:

Migrating Subscribers from OCUDR to CnUDR

Subscribers from OCUDR are migrated to CnUDR either using the migration tool or on-demand.

Using the migration tool, the subscribers are migrated in batches based on subscriber range during the off peak hours.

The subscriber data is exported in EXML format, which is compatible with 4G OCUDR export format. It supports the export of 4G policy data (VSA and umData/umDataLimits) in EXML

Copyright © 2019, 2026, Oracle and/or its affiliates.

format from 5G UDR to 4G OCUDR using the subscriber export tool. In case of any error during the migration, the EXML format supports rollback of exported data.

For more details on the data export, see *Support for EXML Format* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

> **Note**
>
> When Migration is in progress, dual provisioning at both OCUDR and CnUDR is not supported.

For more details on how the subscribers are migrated from OCUDR to CnUDR, see *Migrating Subscriber Data from 4G UDR to 5G UDR* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

The migration of the subscriber data can be monitored using the metrics mentioned under *nudr-migration-service Metrics* section in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

In case of migration failure for any reason either at OCUDR or at CnUDR, the quota for the subscriber must be reprovisioned to make up for any quota loss.

In case of new deployment, CnUDR must provision usage monitoring level, which indicates the level of the usage monitoring instance (PDU Session level or per Service). When `Enable Quota Migration` parameter is enabled, CnPCRF reads InitialServiceSpecific from OCUDR and sets the UsageMonLevel in CnUDR.

To set the UsageMonLevel, configure the following mandatory parameters in UDR for SM Policy data for subscriber profile:

Table 4-126 Mandatory Parameters

Parameter	Description
umDataLimits.endDate	Indicates the end date and time till when the usage monitoring level to be applied.
umDataLimits.name	Uniquely identifies the UM Data Limit Profile by a name.
umDataLimits.limitId	Specifies the limit identifier. Multiple limit identifiers may have the same priority.
umDataLimits.umLevel	Indicates the level of the usage monitoring instance (PDU Session level or per Service).
umDataLimits.startDate	Indicates the start date and time from when the usage monitoring level to be applied.
umDataLimits.usageLimit.duration	Indicates the duration of the usage limit in seconds. **Range**: 3600 - 31536000 (1 Year)
umDataLimits.usageLimit.totalVolume	Specifies the total data octets for both downlink and uplink. **Range**: 512 - 1073741824000 (1000 GB)
umDataLimits.usageLimit.uplinkVolume	Specifies the uplink data octets. **Range**: 512 - 1073741824000 (1000 GB)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-126 (Cont.) Mandatory Parameters

Parameter	Description
umDataLimits.usageLimit.downlinkVolume	Specifies the downlink data octets. **Range**: 512 - 1073741824000 (1000 GB)
umDataLimits.resetPeriod.period	Indicates whether the periodicity is "YEARLY", "MONTHLY", "WEEKLY", "DAILY" or "HOURLY". **Default value**: Monthly
umDataLimits.Type	Indicates which day of the period to reset the usage limit. **Default value**: LAST_DAY **Note**: If this configuration is updated, the new configuration shall be applied in the next billing cycle.
umDataLimits.Priority	A Priority is used to weigh it with other Data Limit Profiles and UDR provisioned Data Limits of the same Plan Type. The priority can be used by Policy or Data Limit Selection Profile for choosing among different candidate profiles. The Plan Type, Priority within that Plan Type and the Selection Order of Plan Types together decide the order of selection of Data Plans.

For disaster recovery purposes on CnUDR, the database is backed up as described in *Manual Database Backup and Restore* section in *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*.

Diverting the Sh Traffic from OCPM to CnUDR

OCPM interacts with CnUDR over Sh interface.

To migrate the incoming traffic from OCPM to CnUDR:

1. Log in to the OCPM Console with the given credentials.
2. Add the new data source.
   a. Under **Configuration** section for MPE_CLUSTER, click **Data Sources** tab.
   b. Add the new data source as explained in *Adding a Data Source* section in *Oracle Communications Policy Management Configuration Management Platform Wireless User's Guide*.
3. Configure Sh data source.
   a. Under **Configuration** section for MPE_CLUSTER, click **Data Sources** tab.
   b. Click **Modify**.
   c. Add the Sh data source as as explained in *Configuring an Sh Data Source* section in *Oracle Communications Policy Management Configuration Management Platform Wireless User's Guide*.
4. Configure the server information as explained in *Configuring Sh Server Information* section in *Oracle Communications Policy Management Configuration Management Platform Wireless User's Guide*. Perform all the necessary
5. **Reports** tab under **Configuration** section for MPE Clusters can be used to monitor the status and activity of the connection. For more details, see *Policy Server Reports* section in

Copyright © 2019, 2026, Oracle and/or its affiliates.

Oracle Communications Policy Management Configuration Management Platform Wireless User's Guide.

> **Note**
>
> If CnUDR receives any Sh-UDR request from OCPM and the subscriber profile is not yet migrated to CnUDR, CnUDR fetches the data from OCUDR on-demand and responds to OCPM.

On the CnUDR front, you can monitor the connectivity to OCPM using the metrics mentioned under *Diameter Gateway Metrics* and *nudr-diameterproxy-service Metrics* sections in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*.

In case of errors from cnUDR, rollback the Sh connection from CnUDR to OCUDR by configuring the data source back to OCUDR and changing the server connectivity as explained in *Configuring Sh Server Information* section in *Oracle Communications Policy Management Configuration Management Platform Wireless User's Guide*.

Configuring CnPCRF to fetch the data from CnUDR

1. Configure the CnPCRF to fetch the data from CnUDR.
   a. Perform the following congurations in **Usage Monitoring** page under **Service Configurations** in CNC Console:
      i. Enable **Enable Quota Migration** field to allow retrieval of OCPM data from CnUDR.
      ii. Configure the following fields under **Custom Attribute Mapping**:
         - Reset Day & Time
         - Data Plan Name
         - Data Plan Priority
         - Data Plan Type
         - Data Rollover
         - Data Rollover Profile
         - Parent Plan Name
         - Parent Plan Source

         Data migrated from CnUDR includes the volume usage as is in custom attributes. Based on the Total available volume, CnPCRF calculates the InputVolume and OutputVolume for both Monthly quota and Dynamic Quota for Passes and Top-Ups.
      iii. Verify the priority of the plans and configure **Reverse Priority** field accordingly to make sure that the order or priority in both OCPM and CnPCRF are aligned.

      For more details, see *Configuring Usage Monitoring* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
   b. If Data Limit Sorting Profiles is enabled, configure the fields in **Data Limit Sorting Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
      For more details, see *Data Limit Sorting Profiles* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.
   c. Create the Policy projects for OCPM subscribers using the blocks in **Policy Projects** under **Policy Management** in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

With more number of subscribers migrated from OCUDR to CnUDR, more number of subscribers can be configured on CnPCRF to fetch the profiles from CnUDR.

For more details on writing polices, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

d. Once all the OCPM subscribers are migrated to CnPCRF, terminate the sessions at OCPM and configure the subscriber range to divert the subscribers to CnPCRF. Only CnPCRF will send the GET request to CnUDR for subscriber profiles.

e. In case of any failure either at CnUDR or at CnPCRF during the migration:

   i. Disable `Enable Quota Migration` flag

   ii. Bring up the OCPM again.

   iii. Configure the OCPM to fetch the data from CnUDR over Sh interface.

   Any quota loss during the fallback from CnPCRF to OCPM is made up by reprovisioning the quota.

For details on the metrics used to monitor the successful migration at CnPCRF, see *Usage Monitoring Metrics* section in *Oracle Communications Cloud Native Core, Converged Policy User Guide*.

For detail on the metrics used to monitor the successful migration at CnUDR, see the following sections in *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*:

- nudr-dr-service Metrics
- nudr-notify-service Metrics
- nudr-ondemand-migration-service Metrics

> **Note**
>
> Configuring the PGW to connect to CnPCRF instead of OCPM and also setting the subscriber range at PGW is not in the scope of this document as PGW is outside the Oracle system.

4.67.2 Performance Considerations while Running Quota Management

The following configurations are required in order to achieve optimal performance while running quota management scenarios:

1. Enable compression scheme for both PolicyDS and Usage Monitoring Service. For more information, see PDS Settings and Configuring Usage Monitoring.
2. Optimize PolicyDS database query with SINGLE_UE_ID_PREFERENTIAL_SEARCH. For more information, see PDS UE ID Configuration.

4.68 Support for Autoenrollment of Subscribers

Policy supports auto provisioning of the subscribers at UDR when the subscriber profile is not present in UDR.

1. When PCRF Core receives a CC-i request, it tries to retrieve the subscriber profile from UDR.
2. If the subscriber profile is not present at UDR, PCRF Core handles the subscriber plan as configured at PCRF Core. The plan is chosen based on MCC-MNC, APN received in the

Copyright © 2019, 2026, Oracle and/or its affiliates.

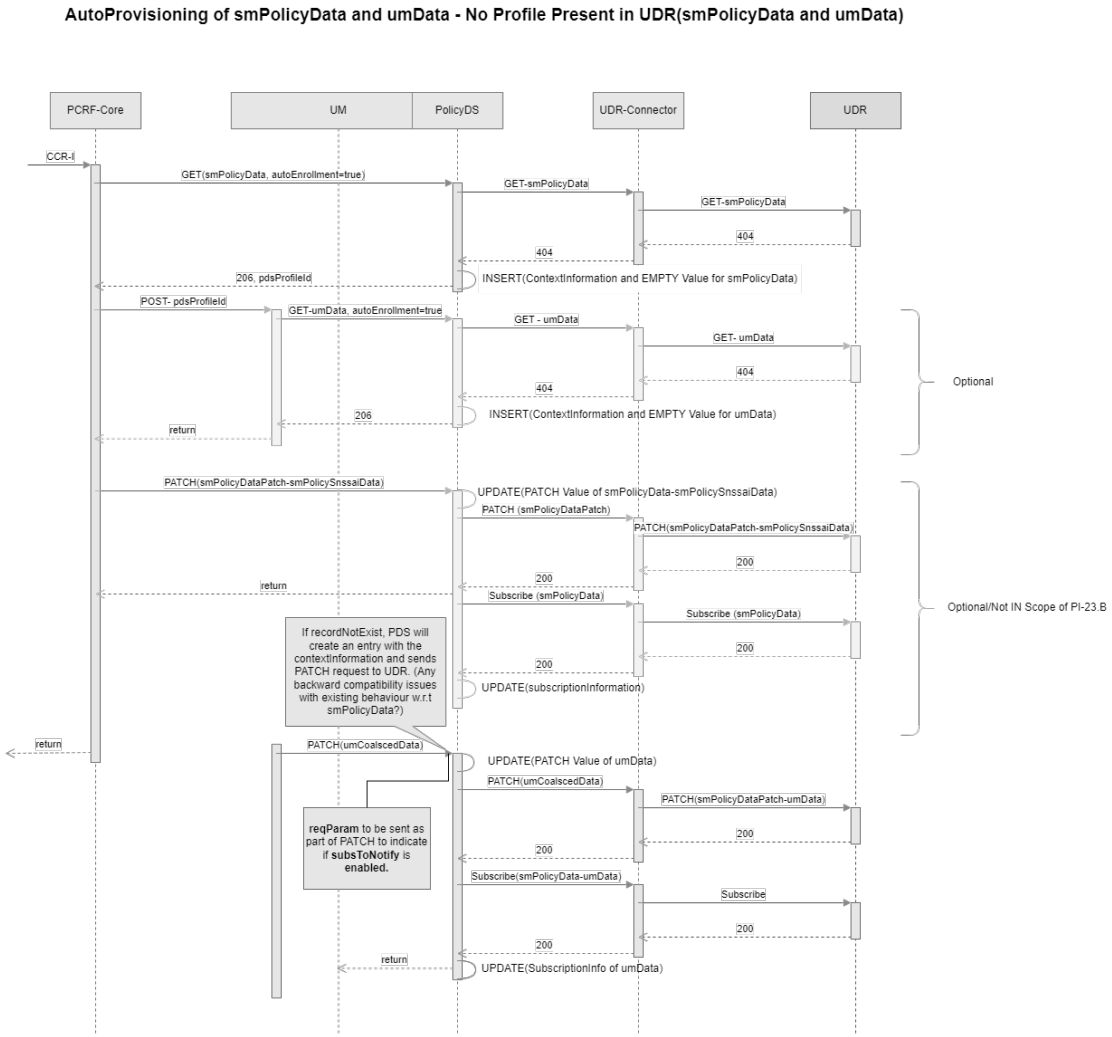
request Message. It applies the right quota to the user and triggers a PATCH towards UDR.

3. A PATCH request is sent to UDR on SM-Data with details of policy-data including UM-Data.
4. UDR triggers auto provisioning of the profile.

Call Flow

The following call flow depicts the scenario when the subscriber profile is not provisioned at UDR.

Figure 4-158 Scenario when user profile is not available in UDR



1. PCRF Core receives a CCR-I request.
2. PCRF Core sends a GET request to PDS with the autoenrollment flag set to *true*.
3. PDS sends the GET request to UDR Connector, which in turn forwards the request to UDR.
4. If the subscriber profile is not present at UDR, UDR responds with a 404 message.

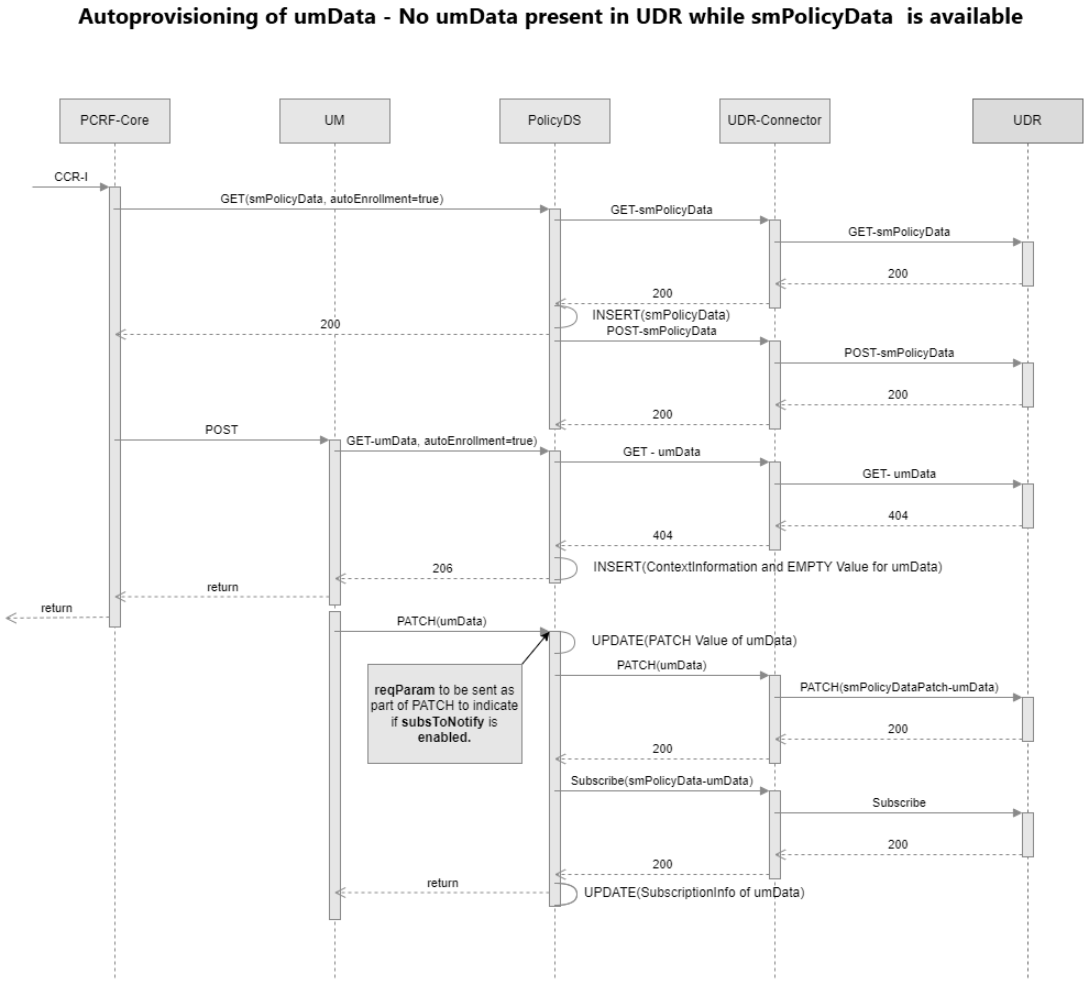
Copyright © 2019, 2026, Oracle and/or its affiliates.

5. UDR connector forwards the error message to PDS.
6. PDS receives the 404 response and then reads the autoenrollment flag. It generates the default SM Policy data and adds the last error code as 404 indicating that UDR sent the 404 error in the same SM Policy data.
7. PDS sends the generated SM Policy data to the core service.
8. Optionally, Usage Monitoring service can send a GET request to PDS requesting for the quota profile.
9. PDS sends the GET request to UDR Connector, which in turn forwards the request to UDR.
10. If the quota profile is not present at UDR, UDR responds with 404 error and UDR connector forwards the 404 error message to PDS.
11. PDS reads the autoenrollment flag and generates a default UMquota with last error code as 404 and sends the data to Usage Monitoring service.
12. The default UM data that is generated at PDS is inserted into the association table with all the context information.
13. The Usage Monitoring service generates quota based on APN, MCC and MNC and sends a PATCH request to PDS.
14. PDS creates an entry in the database and sends this PATCH request to UDR Connector, which in turn forwards the request to UDR.
15. Once the auto provisioning is done at UDR, it responds with a 200 success message.
16. After the PATCH request is successful, PDS sends a subscription request to UDR to subscribe for umData.

The following call flow depicts the scenario when the subscriber profile is provisioned at UDR, but the umData is not provisioned.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-159 Scenario when the subscriber profile is provisioned at UDR, but the umData is not provisioned



1. PCRF Core receives a CCR-I request.
2. PCRF Core sends a GET request to PDS with the autoenrollment flag set to *true*.
3. PDS sends the GET request to UDR Connector, which in turn forwards the request to UDR.
4. If the subscriber profile is present at UDR, UDR responds with a 200 ok message with the subscriber data.
5. UDR connector forwards the message to PDS.
6. PDS sends the SM Policy data to the core service.
7. Optionally, Usage Monitoring service can send a GET request to PDS requesting for the quota profile.
8. PDS sends the GET request to UDR Connector, which in turn forwards the request to UDR.
9. If the quota profile is not present at UDR, UDR responds with 404 error and UDR connector forwards the 404 error message to PDS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

10. PDS reads the autoenrollment flag and generates a default UMquota with last error code as 404 and sends the data to Usage Monitoring service.
11. The default UM data that is generated at PDS is inserted into the association table with all the context information.
12. The Usage Monitoring service generates a quota based on APN, NCC and MNC and sends a PATCH request to PDS.
13. PDS creates an entry in its database and sends this PATCH request to UDR Connector, which in turn forwards the request to UDR.
14. Once the autoenrollment is done at UDR, it responds with a 200 success message.
15. After the PATCH request is successful, PDS sends a subscription request to UDR to subscribe for umData.

Managing the Feature

This section provides information on enabling, configuring, observability and logging for Support for autoenrollment for the subscriber.

Enable

You can enable the support for autoenrollment of the subscribers using CNC Console.

To enable the auto provisioning of the subscriber profile at UDR when the subscriber profile is not available, enable `Auto Enrollment on UDR` parameter for `SmPolicyData` under **User** group in **PCRF Core Settings** page for **Service Configuration**.

For more information, see Settings.

Configure

You can configure the support for autoenrollment of the subscribers using CNC Console.

For more information, see *SmPolicyData* under **User** group in Settings section.

4.69 Support for Subscriber Notification Using SMPP

Policy supports sending subscriber notification (SMS alerts regarding Quota management or usage reporting and activation/deactivation of services) to subscribers through SMPP (Short Message Peer-to-Peer) protocol. This feature enables transfer of short messages between External Short Message Entities (ESME) and Message Centers (MC).

To support notification through SMPP, Policy uses the HTTP notification framework.

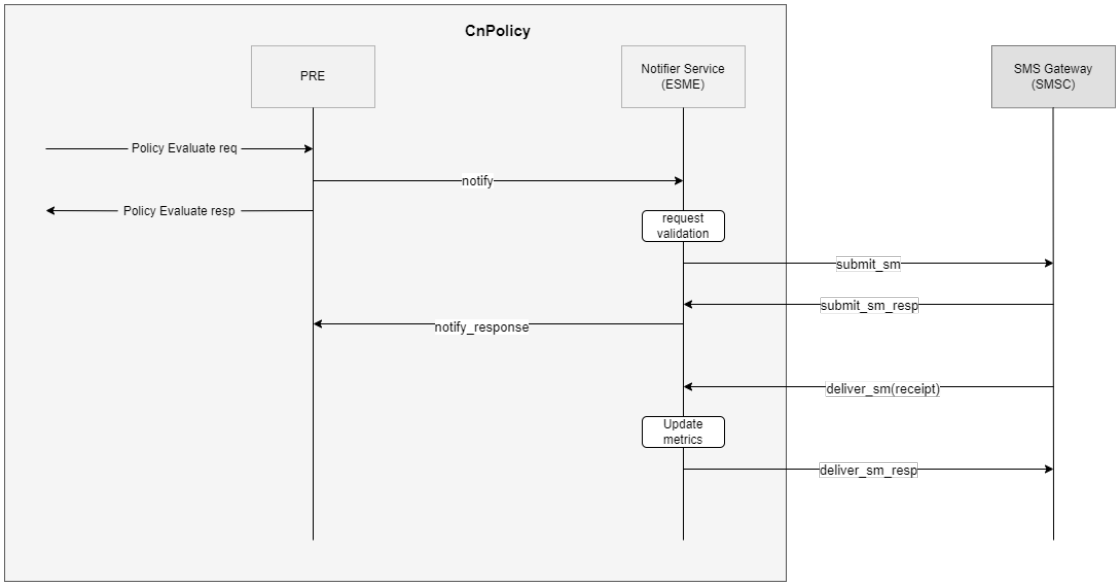
Policy supports this feature using Notifier Service. You must enable the Notifier Service to use this feature. For more information, see Notifier Service.

> **Note**
>
> Currently, this feature is supported only for PCRF-Core call flows.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

Figure 4-160 Call flow for sending messages using SMPP protocol



1. PRE receives a Policy Evaluate request.
2. After the evaluation, PRE sends a notification message to the Notifier Service.
3. Notifier service evaluates the request and sends the notification to SMS Gateway (SMSC).
4. The SMS Gateway acknowledges the notification request.
5. The SMS Gateway sends a delivery receipt to Notifier Service.
6. The Notifier Service acknowledges the delivery receipt to the SMS Gateway.
7. The Notifier Service updates the metrics and then notify response to PRE.
8. PRE sends the Policy evaluation response to the core service.

Managing Support for Subscriber Notification Using SMPP

Enable

User can enable Subscriber Notification through SMPP using CNC Console or REST API for Policy.

- **Enable using CNC Console**: Set the value of **Enable SMPP** parameter to `true` under **Notifier Configurations** page in CNC Console.
  For more information, see Notifier Configurations.
- **Enable using REST API**: Set the value of **smppConfiguration.isEnabled** parameter under **{apiRoot}/oc-cnpolicy-configuration/v1/notifier** API to `true`.
  For more information, see *Notifier Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

User can configure Subscriber Notification through SMPP using CNC Console or REST API for Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Configure using CNC Console**: To configure the Subscriber Notification through SMPP, perform the configurations under **Notifier Configurations**, **Notification Server**, **SMS Gateway Group**, and **SMSC Host Info** pages in CNC Console.
  For more information, see Notifier Configurations.
- **Configure using REST API**: To configure the Subscriber Notification through SMPP use the following REST APIs:
  - To enable and configure the notification through SMPP: **{apiRoot}/oc-cnpolicy-configuration/v1/notifier**
  - To configure the SMS Gateway: **{apiRoot}/oc-cnpolicy-configuration/v1/smsGateway**
  - To configure the SMSC Host Info: **{apiRoot}/oc-cnpolicy-configuration/v1/smsHostInfo**

  For more information, see *Notifier Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observe

The following metrics are added to support the subscriber notification using SMPP:

- `http_in_conn_request_total`
- `http_in_conn_response_total`
- `smpp_request_total`
- `smpp_response_total`
- `active_smsc_conn_count`

For more details on metrics, see Notifier Metrics.

The `SMSC_CONNECTION_DOWN` alert is added to trigger an alarm when the connection to Short Message Service Center (SMSC) Host is down.

For more information, see SMSC_CONNECTION_DOWN.

4.70 Support for Query on Update and Subscription to UDR

PCF uses the Query data procedure to retrieve user data from the UDR, when Policy core services such as SM, AM, or UE receives an update request.

If `queryOnUpdate` and `subscriberToNotify` flags are enabled and an `update` request is received then PCF makes a GET Query request along and Post Subscriber request to the UDR.

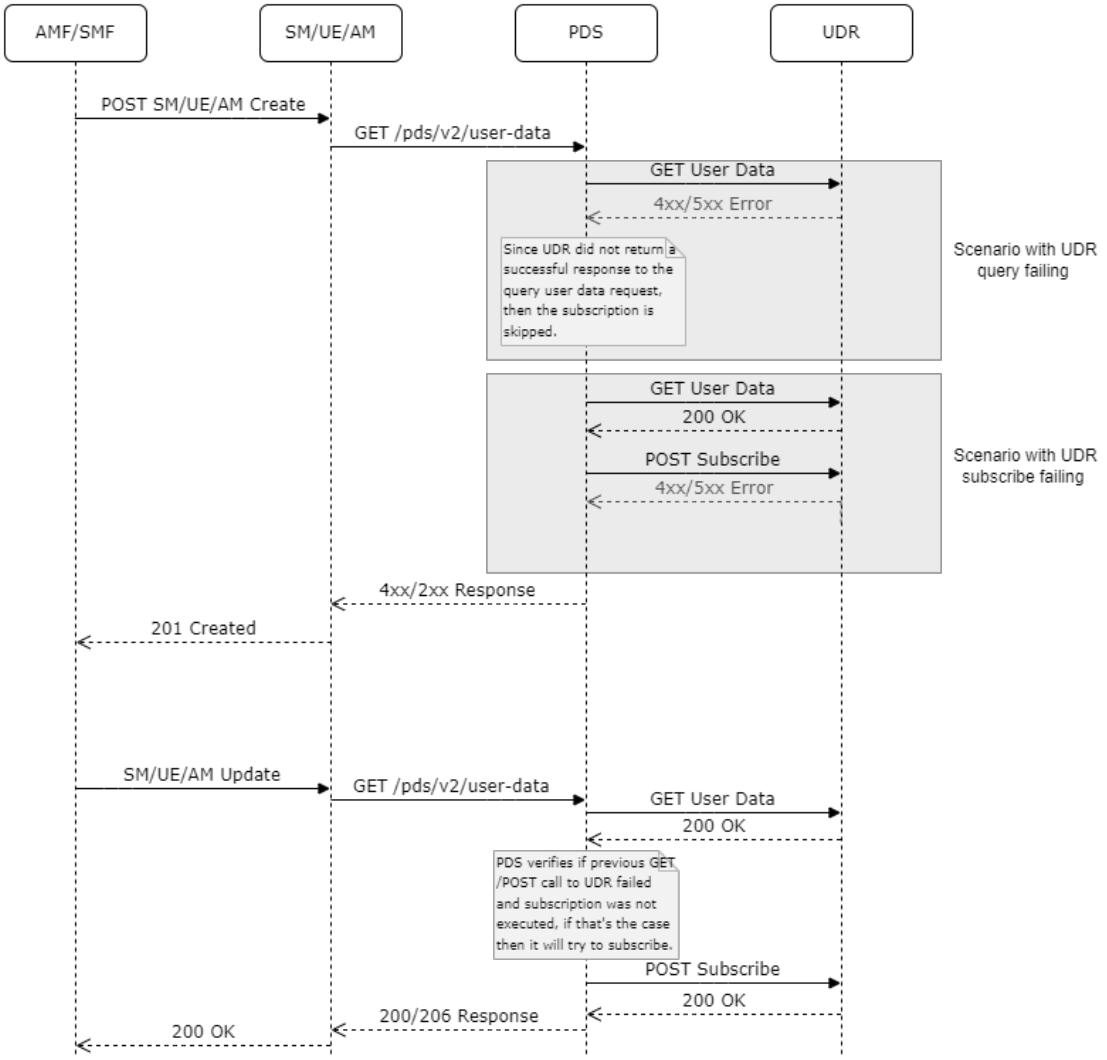
That is,

- Policy should query and subscribe to UDR during Update request if `subscribeToNotify` and `queryOnUpdate` flags are enabled and the previous GET or POST requests failed (could be in the Create request or a previous Update request).
- Policy should not query UDR once GET or POST request is successful and subscription is successful.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

Figure 4-161 Retrieving user data from UDR upon a GET or Update request to a Policy Service



1. Policy Service (SM Service/ AM Service/ UE Policy Service) receives a create request from SMF/AMF.
2. Policy Service sends a request to PDS to get the user data.
3. PDS sends a GET request to UDR to retrieve the data.
4. If the user data does not exist, UDR responds with an error and subscription to user data from UDR is also not performed.
5. If the user data is found, UDR responds with a 200 OK message.
6. PDS sends a POST Subscription to UDR to subscribe for any update to the user data.
7. The respective Policy service (SM Service/ AM Service/ UE Policy Service) creates an association for the request and responds to SMF/AMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8. When the Policy service (SM Service/ AM Service/ UE Policy Service) receives an update request from SMF/AMF, the service do not send a GET request to PDS to retrieve the user data from UDR with `queryOnUpdate` and `subscribeToNotify` flags are enabled.
9. PDS sends the GET request to UDR and receives a 200 OK response.
10. If the previous GET or POST Subscription request to UDR has failed, PDS sends a POST subscription request to UDR once again to subscribe for notification on any update to user data in UDR.
11. PDS forwards the successful response to the respective Policy Service (SM Service/ AM Service/ UE Policy Service), which in turn forwards the response to SMF/AMF.

PDS Handling Subscription Failure from UDR

If UDR subscription fails with subscribeToNotify flag enabled, the user must configure the following advanced settings keys under PDS Settings page on CNC Console to reattempt the subscription call on next SM update.

- NOTIFY_PCF_SM_ON_SUBSCRIPTION_FAILURE
- SUBSCRIPTION_FAILURE_NOTIFICATION_DELAY
- SUBSCRIPTION_FAILURE_NOTIFICATION_RETRY_COUNT
- SUBSCRIPTION_FAILURE_NOTIFICATION_RETRY_DELAY

For more information, see PDS Settings.

> **Note**
>
> In this case, queryOnUpdate flag for SM Service must be set to false.

With these configurations, PCF sends the subscription request towards UDR on receiving subscription failure notification from SM service.

> **Note**
>
> For AM and UE Policy services, UDR subscription request is reattempted using queryOnUpdate flag.

If PDS receives 404 status code from UDR, it performs user-level clean up for core services and session-level clean up for Pcrf-Core.

When re-validation and resetContext flags are set to false and the request is same for the existing context without the subscription information and the fetch request from the data source is successful, PDS updates the database with subscriber and context information.

The core services (SM, UE, or AM services) have flags to persist subscription failure. The flag is set to false when GET operation is performed and set to true when subscription failure notification is received from PDS.

A new property called "subscriptionFailure" is added to the JSON schema of SmPolicyAssociation. This property holds an integer value, whether there is a subscription failure or not. This property value is determined by setting some specific bits in the integer number. The following table shows which bit specifies the type of data subscription failure:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-127 SmPolicyAssociation Data Type

Data Type	Bit Number
smData	1
operatorSpecificData	2

Managing the Query on Update feature

Enable

You can enable the Query on Update feature using CNC Console or REST API for Policy.

- **Enable using CNC Console**:
  - To enable the feature for SM Service, set the value of **Query User on Update** parameter to `true` under **User** group on **PCF Session Management** page.

    For more information, see PCF Session Management.
  - To enable the feature for AM Service, set the value of **Query User on Update** parameter to `true` under **User** group on **PCF Access and Mobility** page.

    For more information, see PCF Access and Mobility.
  - To enable the feature for UE Policy Service, set the value of **Query User on Update** parameter to `true` under **User** group on **PCF UE Policy Service** page.

    For more information, see PCF UE Policy Service.
- **Enable using REST API**:
  - Set the value of **queryUserOnUpdate** parameter under **{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm** API to `true`.

    For more information, see *Session Management Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.
  - Set the value of **queryUserOnUpdate** parameter under **{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam** API to `true`.

    For more information, see *Access and Mobility Service* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.
  - Set the value of **queryUserOnUpdate** parameter under **{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfue** API to `true`.

    For more information, see *UE Policy* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the Query on Update feature using the CNC Console or REST API for Policy.

- **Configure using CNC Console**: To configure Query on Update feature for SM Service, AM Service and UE Policy service, perform the feature configurations under the User group on the respective service configurations page. For more information, see the following sections:
  - PCF Session Management
  - PCF Access and Mobility
  - PCF UE Policy Service

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Configure using REST API**: Policy provides the following REST API to configure the Query on Update feature:
  - **{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm**
  - **{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam**
  - **{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfue**

Observe

The following PDS metrics provide the information about query on update feature:

- server_request_total
- server_response_total

For more information, see Policy DS Metrics.

4.71 Support for Presence Reporting Area

PCF supports the Presence Reporting Area (PRA) functionality to comply with the 3GPP standards.

Policy supports PRA functionality for SM Service, AM Service and UE Policy Service.

The Presence Reporting Area is an area defined within the 3GPP packet domain for reporting the presence of UE within that area. This is required for policy control and in charging scenarios. In E-UTRAN, the PRA can consist in a set of neighbor or non-neighbor Tracking Areas, or eNBs or cells.

There are two types of Presence Reporting Areas:

- UE-dedicated Presence Reporting Areas: Defined in the subscriber profile and composed of a short list of TAs and/or NG-RAN nodes and/or cells identifiers in a PLMN.
- Core Network pre-configured Presence Reporting Areas: Predefined in the AMF and composed of a short list of TAs and/or NG-RAN nodes and/or cells identifiers in a PLMN.

If the PRA feature is supported and SMF or AMF receives the PRA information from the serving node indicating any of the following:

- the UE is inside or outside of one or more PRAs
- any of the presence reporting areas is set to inactive

the SMF or AMF checks if the reported PRA identifier corresponds to a PRA that is relevant for the PCF. In that case, the SMF or AMF within the `SmPolicyUpdateContextData` or `AmPolicyUpdateContextData` or `UEPolicyUpdateContextData` data structure includes the `PRA_CH` within the `repPolicyCtrlReqTriggers` attribute and one or more PRA information report within the `repPraInfos` attribute. For each `PresenceInfo` data structure, the SMF or AMF includes the PRA status within the `presenceState` attribute and the PRA identifier within the `praId` attribute for each of the presence reporting areas reported by the serving node.

If the SMF or AMF receives additional presence reporting area information along with the PRA Identifier, the SMF or AMF only provides the PCF with the presence reporting area information corresponding to the additional PRA information.

- The SMF or AMF receives additional presence reporting area information when the UE enters or leaves one or more presence reporting areas related to a PRA set. In that case, the additional presence reporting area information corresponds to the actual individual presence reporting area. The received presence reporting area identifier corresponds to

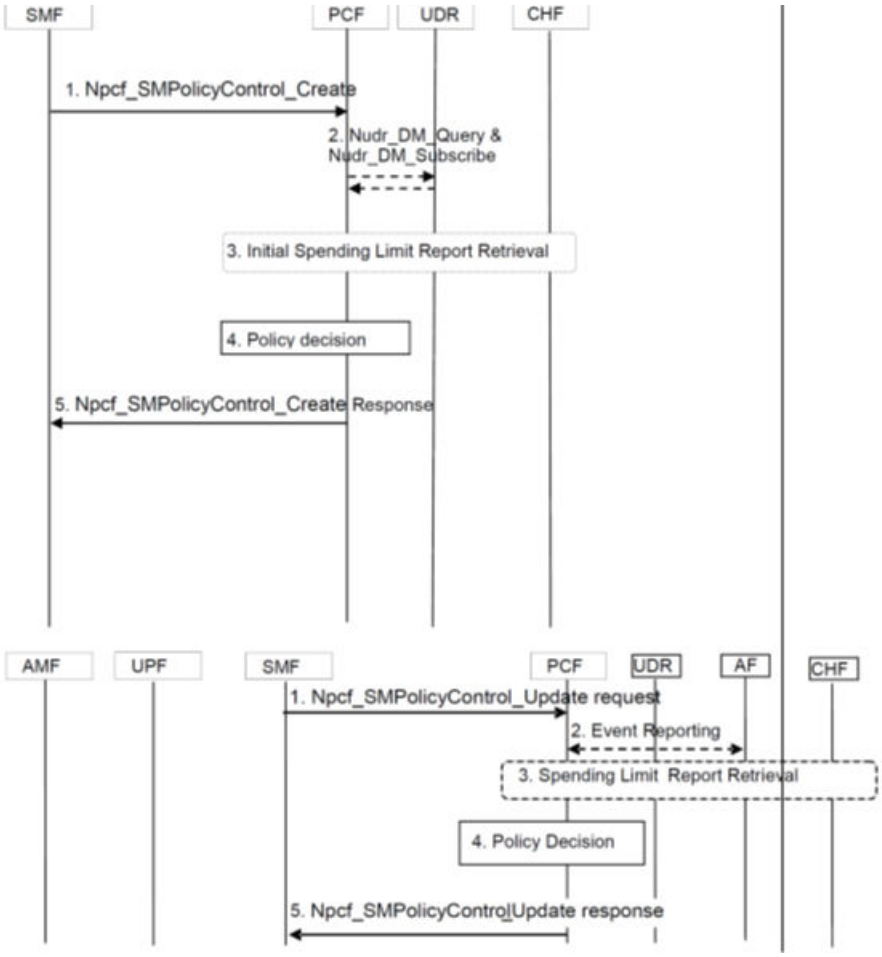
Copyright © 2019, 2026, Oracle and/or its affiliates.

the PRA set ID and is used to identify the requester (PCF or CHF) of the notification information.

- PCF can acquire the necessary data for presence reporting from the UDR.
- Homogeneous support of PRA in a network is assumed.
- The serving node can activate the reporting for the PRAs which are inactive as described in the 3GPP TS 23.501 [2].

The following figure shows a call flow for PRA functionality for SM Service:

Figure 4-162 PRA Support for SM Service



The call flow is described as follows:

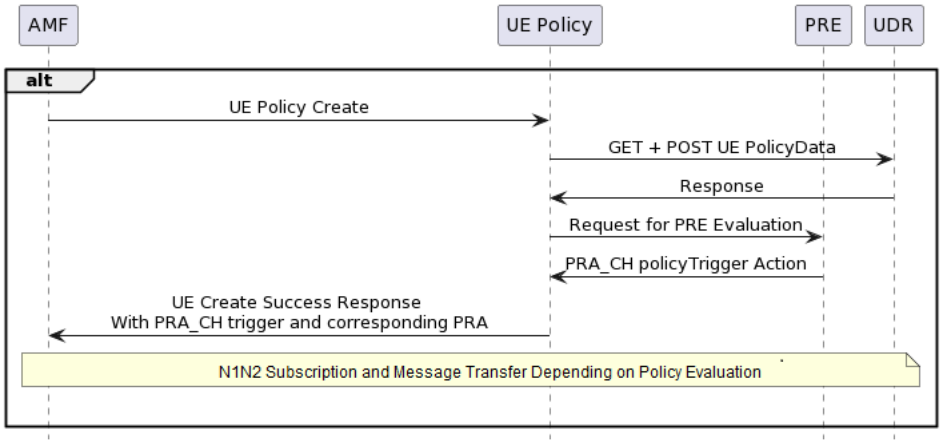
1. UE initiates a PDU session establishment request.
2. SMF sends an *Npcf_SMPolicyControl_Create* request message to PCF to establish an SM policy control correlation including the PDU session related information.
3. PCF completes the policy calculation based on the policy configuration and subscription information and user information. The PCF sends an *Npcf_SMPolicyControl_Create* response message to the SMF, including an SM policy and PRA information. The PRA type can be either UE-dedicated PRA or Set of Core Network PRA.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Currently, UE-dedicated PRA is not supported for SM Service.

4. When the user changes across the PRA, the SMF sends an *Npcf_SMPolicyControl_Update* request message to PCF to modify the SM policy control correlation, and report the change in location of the user to the PCF. The message contains the information related to change of UE presence in Presence Reporting Area.
5. The PCF sends an *Npcf_SMPolicyControl_Update* response message to the SMF, including the updated SM policy.

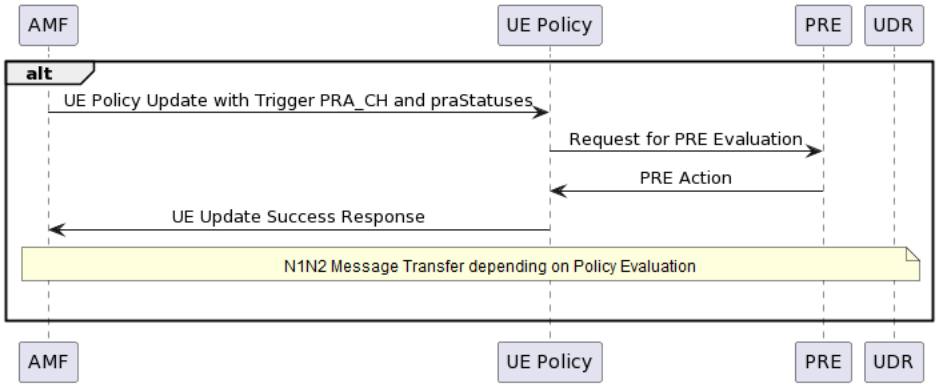
Figure 4-163 UE Policy Association create scenario:



1. UE Policy Service receives a UE Policy Association create request from AMF.
2. UE Policy Service sends a GET request to PDS along with a POST subscribe to fetch the user data from UDR.
3. PDS sends the request to UDR via the UDR Connector.
4. UDR responds with the user data as well as the triggers for UE location change and PRA change.
5. PDS forwards the details to UE Policy Service.
6. UE Policy Service sends the details to PRE for evaluation.
7. PRE evaluates and installs the PRA successfully.
8. If there is a Policy Evaluation that requires N1/N2 Policy transfer, AMF subscribes and transfers N1N2 messages.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-164 UE Policy Association update scenario



1. UE Policy Service receives a UE update request from AMF which includes the UE Policy update along with PRA_CH and praStatuses.
2. UE Policy service sends the updates to PRE for evaluation.
3. PRE evaluates the details and triggers the appropriate action on the PRA. '
4. UE Policy Service responds to AMF with a UE Policy update successful message.
5. If there is a Policy Evaluation that requires N1/N2 Policy transfer, AMF transfers N1N2 messages.

Managing Presence Reporting Area

Enable

The PRA functionality is a part of Policy configurations. You do not need to enable or disable this feature.

Configure

You can add new PRAs and configure the them using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the configurations on the **PCF Presence Reporting Area** page. For more information about configuring PRAs, see PCF Presence Reporting Area.
- **Configure using REST API:** Policy provides the following REST API for PRA configuration:
  API: {apiRoot}/ocpm/pcrf/v1/configuration/policy/pra

  You can perform the POST, PUT, or GET operations to configure the PRA feature. For more information about REST API configuration, see "PRA" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.72 Handling Install and Remove Conflict for Same Rule

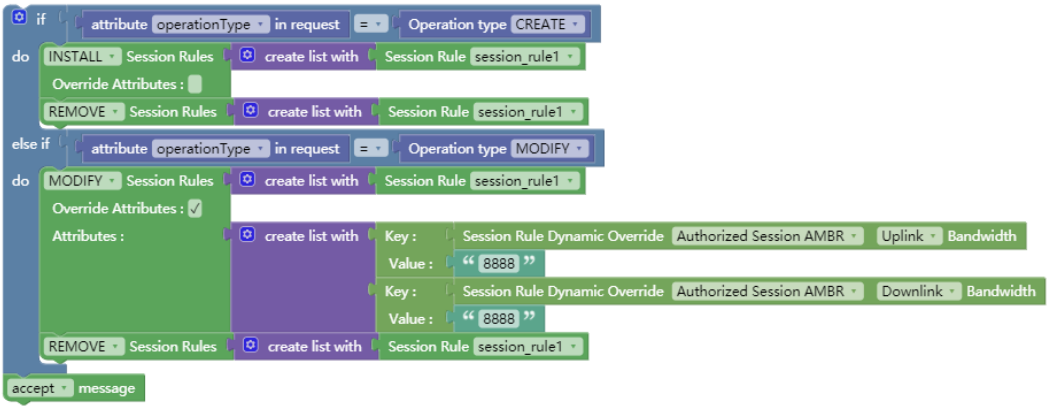
This section describes a high-level design of the Conflict Resolution of INSTALL and REMOVE actions on the same PCC/Session Rules when the remove action is **Remove** (ALL, Predefined, Dynamic, Conditioned, non-conditioned) in the policy project.

Copyright © 2019, 2026, Oracle and/or its affiliates.

In certain policies, install/update and remove actions are applied for the same rule - which can be either a session rule or a PCC rule.

The following screen capture illustrates a policy to show conflicts in same session rule. In this example, the install, update, and remove actions are applied to the same session rule, that is, session_rule1:

Figure 4-165 Example of Policy with Conflicts in a Session Rule



In previous releases, after executing a similar policy, SM service would remove the rule. However, with this feature, PCF is enhanced to configure the precedence and resolve the conflicting install and remove actions on the same rule.

When SM service receives two action types, such as install and remove for the same rule, SM service processes the remove action for the first rule, and then installs it. However, if install is not configured for the rule, SM service can remove it.

Policy allows its users to select how to resolve such conflicts in the most suitable manner by using the `Install/Remove Rule Conflicts Strategy` parameter under PCF Session Management service configurations.

Managing Install/Remove Rule Conflicts Handling

Enable
The Handling Install/Remove Rule Conflicts is the core functionality of Policy configurations. You do not need to enable or disable this feature.

Configure
You can configure the managing Rule conflict functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Set value of the **Install/Remove Rule Conflicts Strategy** parameter under the **Rule** group on the PCF Session Management page. For more information, see configurations for **Rule** in PCF Session Management.
- **Configure using REST API:** Policy provides the following REST API for Install/Remove Rule Conflicts configuration:
  API: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm

  Set value of the **ruleConflictsStrategy** parameter in the **Session Management Service** API. For more information about REST API configuration, see Rule Configurations of the

Copyright © 2019, 2026, Oracle and/or its affiliates.

"Session Management Service" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.73 Diameter Session Retry

In PCF, diameter connector sends the request messages such as Rx RAR (Re-Authorization Request) or Rx ASR (Abort Session Request) via the diameter gateway to Application Function (AF). AF acknowledges these commands by sending a successful or failed messages Re-Authorization Answer (RAA) or Abort Session Answer (ASA) respectively to PCF.

The RAA or ASA messages answers when received with protocol errors such as 3002 (DIAMETER_UNABLE_TO_DELIVER) or 3004 (DIAMETER_TOO_BUSY) or session timeout, the operator would want to retry sending the same Rx RAR or Rx ASR diameter messages from PCF to AF through a different or an alternate BSF (Binding Support Function) or DRA (Diameter Routing Agent).

The Diameter Message Retry for Rx RAR and Rx ASR diameter messages is enabled through the Error Mapping Framework feature in the diameter gateway service. This framework resolves application errors and takes necessary action based on the error context. The error handler framework tries to find an alternate solutions based on the configurations set in CNC Console. If the error is resolved, it sends back the success result to the caller, else it either retries based on the configured maximum resolution attempts number or terminates by forwarding the last known error.

The operator should have configured a host and realm for retry of failed diameter messages in the diameter routing table. Diameter Gateway finds the alternate peer from the routing table. If the diameter routing table is not configured then there is no retry behavior from policy.

> **Note**
>
> Default number of retry attempts is one, when the alternate peers are available. If alternate peers are not available, no retry attempt is made.

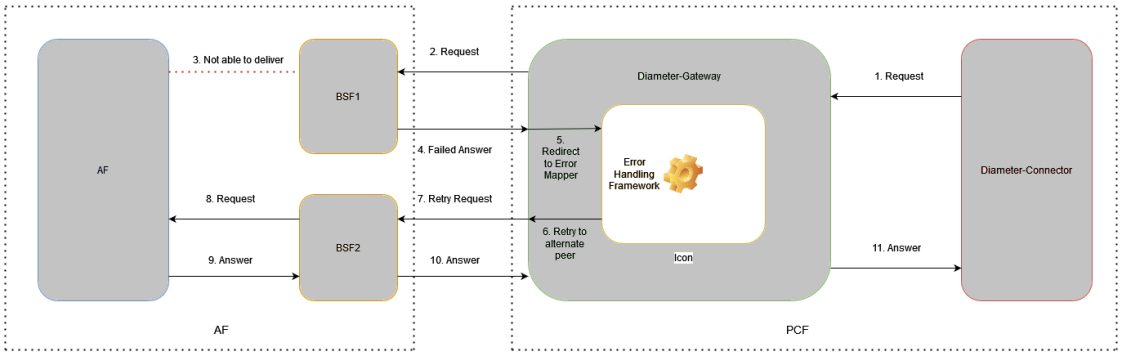
PCF retries resending Rx-RAR and Rx-ASR diameter messages for the following configurable error code series:

- 3xxx (Protocol Errors)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failure)

For more information about these error codes refer to Diameter Error Codes feature section.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-166 The block diagram represents the diameter Rx RAR and Rx ASR message flow with a retry:



The block diagram represents the diameter Rx RAR and Rx ASR message flow with a retry using the Error Handler Framework in Policy.

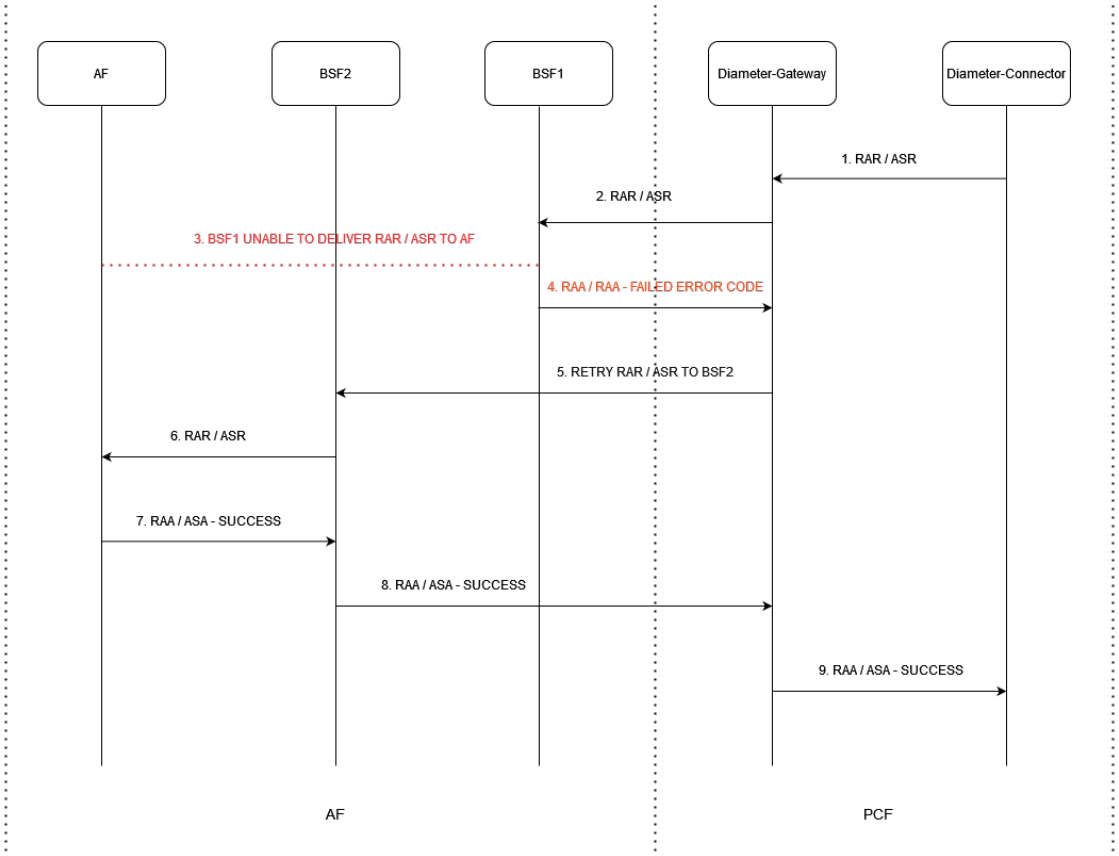
1. The diameter connector sends the diameter request and the diameter gateway receives the diameter request.
2. The diameter gateway forwards this diameter request to available BSF1 based on routing table and priority.
3. The BSF1 is not able to deliver this message to AF due to some reason.
4. The diameter gateway receives the failed diameter answer from the BSF1 then it redirects the request context to Error Handler.
5. Error Handler gets the request context from the failed diameter request and finds the alternate retry action configured.
6. The Error Handler provides the retry action for the same request to next available alternate BSF2.
7. The diameter gateway sends the retry diameter request to next alternate BSF2.
8. BSF2 sends the retry request to AF.
9. AF sends the answer to BSF2 back.
10. BSF2 sends the answer to diameter gateway.
11. The diameter gateway forwards the answer received from BSF2 to the diameter connector.

Session Retry Call Flows

The following call flow describes a successful transmission of Rx RAR or Rx ASR message to AF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-167 Call Flow Rx RAR or Rx ASR one time message retry - Success Case:

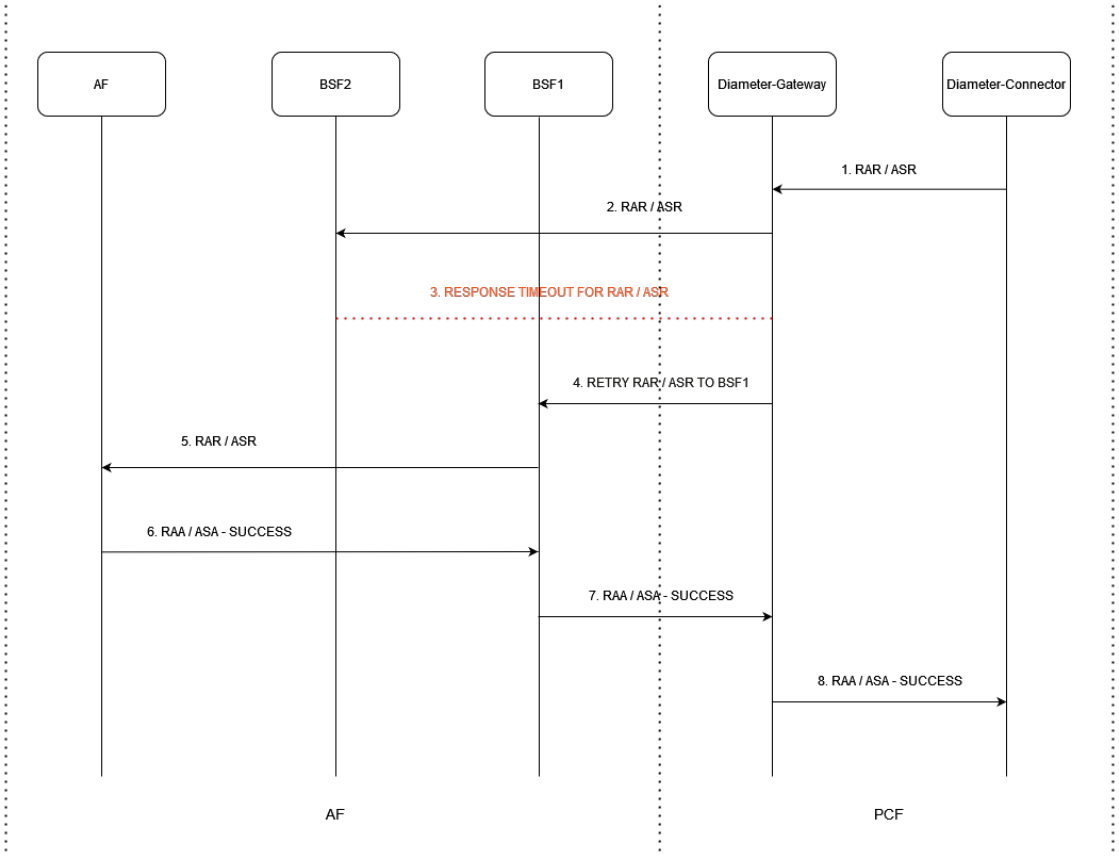


1. Diameter connector sends RAR or ASR request to diameter gateway.
2. Diameter Gateway sends the request to the available BSF, here to BSF1.
3. BSF1 is unable to deliver the RAR or ASR message to AF.
4. BSF1 returns a failed RAA or ASA message along with an error code to diameter gateway.
5. Diameter Gateway interprets the error code, and retries to send the failed message to the next available BSF, here BSF2 gets the message.
6. BSF2 sends the RAR or ASR message successfully to AF.
7. AF returns successful RAA or ASA message response to BSF2.
8. BSF2 sends this successful response to diameter gateway.
9. Diameter Gateway sends this response to diameter connector.

The following call flow describes a successful retry in case of a response timeout for Rx RAR or Rx ASR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-168 Call Flow RX RAR or RX ASR Timeout Retry - Success Case:



1. Diameter connector sends RAR or ASR request to diameter gateway.
2. Diameter Gateway sends the request to the available BSF, here to BSF1.
3. BSF1 is unable to deliver the RAR or ASR message to AF.
4. BSF1 returns a failed RAA or ASA message along with an error code to diameter gateway.
5. Diameter Gateway interprets the error code, and retries to send the failed message to the next available BSF, here BSF2 gets the message.
6. BSF2 sends the RAR or ASR message successfully to AF.
7. AF returns RAA or ASA message successful response to diameter gateway.
8. Diameter Gateway sends this response to diameter connector.

Retry Attempts

The user can choose to configure the number of retries to find a Peer for sending the Rx-RAR and Rx-ASR diameter messages. This retries is possible only when the alternate peers are available, that is, the Peer is alive, if it is not available, that is, the Peer is not alive then there is no retry attempt made. The default number of retry attempts is 1. The number of retry value can be any positive number between 1 to 2147483647.

The number of retries can be set through the advance settings configurations using the following advance setting keys:

- DIAMETER.ErrorHandler.MaxRetryCount.Rx.RAR

Copyright © 2019, 2026, Oracle and/or its affiliates.

- DIAMETER.ErrorHandler.MaxRetryCount.Rx.ASR

If the above advance settings configurations are not supported in the CNC Console, then the default retry attempt is 1. If retry attempt value configured is a zero or negative number, then the default retry attempt value shall be considered.

Peer Cycle Back Retry

The user can choose to perform Peer retry in a cyclic manner if the number of retries configured is more than the number of alternate peers available for both Rx RAR and RX ASR message retries. This retries is possible only when the alternate peers are available, that is, the Peer is alive, if it is not available, that is, the Peer is not alive, then there is no retry attempt made. The user configures this in CNC Console by setting `retry peer cycle back` field to true.

This peer cycle back retry configuration is performed using the following advance setting keys:

- DIAMETER.ErrorHandler.CycleBackRetry.Rx.RAR
- DIAMETER.ErrorHandler.CycleBackRetry.Rx.ASR

If above advance settings configurations are not supported in the CNC Console, then the default peer cycle back retry is false.

Described below are the scenario that shows how the Diameter message retry mechanism works.

For example 1: Consider, the number of configured retries is 2 and only 2 BSF/DRA are configured as alternate peers in PCF. Both the peers are alive.

- The Rx RAR message is sent via (PCF-1) - (BSF1/DRA1) - (PCSCF-1) but the response has failed with error code 5012/timeout/3002/3004
- Then the message is resent (retry 1) via (PCF-1) - (BSF2/DRA2) - (PCSCF-1) but the response has failed with error code 5012/timeout/3002/3004.
- Then the message is resent (retry 2) again via (PCF-1) - (BSF1/DRA1) - (PCSCF-1) but the response has failed with error code timeout.

During the second time, the message is resent using the first peer again as only 2 BSF/DRA are available and alive, and peer cycle back retry mechanism is applied.

For example 2: Consider that the number of configured retries is 3 and only 2 BSF/DRA are configured as alternate peers in PCF and just one of the Peer BSF/DRA is alive.

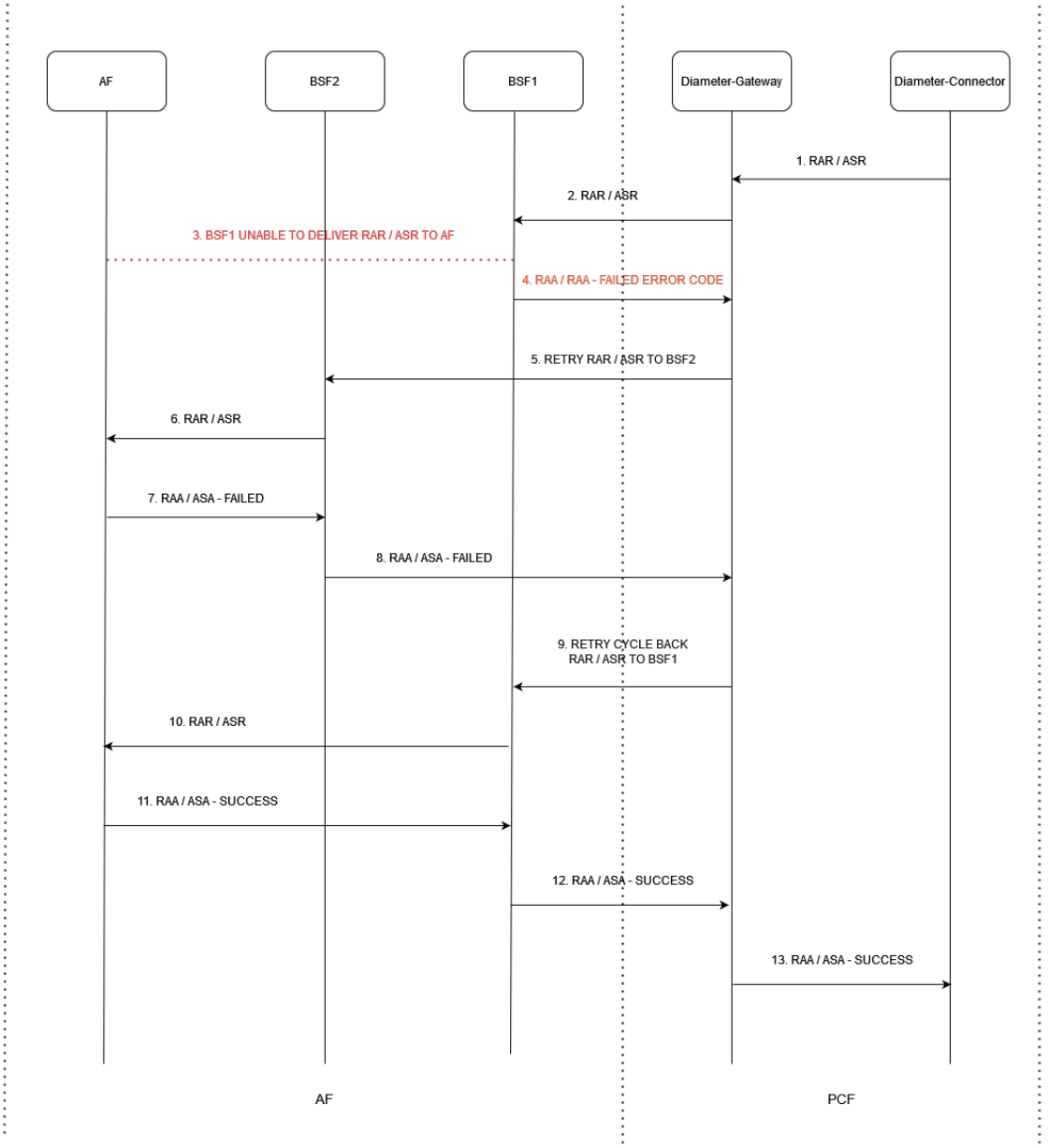
- The Rx RAR message is sent via (PCF-1) - (BSF1/DRA1) - (PCSCF-1) but the response has failed with error code 5012/timeout/3002/3004
- Then the message is resent (retry 1) via (PCF-1) - (BSF1/DRA1) - (PCSCF-1) but the response has failed with error code 5012/timeout/3002/3004.
- Then the message is resent (retry 2) again via (PCF-1) - (BSF1/DRA1) - (PCSCF-1) but the response has failed with error code timeout.

The message is resent 3 times through the same peer as only one BSF/DRA is alive, and cycle back retry mechanism is applied

The following call flow describes the peer cycle back retry when the number of retry count is higher than the alternate peers available.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-169 RX RAR/RX ASR Retry - Peer Cycle Back When Retry Count > Alternate Peers



1. Diameter connector sends ASR or RAR request to the diameter gateway
2. Diameter Gateway sends the request to the available BSF, here to BSF1.
3. BSF1 is unable to deliver the RAR or ASR message to AF.
4. BSF1 returns a failed RAA or ASA message along with an error code to diameter gateway.
5. Diameter Gateway tries to resend the failed message to the next available BSF, here BSF2 gets the message.
6. BSF2 sends the RAR or ASR message successfully to AF.
7. AF responds with failed RAA/ASA response to BSF2.
8. BSF2 sends the failed RAA/ASA response to diameter gateway.

Copyright © 2019, 2026, Oracle and/or its affiliates.

9. At Diameter Gateway, if retry cycle back is enabled, then it resend the RAR or ASR message back to BSF1.
10. BSF1 sends the RAR or ASR message successfully to AF.
11. AF returns RAA or ASA message successful response to BSF1.
12. BSF1 returns RAA or ASA message successful response to diameter gateway.
13. Diameter Gateway returns RAA or ASA message successful response to diameter connector.

Error Originator Peer

The Error Originator Peer indicates the peer host where the Rx RAR or Rx ASR failed message error occurred/originated while sending or retry sending the Diameter messages. The user can customize the error origination peer by using `Error Originator` field in the CNC Console and the customizing options are based on:

- An error received from an intermediate peer (INTERMEDIATE PEER).
- An error received from the destination peer, which is not an intermediate peer (DESTINATION PEER).
- An error received from any peer (ANY).

An intermediate peer is BSF/DRA and a destination peer (not intermediate peer) is P-CSCF.

By default, the error originator peer option is any peer. If multiple error originator peers are configured for the same error code, then the first priority error originator configurations, applies for the response failures.

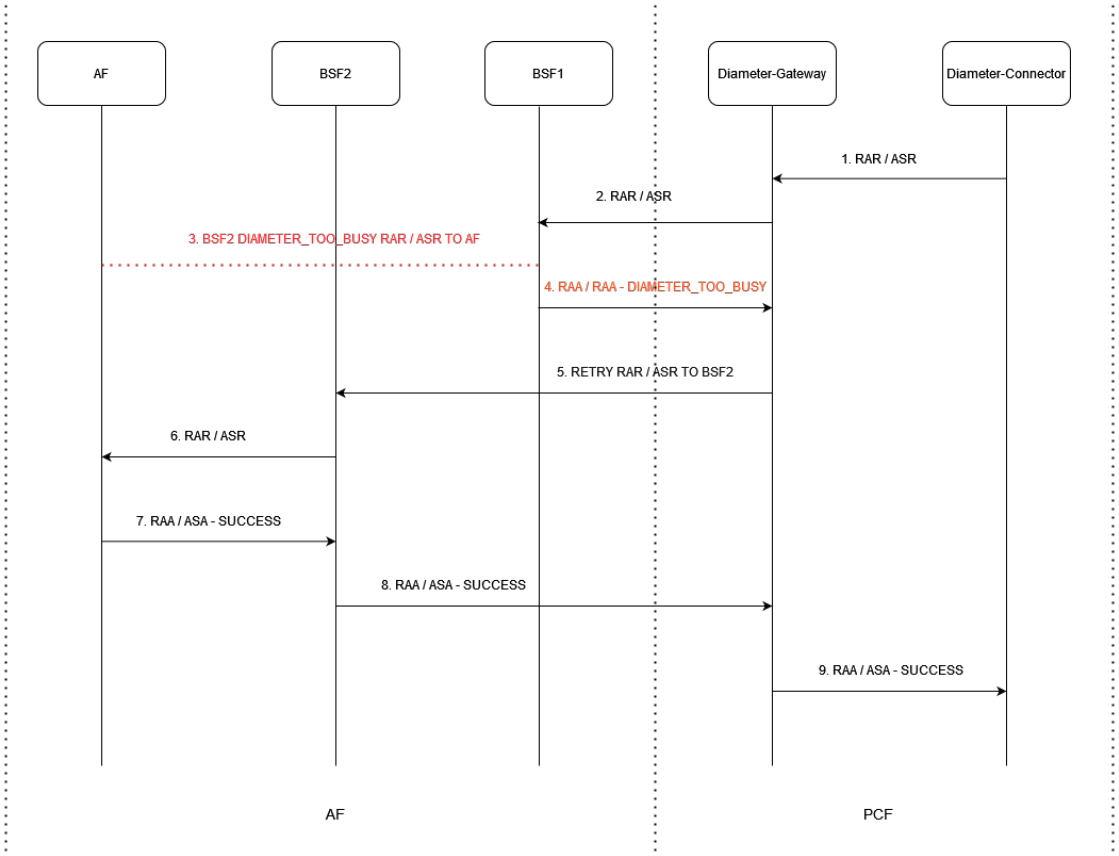
In case of response timeout, the error originator would be considered based on:

- The destination host in RAR/ASR is af.xxx.com. If message is sent to bsf.xxx.com and if response timeout happens, then it is considered as error originated from intermediate peer.
- The destination host in RAR/ASR is af.xxx.com. If message is sent to af.xxx.com and if response timeout happens, then it is considered as error originated from destination peer.

The following call flow describes the error origination by intermediate peer.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-170 RX RAR/RX ASR Retry - Error Originated by Intermediate Peer

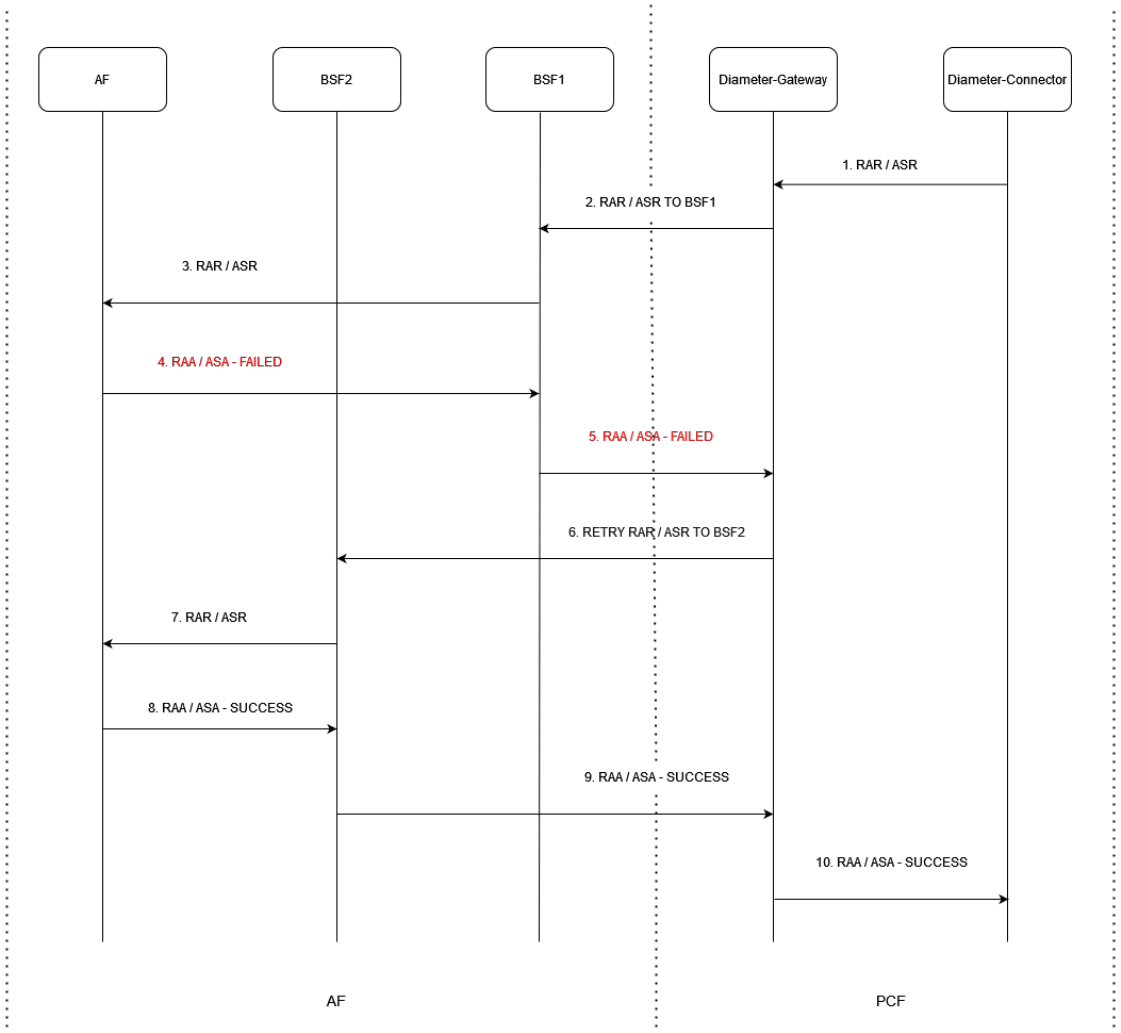


1. Diameter connector sends ASR or RAR request to the diameter gateway.
2. Diameter Gateway sends the request to the available BSF, here to BSF1.
3. BSF1 gets DIAMETER TOO BUSY error.
4. BSF1 forwards this error to diameter gateway.
5. Diameter Gateway retries sending this failed message through BSF2.
6. BSF2 sends this message to AF.
7. AF returns RAA or ASA message successful response to BSF2.
8. BSF2 returns RAA or ASA message successful response to diameter gateway.
9. Diameter Gateway returns RAA or ASA message successful response to diameter connector.

The following call flow describes the error origination by destination peer (not intermediate peer).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-171 RX RAR/RX ASR Retry - Error Originated by Destination Peer (Not Intermediate Peer)



1. Diameter connector sends ASR or RAR request to the diameter gateway.
2. Diameter Gateway sends the request to the available BSF, here to BSF1.
3. BSF1 sends the RAR or ASR message successfully to AF.
4. AF (Destination Peer) sends the failed RAA/ASA response to BSF1.
5. BSF1 sends the failed RAA/ASA response to diameter gateway.
6. Diameter Gateway retries sending this failed message through BSF2.
7. BSF2 sends this message to AF.
8. AF returns RAA or ASA message successful response to BSF2.
9. BSF2 returns RAA or ASA message successful response to diameter gateway.
10. Diameter Gateway returns RAA or ASA message successful response to diameter connector.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Default Error Handling Configuration

PCF provides the default error handling configuration to attempt diameter session retry on all error codes (except diameter result code 2xxx) and timeout for Rx RAA and Rx ASA failed diameter messages. When the diameter message retry feature is enabled on Rx interface, these default error handling configurations get applied by default. The user has an option to enable/disable these default configurations through the CNC Console edit configurations.

The error configuration consists of error state and error cause. Error state, a mandatory parameter provides the details about the error that occurred. Error cause, a optional parameter provides additional information on the error occurred such as sub-status, error message. The error configuration can be assigned a priority of evaluation in case the error matches with more than one error state.

For all default error handling configurations, the value for retry attempt is 1 and peer cycle back retry is false. The number of retry value can be any positive number between 1 to 2147483647.

> **Note**
>
> If retry attempt value configured is a zero or any negative number, then the default retry attempt value shall be considered.

A sample default configuration looks like:

- Message - Rx-RAR, Status code - ANY (except 2001)
- Message - Rx-ASR, Status code - ANY (except 2001)
- Message - Rx-RAR, Status code - ANY, Error Cause Message - TIMEOUT_EXCEPTION
- Message - Rx-ASR, Status code - ANY, Error Cause Message - TIMEOUT_EXCEPTION

Managing Diameter Session Retry

This section explains the procedure to enable and configure the feature.

Enable

By default, Diameter Message Retry behavior is disabled for Rx interface and operator can enable this feature through the CNC Console configurations.

Configure Using CNC Console

Perform the feature configurations in CNC Console as described in Error Configurations section.

To enable over-writing of destination host on retry message, `DIAMETER.ErrorHandler.Enable.UpdateDestinationHost` key must be set to **true** in the Advanced Settings. For more information, see Settings.

Configure Using REST API

Perform the export/import error configurations as described in "Error Configurations" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Document*

Observability

Metrics

Following metrics were updated in the Diameter Gateway Metrics section:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- occnp_diam_request_local_total
- occnp_diam_request_network_total
- occnp_diam_request_inter_total

Alerts

Following alerts are used by this feature:

- RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
- RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
- RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
- ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
- ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
- ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Maintain
If you encounter alerts at system or application levels, see Alerts section for resolution steps.

In case the alerts still persist, perform the following:

- Collect the logs: For more information on how to collect logs, see *Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide*.
- Raise a service request: See My Oracle Support for more information on how to raise a service request.

4.74 Monitoring the Availability of SCP using HTTP2 OPTIONS

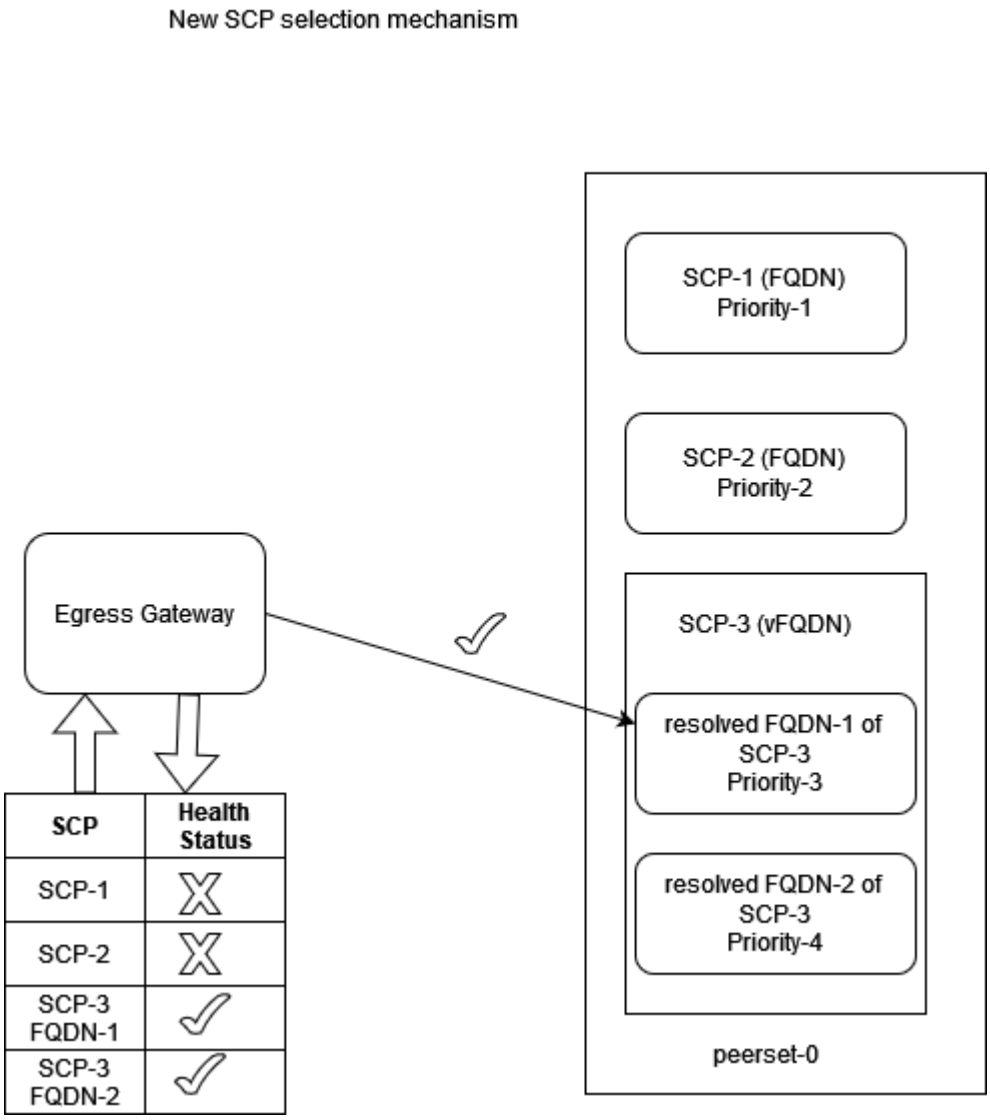
Policy determines the availability and reachability status of all SCPs irrespective of the configuration types.

This feature is an enhancement to the existing SBI routing functionality. Egress Gateway microservice interacts with SCP on their health API endpoints using HTTP2 OPTIONS method. It monitors the health of configured SCP peers to ensure that the traffic is routed directly to the healthy peers. This enhancement avoids routing or rerouting towards unhealthy peers, thus minimizing the latency time.

Egress Gateway microservice maintains the health status of all available and unavailable SCPs. It maintains the latest health of SCPs by periodically monitoring and uses this data to route egress traffic to the most preferred healthy SCP.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-172 New SCP selection mechanism



Once `peerconfiguration, peersetconfiguration, routesconfiguration, and peermonitoringconfiguration` parameters are configured at Egress Gateway microservice, and all SCPs (after Alternate Route Service (ARS) resolution, if any vFQDN is configured) are marked initially as healthy. The peers attached to the associated peerset are scheduled to run health API checks and update the health status continuously.

During the installation, the value of the parameter `peermonitoringconfiguration` is set to false by default. Since, this feature is an add-on to the existing SBI Routing feature and will be activated if the `sbirouteconfig` feature is enabled. To enable this feature, perform the following:

- configure `peerconfiguration` with `healthApiPath`
- configure `peersetconfiguration`
- configure `sbiroutingerroractionsets`
- configure `sbiroutingerrorcriteriasets`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- configure `routesconfiguration`
- enable `peermonitoring`

If SBI Routing feature is enabled before upgrading, the `healthApi` in `peerconfiguration` should be attached manually to existing configured peers. If the operator tries to enable peermonitoringconfiguration and the targeted peers do not have the `healthApiPath` then an appropriate error response is sent.

Managing Monitoring the Availability of SCP Using SCP Health APIs

This section explains the procedure to enable and configure the feature.

Configure

You can configure the Monitoring the Availability of SCP using the REST API.

Configure Using REST API: Perform the following feature configurations as described in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Document*:

- create or update peer `Peer Configuration` with health status endpoint details.
- create or update the peerset `peersetconfiguration` to assign these peers
- enable the feature using the below peermonitoring configuration `peermonitoringconfiguration`.

> **Note**
>
> Health Monitoring of the peer will start only after the feature is enabled and the corresponding peerset is used in `sbirouteconfig`.

Observe

Following metrics are added in the CNC Policy Metrics section:

- oc_egressgateway_peer_health_status
- oc_egressgateway_peer_health_ping_request_total
- oc_egressgateway_peer_health_ping_response_total
- oc_egressgateway_peer_health_status_transitions_total
- oc_egressgateway_peer_count
- oc_egressgateway_peer_available_count

Alert

Following alerts are added in the Alert section:

- SCP_PEER_UNAVAILABLE
- SCP_PEER_SET_UNAVAILABLE

4.75 Supports 3gpp-Sbi-Correlation-Info Header

The 3gpp-Sbi-Correlation-Info header contains correlation information, User Equipment (UE) identity that is used by an operator in various offline network management, performance analysis, and troubleshooting tools and applications to identify messages (requests, responses, subscriptions, and notifications) related to a particular subscriber.

Copyright © 2019, 2026, Oracle and/or its affiliates.

In CNC Console, enable this feature in the global configuration page. By enabling this, the correlation-info header gets applied across all of the PCF external interfaces like PCF Session Management(SM), PCF Access and Mobility(AM), PCF UE Policy, PCF User Connector and Gateways. The generation of new correlation-info headers and forwarding them to producer NF's is not managed by this global configuration UI option.

The generation of new correlation-info header in PCF is managed by the **NF Communication Profiles** configuration page. Communication profiles once attached with the respective interfaces (PCF SM, PCF AM, PCF UE Policy, and PCF User Connector) allows to enable or disable of header generation along with the flexibility of selecting correlation type to be used for the header. The Correlation types namely SUPI, GPSI or both are supported for this release. For more details about *NF Communication Profiles*, see the NF Communication Profiles section.

The following conditions are to be met for header generation in PCF:

1. Correlation-info header, not sent by consumer NF towards PCF interfaces.
2. CNC Console global settings configuration is enabled.
3. Communication profile attached to the respective interface has the required configuration.

Further, the received or generated headers are forwarded only when the setting **Send Correlation-Info Header** is set to Enable.

3gpp-Sbi-Correlation-Info

The header contains correlation information e.g., UE identifier related to the HTTP request or response.

> **Note**
>
> 1. The possibility to include more than 1 correlationinfo parameter in the 3gpp-Sbi-Correlation-Info header is kept for future extensibility.
>   correlationinfo = ctype "-" cvalue
>
>   ctype = "imsi" / "impi" / "suci" / "nai" / "gci" / "gli" / "impu" / "msisdn" / "extid" / "imei" / "imeisv" / "mac" / "eui" / token
> 2. The token is defined for future extensibility.
>   The token of ctype shall not use the dash ("-") character.
>
>   cvalue = 1*tchar

Table 4-128 The format of cvalue shall comply with the data type description.

ctype	Description
SUPI	VarUeId format defined for IMSI and starting after the string "imsi-"
GPSI	VarUeId format defined for MSISDN and starting after the string "msisdn-"

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-129 3GPP defined Custom HTTP Headers

Header	Description	Example
3gpp-sbi-correlation-info	This header may be used to contain correlation information (e.g., UE identity), that may be used by an operator in various offline network management, performance analysis and troubleshooting tools/applications to identify messages (requests, responses, subscriptions, notifications) related to a particular subscriber.	EXAMPLE 1: When UE identifier used is SUPI and SUPI type is an IMSI: 3gpp-Sbi-Correlation-Info: imsi-345012123123123 EXAMPLE 2: When UE identifier used is GPSI and GPSI type is an MSISDN:3gpp-Sbi-Correlation-Info: msisdn-1234567890 EXAMPLE 3: When UE identifiers used are SUPI and GPSI where SUPI type is an IMSI and GPSI type is an MSISDN:3gpp-Sbi-Correlation-Info: imsi-345012123123123; msisdn-1234567890

Identifier Precedence for Generation of Correlation Header in request Toward other NFs

The UDR Connector service supports configurations to provide default user identifier that takes precedence over other identifiers. This ensures that these configured identifier should be considered while sending the requests toward external NFs like NRF or UDR. This key precedence `UDR.KeyPrecedence` value can be set by the user in the advanced settings of `PCF User Connector` service page in CNC Console. For more details, see the `Advanced Settings` in PCF User Connector section.

The configured precedence identifiers affects the generation of correlation header. The first identifier in the configuration shall be considered for the generation of the correlation header.

Consider a scenario where SBI Correlation header is configured and the default key precedence's are set to `IMSI,GPSI`. If both of the identifiers exists in the request then one of them takes priority based on the configured default key precedence. In this case IMSI shall be used for generating the correlation header while sending requests to external NFs UDR or NRF. If the precedence's are changed to `GPSI, SUPI` then for generation of correlation header GPSI is considered while sending the request to external NFs UDR or NRF.

Managing SBI messages correlation using Subscriber Identity

This section explains the procedure to enable and configure the feature.

Configure

In CNC Console, enable this feature by enabling `Enable SBI Correlation` field in the general settings page, see General Settings.

Configure Using REST API

For configuring the SBI messages correlation using Subscriber Identity feature using REST APIs, see *Oracle Communications Cloud Native Core, Policy REST API Specification Guide*.

Observe

Following metrics are added in Correlation-Info Header Metrics section:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- occnp_correlation_info_header_received
- occnp_correlation_info_header_forwarded
- occnp_correlation_info_header_generated

4.76 HTTP Error Codes

Policy can handle Protocol or Application errors and a few other additional defined errors for various scenarios. When Policy encounters an error in processing a request, it sends error codes in the response message to the request. With this enhanced functionality, Policy allows users to mitigate errors from different NFs.

Error Mapping for CHF and UDR Interfaces

Configure
In UDR and CHF, the session retry functionality is used to mitigate the errors. For more information, see Support for Session Retry and Alternate Route Service.

In addition to session retry, we can mitigate the errors using the object expressions with action as "Reject session with error code" blockly. If this blockly is not configured, PCF responds to SMF or AMF with "400" error code and "USER_UNKNOWN" cause code for any error response received from UDR while fetching subscriber profile. For more information, see "PCF-SM" section in Oracle Communications Converged Policy Design Guide.

Enable
To enable Error Handling feature where the Error Codes from CHF & UDR to reach the core services, the following flags needs to be updated in the Advanced Settings specific to the service:

- For UDR, **UDR_errorHandlerEnabled** key must be set to true, in the advanced settings for PCF User Connector service.
- For CHF, **CHF_errorHandlerEnabled** key must be set to true, in the advanced settings for PCF User Connector service.
- For PDS, **PDS_ERROR_HANDLER_ENABLED** key must be set to true, in the advanced settings for PDS service.

For more information, see Configuring Policy Using CNC Console.

Observe
Added the following metrics for Error Mapping for CHF and UDR Interfaces :

- error_handler_in_total
- error_handler_out_total

> **Note**
>
> When the UDR Connector, CHF Connector, and PDS act as a consumer of the error and the Error Handler feature is integrated with these services and is enabled, and if these services are generating any error while interacting with other services, then the above metrics will increment. Whereas, When the UDR Connector, CHF Connector act as a producer of the error, the Error Handler feature is not considered. Hence, these metrics does not get incremented even when the feature is enabled.

For more information, see Error Mapping Metrics.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Error Mapping for AM, SM, and UE Interfaces

In AM, SM, and UE, the session retry functionality is used to mitigate some of the errors. For more information, see Support for Session Retry and Alternate Route Service.

Enable
This is a core functionality of Policy. You do not need to enable or disable this feature.

Configure
The following blockly has been added in the PCF-SM to reject a session with error code:

Figure 4-173 Reject Session with Error Code and Error Cause



This action blockly allow to reject the session with a custom error code and a custom error cause.

For more information, refer to Oracle Communications Cloud Native Core, Policy Design Guide.

Observe
The following metrics is incremented in case of error mapping for AM, SM, and UE interface:

- ocpm_ingress_response_total

For more information, see

Error Mapping for NRF Interface

In NRF, the Policy retries with primary and non-primary NRFs to configure the errors.

Enable
To enable the service, set the following parameter to true at the time of installing or upgrading Policy:

`notifySemanticValidationEnabled`

For information on the parameter, refer to Oracle Communications Cloud Native Core, Policy Installation, Upgrade, and Fault Recovery Guide .

Configure
This feature can be configured using the `notifySemanticValidationEnabled` parameter.

Observe
Added the following metrics for Error Mapping for NRF Interface :

- nrfclient_nw_conn_in_response_total
- nrfclient_nw_conn_out_notify_response_total

For more information, see NRF Client Metrics.

For the list and the details of the HTTP error codes of CHF, UDR, AM, SM, UE, and NRF interfaces, see HTTP Error Codes Supported by Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.77 Diameter Error Codes

Policy can handle protocol or application errors and a few other additional defined errors for various scenarios. When Policy encounters an error in processing a request, it sends error codes in the response message to the request. Policy interacts with BSF and at Rx interface during the life of a session there could be an error scenario.

Policy should handle error gracefully and there should be defined path for each error scenario for effective functioning of NF. With this enhanced functionality, Policy allows users to configure error codes.

The error codes are configured by adding customized values, for a defined condition, for the following fields:

- Error Description
- Diameter Result Code
- Experimental Result
  - Vendor ID
  - Experimental Result Code

Configure

To configure the diameter error codes for Policy, users can use any of the following ways:

- **CNC Console**: Perform the configurations on the Diameter Error Codes page. For more information, see Diameter Error Configurations .
- **REST API**: Perform the configurations using POST, PUT, or GET operations. For more information about REST API configuration, see *Cloud Native Core Policy REST Specification Document*.

Observe

The *occnp_diam_response_local _total* and *occnp_diam_response_network_total* metrics are applicable for this feature. For more details, see Diameter Gateway Metrics.

4.78 Configurations for Pre and Post Upgrade/Install Validations

This feature applies validation checks that are required on the application, databases, and its related tables before and after the upgrade/installation of Policy application.

On enabling this mandatory pre-flight and post-flight validation checks, for successful upgrade/ installation following are validated:

- does the related database exists
- does all the required tables exist
- does the required table schema exist for all the required tables
- does all the required infrastructure exists

This pre-flight and post-flight checks ensures that all the dependent databases, tables, schema, applications are in right order for performing successful update/installation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information on how to how to set the parameter value for pre and post flight checks, see *Configurations for Pre and Post Upgrade/Install Validations* in *Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

4.79 Support Multiple Cluster Deployment at CNC Console

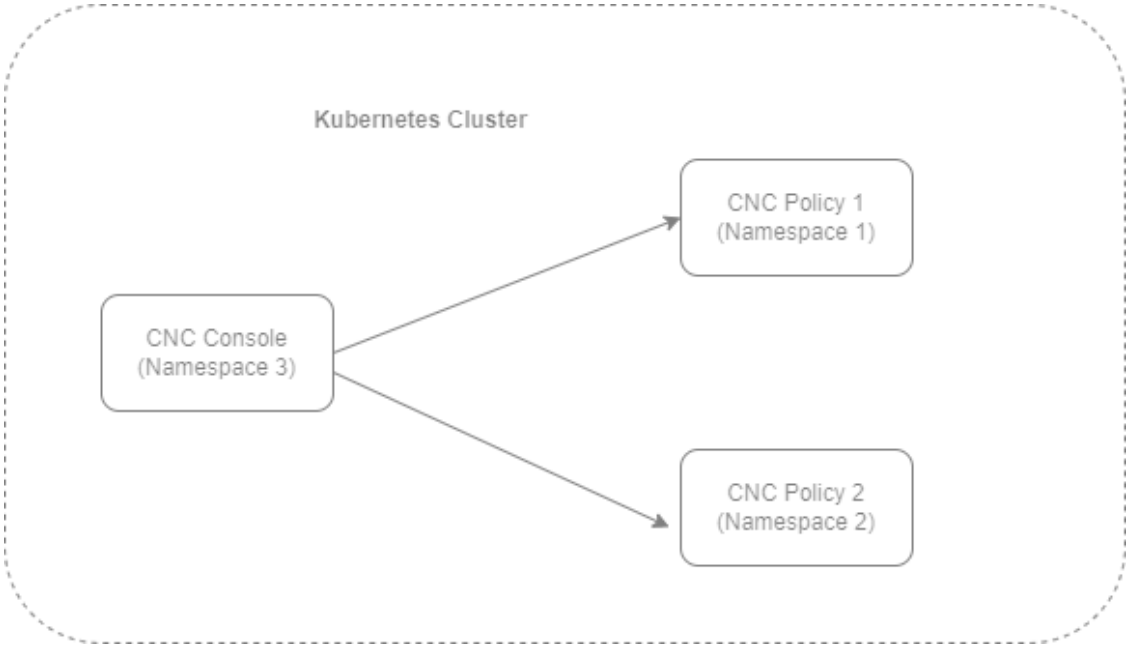
The CNC Console supports both single and multiple cluster deployments.

In a single cluster deployment, the CNC Console can manage NFs and Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) common services deployed in the local Kubernetes clusters.

In a multiple instances deployment, the CNC Console can manage multiple Policy instances and CNE common services deployed within a Kubernetes cluster. For more information about single and multiple cluster deployments, see *Oracle Communications Cloud Native Core, Cloud Native Configuration Console Installation, Upgrade and Fault Recovery Guide*.

The following image represents a Kubernetes cluster with one instance of CNC Console and two instances of Policy. The single instance of the CNC Console is configuring two instances of Policy with different namespaces.

Figure 4-174 Support for Multiple Instance Deployment

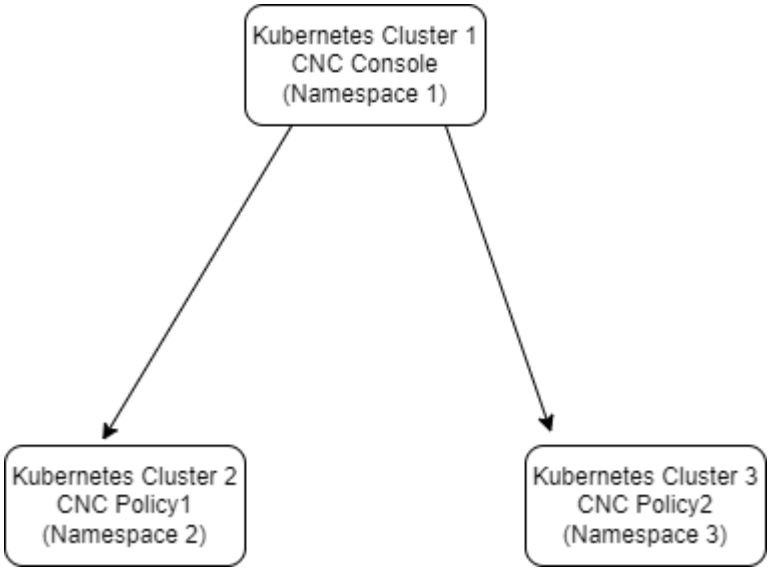


With the support of multicluster deployment, Policy deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a multicluster deployment, the CNC Console can manage Policy and CNE common services deployed in the remote Kubernetes clusters.

The following image represents multiple Kubernetes clusters with one CNC Console and two Policy deployments. The single instance of the CNC Console is configuring two instances of Policy with different namespaces deployed in different clusters.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-175 Support for Multicluster Deployment



4.80 NetLoc Support

NetLoc is one of the 3GPP-defined features responsible for retrieving access network information in IMS network architecture. Depending on the operator's policy configuration and subscription, the NetLocfeature helps in fetching User Equipment (UE) time zone information and User location information from the access network. Such information is called Network Provided Location Information (NPLI). Operators can use the NPLI information for the following:

- Lawful interception
- Charging
- IMS Emergency Calls Routing
- Retention of Location Information Data
- Special Call Routing for Localized Services
- Location-based service triggering

4.80.1 NetLoc Support in PCF

Based on the response that it receives from SMF over the N7 interface, PCF provides this NPLI to the Application Function (AF) over the Rx interface.

The Application Function initiates a request towards PCF requesting NPLI using the "ACCESS_NETWORK_INFO_REPORT" within Specific-Action AVP and Required-Access-Info AVPs. PCF, upon receiving this request, initiates Npcf_SMPolicyControl_UpdateNotify procedure for AN_INFO event trigger requesting NPLI in terms of user location and/or user timezone information. SMF, upon receiving NPLI information from core network (AMF), provides that info PCF using Npcf_SMPolicyControl_Update procedure. Then, PCF forwards that information to AF using RAR message using 3GPP-User-Location-Info, 3GPP-MS-TimeZone, 3GPP-SGSN-MCC-MNC AVPs.

Copyright © 2019, 2026, Oracle and/or its affiliates.

By default, this feature is not configured on the CNC Policy deployment. You must configure the NetLoc feature using the CNC Console or REST API.

Feature Negotiation

Once the feature has been enabled, feature negotiation needs to happen between AF and PCF during Npcf_PolicyAuthorization_Create Service operation. As defined by the 3GPP feature negotiation mechanism, the following conditions must be met for AF and PCF to agree upon the NetLoc feature:

- NF consumer or AF advertises the support for "NetLoc" feature within the attribute supportedFeatures (suppFeat) as part of SmPolicyData when sending a request to create SM policy association.
- In turn, PCF advertises the same value for the supportedFeatures (suppFeat) while sending the response for the policy association create request.

Managing NetLoc Support

Enable and Configure

By default, this feature is not configured on the CNC Policy deployment. You can opt to configure the NetLoc using the CNC Console or REST API.

On PCF Session Management page, under Service Configurations, select `NetLoc` from the drop-down menu of **Override Supported Features** parameter. For more information about the configurations, see PCF Session Management.

Using the REST APIs for Session Management Service, you can enable the feature by updating the value as `NetLoc` for the following parameter under the `system` group:

```
overrideSupportedFeatures": [
      "NetLoc"
    ],
```

Observe

No new alarms or alerts are introduced specific to this feature.

4.80.2 NetLoc Support in PCRF

Based on the response that it receives from PGW (PCEF) over the Gx interface, PCRF provides this NPLI to the Application Function (AF) over the Rx interface.

The AF initiates a request (AAR-I/U, STR) towards PRCF requesting NPLI using "ACCESS_NETWORK_INFO_REPORT" within Specific-Action AVP and Required-Access-Info AVPs (USER_LOCATION and/or MS_TIME_ZONE). PRCF, upon receiving this request, initiates RAR procedure for AN_INFO event trigger requesting NPLI in terms of user location and/or user timezone information. PGW (PCEF), upon receiving NPLI information from core network (AMF) provides the information to PCRF through CCR-Update. PCRF forwards that information to AF using RAR message using 3GPP-User-Location-Info, User-Location-Info-Time, 3GPP-MS-TimeZone, 3GPP-SGSN-MCC-MNC AVPs.

Feature Negotiation

PGW (PCEF) sends in Supported-Features **"Feature List": "1024"** in CCR-Initial advertising that NetLoc is supported. PCRF sends the same **"Feature List": "1024"** in CCA with DIAMETER_SUCCESS, else it receives a diameter Error. AF sends in AAR-I/U Supported-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Features **"Feature List": "32"** when soliciting NetLoc Information. Then, PCRF sends the same **"Feature List": "32"** in AAA with DIAMETER_SUCCESS.

Managing NetLoc Support

Enable and Configure

By default, this feature is not configured on the CNC Policy deployment. You must configure the NetLoc feature using the CNC Console or REST API.

This feature can be configured or customized using the following Advanced Settings keys in the PCRF Core services in the CNC Console:

- DIAMETER.ENF.AFDirectReply
- DIAMETER.AF.MaxWaitForInfoOnTermination

Fore more information, see Settings.

Observe

No new alarms or alerts are introduced specific to this feature.

4.81 Subscription to Notification Support for Signaling Path Status

Policy supports notification of the AF signaling Transmission Path Status (SMF → Policy → AF), subscription to notification of the AF signaling Transmission Path Status (AF → Policy → SMF), and cancellation of subscription to notification of the AF signaling Transmission Path Status (AF → Policy → SMF).

PCRF-Core supports notification of the AF signaling Transmission Path Status (PGW → PCRF-Core → AF), subscription to notification of the AF signaling Transmission Path Status (AF → PCRF-Core → PGW), and cancellation of subscription to notification of the AF signaling Transmission Path Status (AF → PCRF-Core → PGW).

For Policy, during a PDU session establishment procedure, the SMF includes the `IMS_SIG` value within the `qosFlowUsage` attribute and the PCF accepts that default QoS flow is dedicated to IMS signaling, the PCF within the SmPolicyDecision data structure must include the `IMS_SIG` value within the `qosFlowUsage` attribute.

For more information on `IMS_SIG` value update in the CNC Console, see PCF Session Management.

For, PCRF-Core, during a PDU session establishment procedure, the SMF includes the `IMS_SIGNALLING` value within the `bearerusage` attribute and the PCF accepts that default QoS flow is dedicated to IMS signaling, the PCF within the SmPolicyDecision data structure must include the `IMS_SIGNALLING` value within the `bearerusage` attribute.

For more information on `IMS_SIGNALLING` value update in the CNC Console, see PCRF Core .

Notification of the AF Signaling Transmission

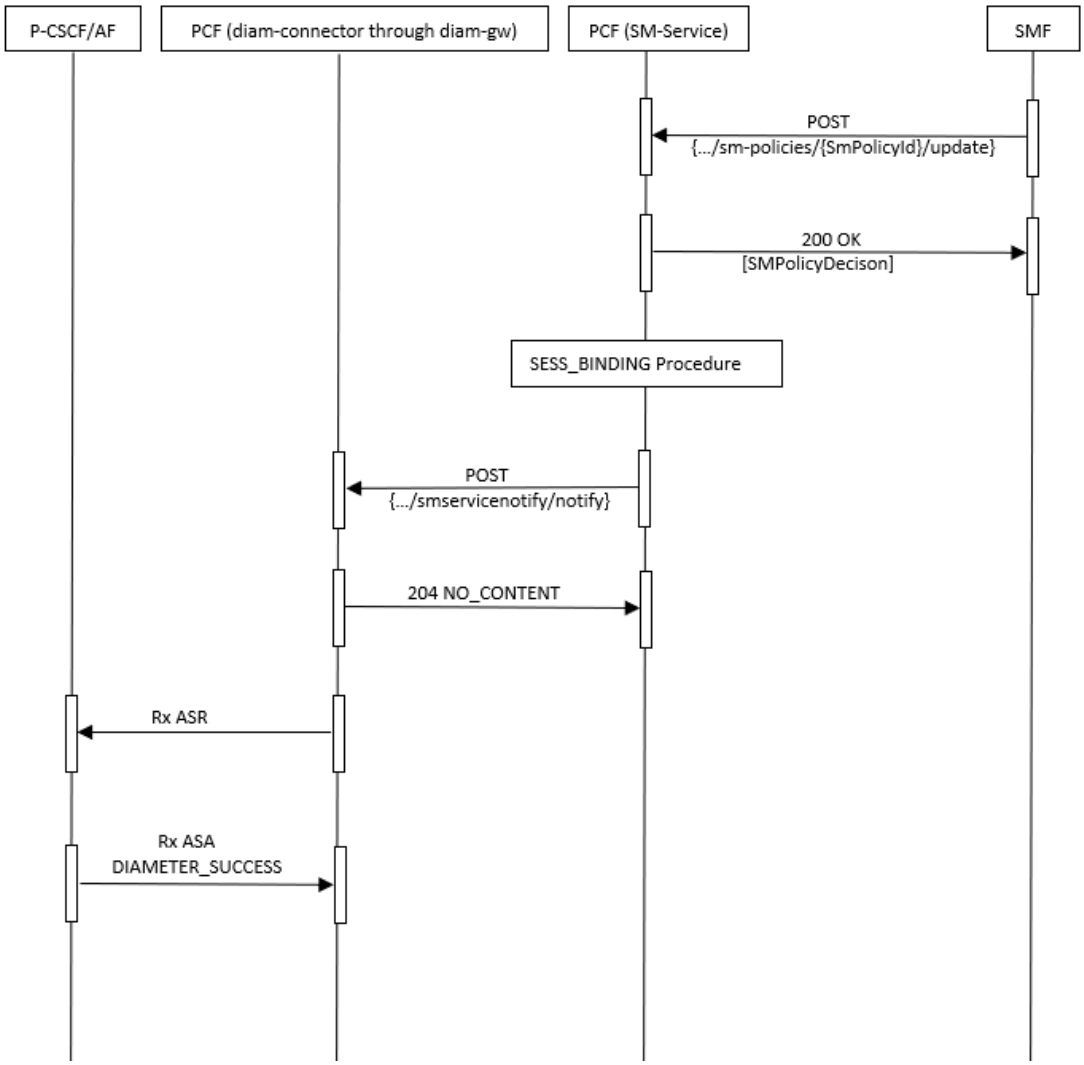
When the Policy is notified of the release of resources associated to the PCC or QoS rules corresponding with AF Signaling IP Flows, the Policy informs the AF about the release of the signaling Transmission path by sending a Re-Authorization Request (RAR) command to the AF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The RAR includes the Specific-Action AVP set to the value "INDICATION_OF_RELEASE_OF_BEARER (4)" and the deactivated IP Flow encoded in the Flows AVP.

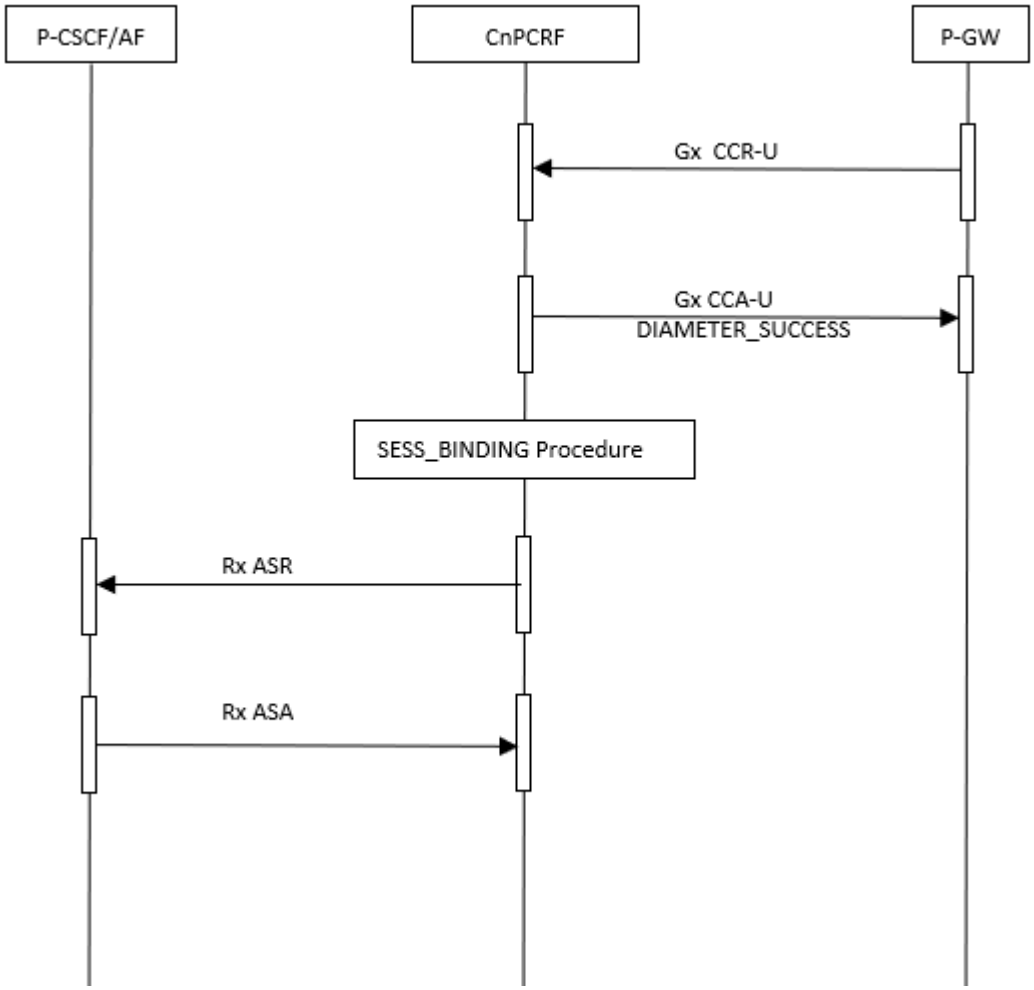
On Sm Update/CCR-U with the IMS Signalling Rule set as inactive, at a minimum, we are able to send an Rx ASR.

Figure 4-176 Notification of the AF Signaling Transmission in 5G



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-177 Notification of the AF Signaling Transmission in 4G



Subscription to notification of the AF Signaling Transmission

When AF receives an initial register SIP message from an attached UE, it subscribes to the notifications of the AF signaling transmission path status.

The AF provides the following:

- UE's IP address (using either the Framed-IP-Address AVP or the Framed-Ipv6-Prefix AVP)
- Specific-Action AVP requesting the subscription to "INDICATION_OF_RELEASE_OF_BEARER"
  - INDICATION_OF_RELEASE_OF_BEARER (4)

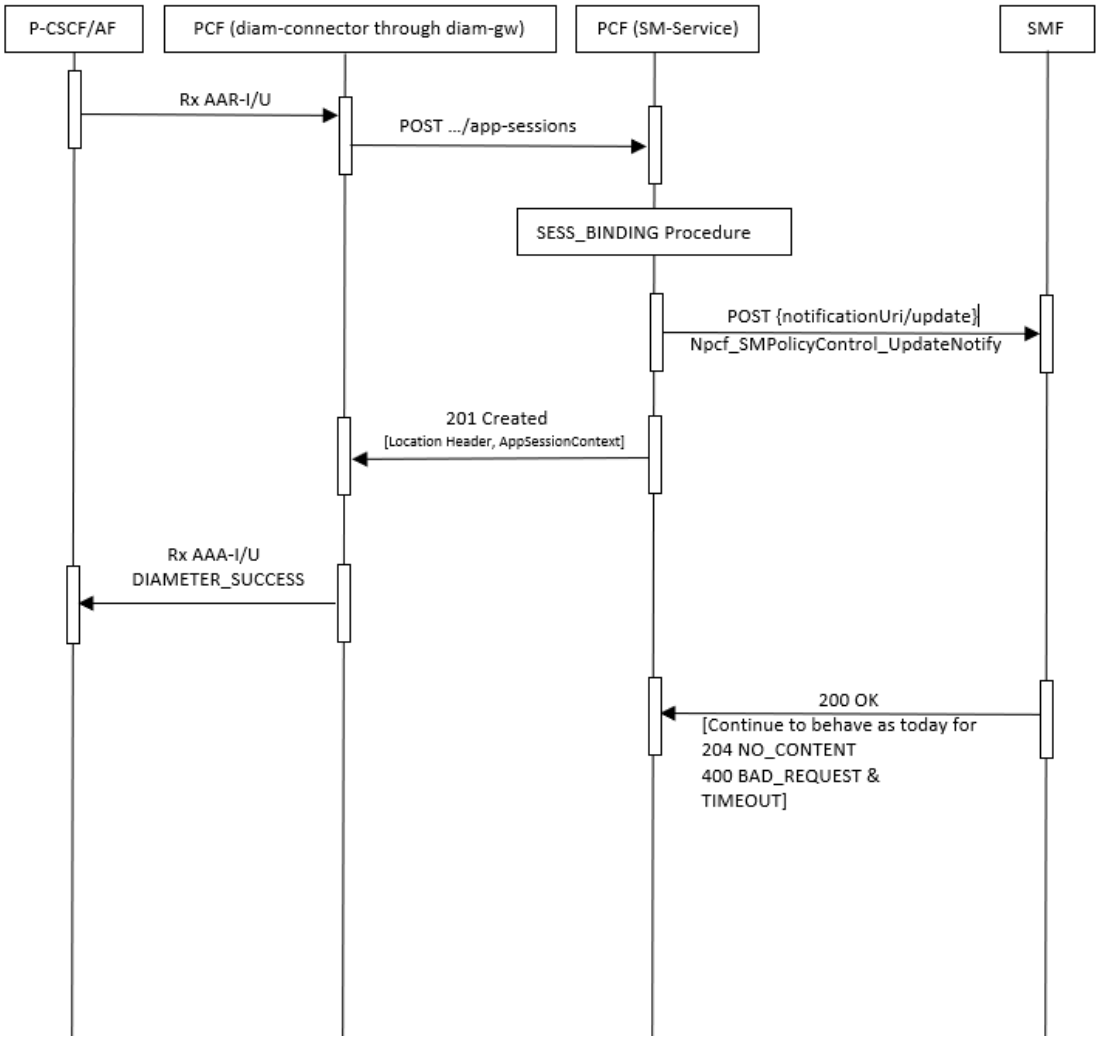
    In the AAR, this value indicates that the AF requests the server to provide a notification at the removal of a bearer
- The AF shall additionally provide a Media-Component-Description AVP including a single Media-Sub-Component AVP with the Flow-Usage AVP set to the value "AF_signaling"
- The Media-Component-Description AVP shall contain the Media-Component-Number AVP set to "0

Copyright © 2019, 2026, Oracle and/or its affiliates.

On Rx AAR with the flow-usage as IMS Signalling, we link the Rx session with the IMS Signalling rule. We do not need to send a Gx RAR or SmUpdateNotify.

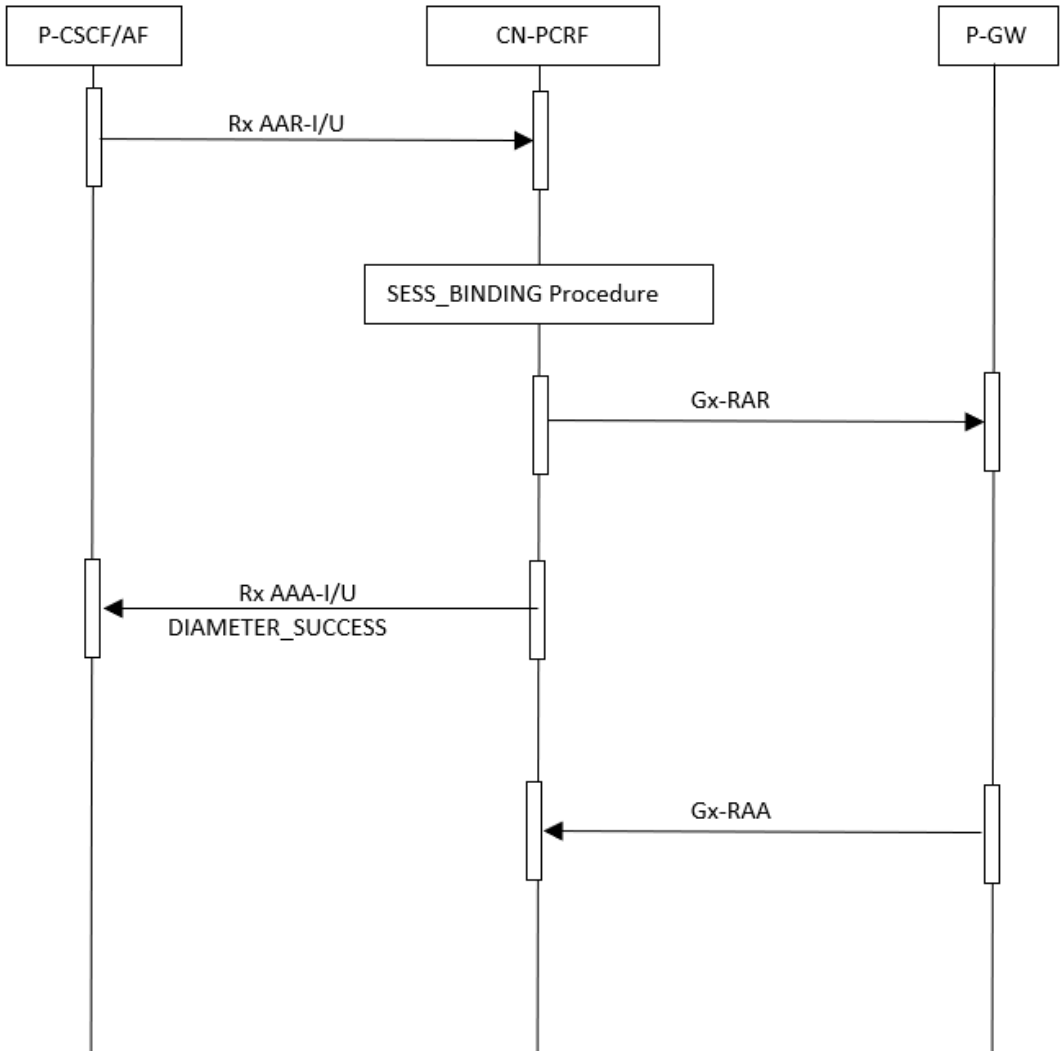
If we do not find an IMS Signalling rule, then bind it to the first PCC rule so we get an ASR only on CCR-T.

Figure 4-178 Subscription to notification of the AF Signaling Transmission in 5G



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-179 Subscription to notification of the AF Signaling Transmission in 4G



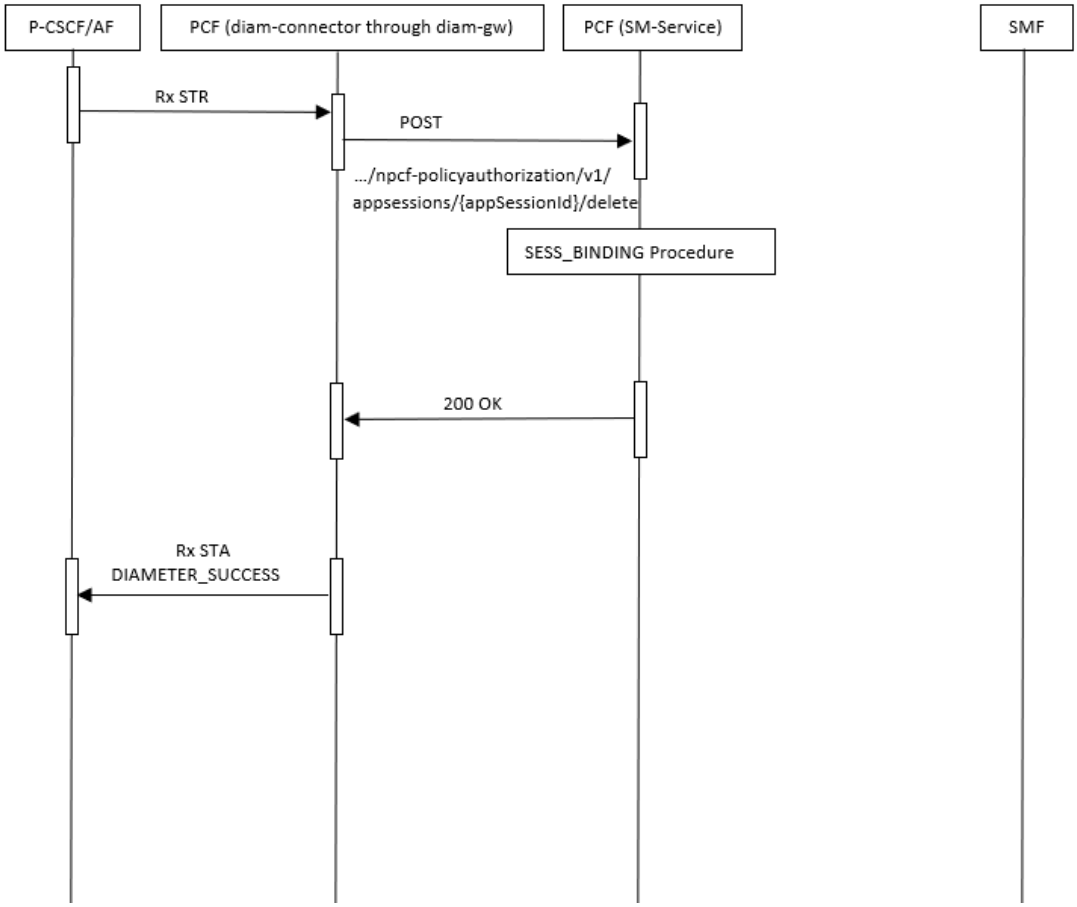
Cancellation of subscription to notification of the AF Signaling Transmission

If the Rx Diameter Session is only used for subscription to Notification of signaling Path Status, the AF may cancel the subscription to notifications of the status of the AF signaling transmission path. In this case, the AF uses a Session-Termination-Request (STR) command to the CNCPolicy, which gets acknowledged with a Session-Termination-Answer (STA) command.

On Rx STR, we simply unlink the Rx session from the Gx session / sm session and IMS Signalling Rule, but we do not remove the IMS Signalling Rule from the Gx or SM.

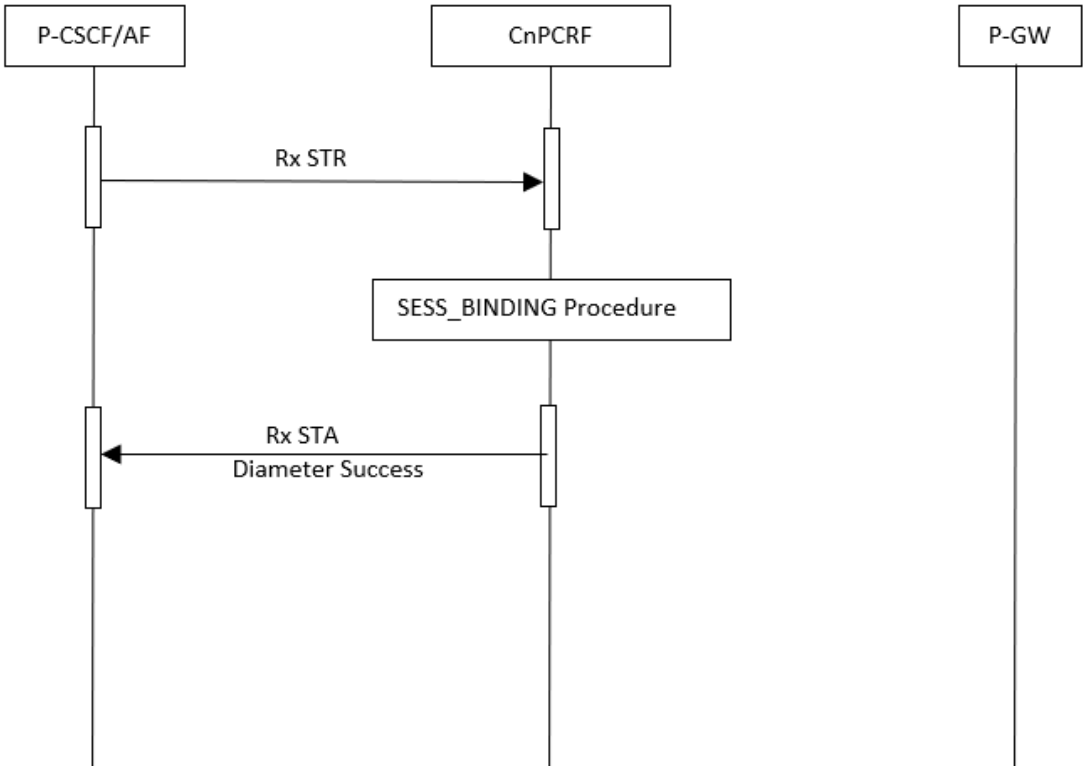
Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-180 Cancellation of subscription to notification of the AF Signaling Transmission in 5G



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-181 Cancellation of subscription to notification of the AF Signaling Transmission in 4G



4.82 Support for SessionRuleErrorHandling

The Session Rule Error Handling is a 3GPP 29.512 TS defined feature. If the SessionRuleErrorHandling feature is supported and SMF receives one or more session rules but it does not enforce some or all session rules then the SMF provides sessionRuleReports.

When SMF detects that the provisioning of some or all the session rules is unsuccessful, it sends a Session Rule Error Report in the `Npcf_SMPolicyControl_Update` and `Npcf_SMPolicyControl_UpdateNotify` Response. Depending on the Session Rule Error Report sent by SMF, the PCF may decide whether to retain the old session rule, re-installation, modification, or removal of the session rule.

> **Note**
>
> When this feature is enabled, RULE_PERMANENT_ERROR and RULE_TEMPORARY_ERROR received in Session Rule Reports are handled by the Session Rule Error Handling feature. These errors do not need to be configured in the SMF Notification Retry Profile.

As per the sessionRuleReport, you can write policy conditions matching the ruleStatus and sessRuleFailureCode received for the session rule and take action of installation, modification, and removal of the session rule. The blocks are available only when you select **PCC/Session Rule Error Report** under **PCF-SM** service while configuring the Policy Project. For more

Copyright © 2019, 2026, Oracle and/or its affiliates.

information about these blocks, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Feature Negotiation

Once the feature has been enabled, feature negotiation needs to happen between SMF and PCF during Npcf_SMPolicyControl_Create service operation. As defined by the 3GPP feature negotiation mechanism, the following conditions must be met for SMF and PCF to agree upon the SessionRuleErrorHandling feature:

- NF consumer or SMF advertises "SessionRuleErrorHandling" feature within the attribute supportedFeatures (suppFeat) as part of SmPolicyData when sending a request to create SM policy association.
- In turn, PCF advertises the same value for the supportedFeatures (suppFeat) while sending the response for the policy association create request.

Enable

By default, this feature is not enabled on the Policy deployment. You can enable the SessionRuleErrorHandling feature using the CNC Console or REST API.

- CNC Console: On PCF Session Management page, under Service Configurations, select `SessionRuleErrorHandling` from the drop-down menu of **Override Supported Features** parameter. For more information about the configurations, see PCF Session Management.
- REST API: Using the REST APIs for Session Management Service, you can enable the feature by updating the value as `SessionRuleErrorHandling` for the following parameter under the `System` group in the `{apiRoot}/oc-cnpolicyconfiguration/v1/services/pcfsm` REST API:

```
overrideSupportedFeatures": [
      "SessionRuleErrorHandling"
    ],
```

Observe

The following metrics have been enhanced for this feature:

- occnp_http_in_conn_request_total
- occnp_http_in_conn_response_total
- occnp_http_out_conn_request_total
- occnp_http_out_conn_response_total

> **Note**
>
> The "sessRuleReports" dimension has been added for *`occnp_http_in_conn_request_total`* and *occnp_http_in_conn_response_total* metrics.

The following metric have been added for this feature:

- occnp_sm_sess_rule_failure_total

For more information, see SM Service Metrics.

Copyright © 2019, 2026, Oracle and/or its affiliates.

No new alerts are introduced for this feature.

Maintain

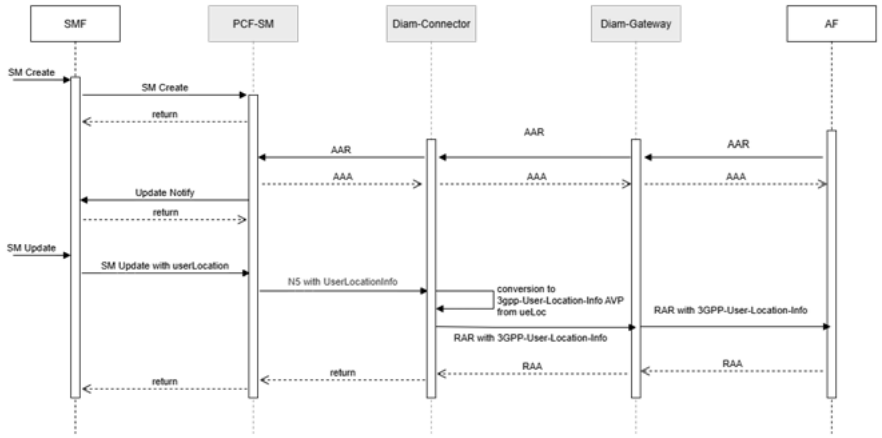
Logs are added for processing of sessionRuleReports attribute as part of SM-Update request and SM-UpdateNotify response.

4.83 3GPP-User-Location-Info AVP in Rx RAR

This section describes the inclusion of 3GPP-User-Location-Info in Rx RAR, when the UserLocation attribute is received on the SMF-N7 flows.

The following call flow describes the RAR message flow from PCF to send 3GPP-User-Location-Info AVP towards AF:

Figure 4-182 3GPP-User-Location-Info Call Flow-for RAR Messages



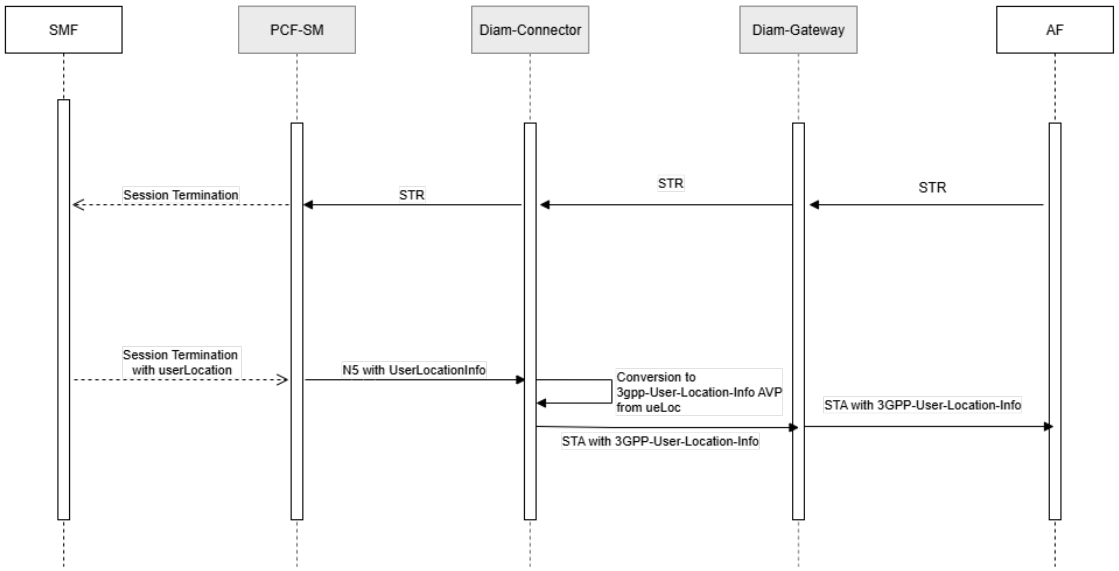
PCF performs the following steps to send 3GPP-User-Location-Info AVP towards AF:

1. Application Function (AF) forwards the supported feature Attribute Value Pair (AVP) with LTE_Phase3 value in the first Authentication Request (AAR) of AF/Rx towards the PCF. In response, PCF exchanges the same AVP in Authentication Answer (AAA).
2. The AF subscribes for any of the specific-action between `INDICATION_OF_SUCCESSFUL_RESOURCE_ALLOCATION` and `INDICATION_OF_RELEASE_OF_BEARER`.
3. After establishing the AF session successfully, Session Management Function (SMF) sends `repPolicyCtrlReqTriggers` with `SUCC_RES_ALLO or RES_RELEASE` along with `ruleReports` and `userLocationInfo` to PCF.
4. SM service generates event notification request for Diameter Connector over N5 along with `ueLoc` attribute.
5. The Diameter Connector generates a Re-Auth-Request (RAR) with `3GPP-User-Location-Info` AVP for AF over Rx interface.

The following call flow describes the Rx-STR and Rx-STA sent to AF with 3GPP-User-Location-Info AVP Diameter message when the AF requests the user location information:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-183 3GPP-User-Location-Info Call Flow-for STR Messages



1. AF requests PCF to report the access network information (user location) at Rx session termination.

   SM service receives the STR message sent by AF through Diameter Gateway and Diameter Connector.
2. SM service sends the session termination notification to SMF.
3. SMF sends the user location information to SM service.
4. SM service sends the user location information to Diameter Connector.
5. Diameter Connector transforms this to Diameter AVP, encodes the header as per the configuration and sends the STA with user location info to AF.

ueLoc Attribute

In case of 3GPP access, the PCF includes the user location information in the `ueLoc` attribute in N5 interface. The `ueLoc` attribute has `eutraLocation` and `nrLocation` attributes.

`eutraLocation`: The data type for the `eutraLocation` attribute is `EutraLocation`. It has the following attributes:

Table 4-130 eutraLocation

Attribute Name	Data Type	Description
tai	Tai	The Type Allocation Code (TAC) of the Tracking Area Identity (TAI) is set to one reserved value. For an example 0x0000 is the TAC of a TAI attribute. If the TAI information is not available, see clause 19.4.2.3 of 3GPP TS 23.003 [7]).
ecgi	Ecgi	E-UTRA Cell Identity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-130 (Cont.) eutraLocation

Attribute Name	Data Type	Description
ignoreEcgi	Boolean	This attribute indicates that the Ecgi is ignored. This attribute is set to `false` by default. When it is set as `true`, the Ecgi is ignored.
globalNgenbId	GlobalRanNodeId	It indicates the global identity of the ng-eNodeB in which the UE is currently located.
globalENbId	GlobalRanNodeId	It indicates the global identity of the eNodeB in which the UE is currently located.

`nrLocation`: The data type for the `nrLocation` attribute is `NrLocation`. It has the following attributes:

Table 4-131 NrLocation

Attribute Name	Data Type	Description
tai	Tai	The TAC of the TAI is set to one reserved value. For an example 0x0000 is the TAC of a TAI attribute.
ncgi	Ncgi	NR Cell Identity
ignoreNcgi	Boolean	This attribute indicates that the Ncgi is ignored. This attribute is set to `false` by default.
globalGnbId	GlobalRanNodeId	This attribute indicates the global identity of the `gNodeB` in which the UE is currently located.

For more information on ueLocation, see the 3GPP technical specification 29.514.

In the RAR message, `GeographicLocation` is used. Following are the types of GeographicLocation used in the RAR message:

- TAI(128): Tracking Area ID for E-UTRAN.
- ECGI(129): Evolved Cell Global ID for E-UTRAN.
- TAI_ECGI(130): Tracking Area ID and Evolved Cell Global ID for E-UTRAN.
- ENODEB(131): global identity of the ng-eNodeB for E-UTRAN.
- TAI_ENODEB(132) : Tracking Area ID and global identity of the eNodeB for E-UTRAN.
- EXTENDEDNODEB(133): global identity of the eNodeB for E-UTRAN.
- TAI_EXTENDEDNODEB(134) : Tracking Area ID and global identity of the eNodeB for E-UTRAN.
- NCGI(135) : NR Cell Global Identity for NR.
- TAI5G(136) : Tracking Area ID for NR.
- TAI5G_NCGI(137) : Tracking Area ID and NR Cell Global Identity for E-UTRAN.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- NGRANNODE(138) : global identity of the gNodeB for NR.
- TAI5G_NGRANNODE(139) : Tracking Area ID and global identity of the gNodeB for NR.

Following is the sample N7 update request for the userLocationInfo attribute:

```
"userLocationInfo": {
    "eutraLocation": {
      "tai": {
        "plmnId": {
          "mnc": "313",
          "mcc": "350"
        },
        "tac": "790"
      },
      "ecgi": {
        "plmnId": {
          "mnc": "313",
          "mcc": "350"
        },
        "eutraCellId": "AB0912"
      },
      "ageOfLocationInformation": 233,
      "ueLocationTimestamp": "2019-03-13T06:44:14.34Z",
      "geographicalInformation": "AAD1234567890123",
      "geodeticInformation": "AAD1234567890123BCEF",
      "globalNgenbId": {
        "plmnId": {
          "mnc": "313",
          "mcc": "350"
        },
        "n3IwfId": "n3iwfid"
      }
    }
  }
```

Following is the sample N5 Notification Request for the ueLoc attribute:

```
"ueLoc": {
    "eutraLocation": {
        "tai": {
        "plmnId": {
          "mcc": "313",
          "mnc": "350"
        },
        "tac": "790"
      },
      "ecgi": {
        "plmnId": {
          "mcc": "313",
          "mnc": "350"
        },
        "eutraCellId": "AB0912"
      }
    },
    "nrLocation": null,
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    "n3gaLocation": null
  }
```

Following is the sample Diameter RAR message:

```
Sample Diameter RAR request:
Diameter Message: RAR
Version: 1
Msg Length: 232
Cmd Flags: REQ,PXY
Cmd Code: 258
App-Id: 16777236
Hop-By-Hop-Id: 4144052655
End-To-End-Id: 2394693330
  Session-Id (263,M,l=9) = 1
  Origin-Host (264,M,l=28) = diam-conn.oracle.com
  Origin-Realm (296,M,l=18) = oracle.com
  Destination-Realm (283,M,l=24) = test.example.com
  Destination-Host (293,M,l=28) = diamcliaf.oracle.com
  Auth-Application-Id (258,M,l=12) = 16777236
  Specific-Action (513,VM,v=10415,l=16) =
INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION (8)
  Flows (510,VM,v=10415,l=44) =
    Media-Component-Number (518,VM,v=10415,l=16) = 1
    Flow-Number (509,VM,v=10415,l=16) = 2
  User-Location-Info-3GPP (22,V,v=10415,l=25) = Type=TAI_ECGI(130)
MCCMNC=313350 TAC=1936 ECI=11208978
```

For more information, see the following 3GPP specification:

- 29.512
- 29.514
- 29.214
- 29.229

Enable

This feature is enabled automatically at the time of Policy installation.

Configure

Diameter connector has an environment variable `PRIORITY_SPECIFIC_ACTION` which prioritizes the action while sending RAR message, if AF has subscribed for `INDICATION_OF_FAILED_RESOURCE_ALLOCATION` and `INDICATION_OF_RELEASE_OF_BEARER`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.83.1 Support for Encoding of NCGI in 3GPP-User-Location-Info

> **Note**
>
> This feature is applicable for Diameter Rx-RAR and Rx-STA messages when `3GPP-User-Location-Info` AVP is sent with Geographic Location Type value `5GS TAI and NCGI`.

Policy supports `3GPP-User-Location-Info` AVP for Rx-RAR and Rx-STA diameter messages and the AVP values.

During SM Update or session terminate call flows, Diameter Connector receives N5 message from SM service containing user location information. Diameter Connector converts the user location information in the N5 message to `3GPP-User-Location-Info` AVP. In case SM Update callflow, Diameter sends `3GPP-User-Location-Info` AVP in a RAR message to the AF and in case of Terminate callflow, Diameter sends `3GPP-User-Location-Info` AVP in a STA message to the AF.

By default, the value of NR Cell Global Identity (NCGI/NR CGI) in `3GPP-User-Location-Info` AVP is encoded as per TS 129.061 v10 - Rel16 3GPP standards.

When this feature is enabled by configuring the value of `ENABLE_REL18_ENCODING_FOR_NCGI` to `true`, the value of NR Cell Global Identity (NCGI/NR CGI) in `3GPP-User-Location-Info` AVP is encoded as per TS 129.061 v10 - Rel18 3GPP standards.

The NR Cell Global Identity (NCGI/NR CGI) is a Size (36) bit string data type, which occupies the four complete Octet and four bits of the 5th Octet. The rest 4 bits are Spare bits. The value of `NCGI` field indicates details of where the UE is currently located (for example, SAI or CGI).`

In the encoding of `3GPP-User-Location-Info` AVP, the value of 137 code correspond to `5GS TAI and NCGI` field.

The placement of the Spare bits for NR Cell Global Identity (NCGI/NR CGI) in `3GPP-User-Location-Info AVP` can be configured using `ENABLE_REL18_ENCODING_FOR_NCGI` Advanced Settings Key. The `ENABLE_REL18_ENCODING_FOR_NCGI` Advanced Settings Key for Diameter Connector can be configured either through CNC Console or using Diameter Connector REST API.

When the value of `ENABLE_REL18_ENCODING_FOR_NCGI` Advanced Settings key is set to `false`, the NR Cell Global Identity (NCGI/NR CGI) is encoded in `3GPP-User-Location-Info` AVP as per TS 129.061 - Rel16 3GPP standard as follows:

If the Geographic Location Type has a value indicating `5GS TAI and NCGI` (that is, the value field is equal to 137), in Geographic Location fields of both `5GS TAI` and `NCGI` are encoded one after another and the Spare bits are set to zero.

When the value of `ENABLE_REL18_ENCODING_FOR_NCGI` Advanced Settings key is set to `true`, the NR Cell Global Identity (NCGI/NR CGI) is encoded in `3GPP-User-Location-Info` AVP as per TS 129.061 - Rel18 3GPP standard as follows:

If the Geographic Location Type has a value indicating `5GS TAI` and `NCGI` (that is, the value field is equal to 137), in Geographic Location field both `5GS TAI` and `NCGI` are encoded one after another. Spare bits for the `NCGI` are placed just after the `PLMN Identity` and are set to zero.

Copyright © 2019, 2026, Oracle and/or its affiliates.

That is, the 5GS TAI And NCGI Geographic Location field values are encoded starting from left side placing the first 4 bits as spare bits just after the PLMN Identity and these spare bits are set to zero. The next 36 bits are set to the 5GS TAI And NCGI field values.

Example:

User-Location-Info-3GPP (22,V,v=10415,I=27) *is* ***Type=TAI5G_NCGI(137) MCCMNC=313350 NCGI=007d4000f*** *and* ***nrCellId*** *is* ***007D4000F***

The ***nrCellId*** is part of TAI5G_NCGI field value and it is a Size (36) BIT STRING, which occupies the 4 complete Octet and 4 bits of the 5th Octet. The rest 4 bits are Spare bits. The below table shows a sample encoding behavior as per the configuration of ENABLE_REL18_ENCODING_FOR_NCGI field.

Table 4-132 Sample encoding of 5GS TAI And NCGI field value

Encoding	Octet 0	Octet 1	Octet 2	Octet 3	Octet 4
Encoding when ENABLE_REL18_ENCODING_FOR_NCGI key is disabled	0x00	0x7D	0x40	0x00	0x***F0***
Encoding when ENABLE_REL18_ENCODING_FOR_NCGI key is enabled	0x**0**0	0x07	0xD4	0x00	0x0F

In the above table, when ENABLE_REL18_ENCODING_FOR_NCGI key is disabled, the NR Cell Global Identity (NCGI/NR CGI) value is set first from the left and then the Spare bits are set to zero in the last. The encoded User-Location-Info-3GPP value is as follows:

User-Location-Info-3GPP (22,V,v=10415,I=27) is 0x8932F4510186A432F451007D4000F0

When ENABLE_REL18_ENCODING_FOR_NCGI key is enabled, the encoding is done by first setting the Spare bits as zero from the left and then by setting the NR Cell Global Identity (NCGI/NR CGI) value. The encoded User-Location-Info-3GPP value is follows:

User-Location-Info-3GPP (22,V,v=10415,I=27) is 0x8932F4510186A432F4510007D4000F

Managing Support for Encoding of NR Cell Global Identity (NCGI/NR CGI) in 3GPP-User-Location-Info

Enable and Configure

The support for encoding of NR Cell Global Identity (NCGI/NR CGI) in 3GPP-User-Location-Info AVP can be configured using ENABLE_REL18_ENCODING_FOR_NCGI Advanced Settings key for Diameter Connector. For more information, see Diameter Connector.

4.84 Support for Server Header

PCF handles various requests from consumer Network Functions (NFs) and other network entities over HTTP protocol. On receiving these requests, PCF validates and processes them before responding to these requests. In case, PCF sends an error response, then the consumer NFs need to know the source of the error to trouble shoot the error and take corrective measures. The integration of this feature at PCF helps to determine the originator of the error response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

This feature offers the support for Server Header in PCF responses, which contains information about the origin of an error response and the type of the error encountered. The Server Header includes the type of NF as "NF Type", followed by a “-” and the identity of the NF or the network entity. It is expected to be present in all PCF responses in the following format:

<NF_Type>-<NF_Instance_Id>

Where,

- `<NF Type>` is the type of the NF generating the error.
- `<NF Instance-Id>` is the unique identifier of the NF instance generating the error response.

For example: PCF-54804518-4191-46b3-955c-ac631f953ed8

The inclusion of the Server header in the PCF response is configurable, and can be enabled or disabled using a flag. Also the error codes that are included as part of the Server header in the error response are also configurable. The configuration of these parameters are done through either with REST APIs that are exposed through configuration server or Helm Configurations.

The operation mode that is either `REST` or `HELM` for Server Header configuration is done using the below flag:

```
ingress-gateway:
  serverHeaderConfigMode: REST # Possible values: HELM, REST. Based on this
value, the feature flag for "server"  header will need to be enabled either
in Helm configuration or Rest  configuration.
```

> **Note**
>
> Nf Type and Nf Instance Id are mandatory fields for Server Header to get included in the error response. If either of the fields Nf Type or Nf Instance Id are configured as empty, then the Server Header will not get included in the error response.

Managing Server Header

Enable

By default, this feature is disabled.

You can enable the Server Header feature using Helm or REST API configurations as follows:

- **Helm:** To enable the server header feature using Helm configuration, set the value for parameter `serverHeaderConfigMode` to `HELM` in the `custom-values.yaml` file. Then, set the value for parameter `serverHeaderEnabled.enabled` to `true` under routesConfig for `ingress-gateway`.
  For more information, see the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
- **REST API:** To enable the server header feature using REST configuration, set the value for parameter `serverHeaderConfigMode` to `REST` in the `custom-values.yaml` file. Using REST API, set the `enabled` parameter to `true` in the following resource URI:

  {apiRoot}/PCF/nf-common-component/v1/igw/serverheaderdetails

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see the section Server Header at Ingress Gateway in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the server header feature using the REST API or CNC Console:

- **Configure using REST API:**Perform the REST API configurations in the following sequence to configure this feature:
  1. Configure **serverheaderdetails** to enable the feature.
     {apiRoot}/PCF/nf-common-component/v1/igw/serverheaderdetails
  2. Configure **routesconfiguration** to map route ID and its corresponding route-level configuration.
     {apiRoot}/PCF/nf-common-component/v1/igw/routesconfiguration
  3. Configure **errorcodeserieslist** to update the **errorcodeserieslist** that are used to list the configurable exception or error for an error scenario in Ingress Gateway.
     {apiRoot}/PCF/nf-common-component/v1/{serviceName}/errorcodeserieslist

  > **Note**
  >
  > If you define server header configuration at both global and route levels, the route level configuration takes precedence over the global level configuration.

  For more information, see the "Server Header at Ingress Gateway" section in *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide*.
- **Configure using helm:** When parameter `serverHeaderConfigMode` is set to `HELM` and to configure the Server Header at Ingress Gateway, you need to perform the helm configurations either at Global or at Route level.

```
# All attributes under "serverHeaderDetails" will need to be configured
only if "serverHeaderConfigMode" is set as "HELM"
serverHeaderDetails:
  enabled: true
  errorCodeSeriesId: E1
  configuration:
    nfType: PCF
    nfInstanceId: INS-1

# Use below configuration to define errorCodeSeries list
errorCodeSeriesList:
  # Value of "id" attribute will need to used for assigning
"errorCodeSeriesId" either at Global or Route level conf for Server header.
- id: E1
  errorCodeSeries:
  - errorSet: 4xx
    errorCodes:
    - 400
    - 408
  - errorSet: 5xx
    errorCodes:
    - 500
    - 503
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
- id: E2
  errorCodeSeries:
  - errorSet: 4xx
    errorCodes:
    - -1
```

Following Helm Configuration performed at Route Level:

```
routesConfig:
- id: backend_ms1_route
  uri: https://backend-ms1:8440/
  path: /ms1/**
  order: 1
  metadata:
    # All attributes under "serverHeaderDetails" will need to be
configured only if "serverHeaderConfigMode" is set as "HELM" and Route
level configuration is required. If not defined, Global configurations
will be used
    serverHeaderDetails:
      enabled: true     # Since this flag is set to true at Route level,
"server" header configuration will be enabled for this Route with
respective "errorCodeSeriesId" as E2
      errorCodeSeriesId: E2 # This attribute will need to be defined if
"server" header configuration is enabled at Route level.
- id: backend_ms2_route
  uri: https://backend-ms2:8550/
  path: /ms2/**
  order: 2
  metadata:
    # All attributes under "serverHeaderDetails" will need to be
configured only if "serverHeaderConfigMode" is set as "HELM" and Route
level configuration is required. If not defined, Global configurations
will be used
    serverHeaderDetails:
      enabled: false    # Since this flag is set to false at Route level,
"server" header configuration will be disabled for this Route altogether.
```

> **Note**
>
> If you define server header configuration at both global and route levels, the route level configuration takes precedence over the global level configuration.

For more information, see the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

- **Configure using CNC Console:** A new group, **NF Server Settings** is added to the NF Communication Profile page. For more information, see NF Communication Profiles.

4.85 SBI Timer Handling

PCF-SM service receives requests from ingress Gateway with the help of the following 3GPP headers:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- `3gpp-Sbi-Origination-Timestamp`- contains the date and time (with a millisecond granularity) when the originating entity initiated the request.
- `3gpp-Sbi-Sender-Timestamp`- contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated.
- `3gpp-Sbi-Max-Rsp-Time`- contains the time duration expressed in milliseconds since the absolute time is indicated in the 3gpp-Sbi-Origination-Timestamp header.

The timer profile sets request timeout values for UDR, CHF, BSF, SMF, and AMF messages in applications or interfaces. Policy applies the specific timeout profile while sending requests to external NFs. For more information on managing timer configurations, see Support for Timer Configurations.

The timeout value used towards different interfaces of PCF such as UDR, CHF, BSF, SMF, and AMF also depends on the message communication towards the HTTP server. The message communication towards the HTTP server can be synchronous or asynchronous:

1. Synchronous:
   - When Timer headers are available:
     - When current time is subtracted from the sum of `3gpp-Sbi-Origination-Timestamp` and `3gpp-Sbi-Max-Rsp-Time` and the result is greater than zero, then it is considered as `potential_requestTimeout`. In this case, if the validation fails you must immediately fail the request towards upstream. Thereafter, a similar check is done by the upstream service.
     - If TimerProfile is configured and applicable for a respective interface on service, then the minimum value out of `potential_requestTimeout` or `TimerProfile_value` is taken as request timeout.
     - If TimerProfile is not configured or applicable for respective interfaces, then the minimum value out of `potential_requestTimeout` or `Static timeout value of service` is taken as request timeout. Here, the static timeout value is the value timeout that the user configures in the Helm.
   - When Timer headers are not available:
     - If TimerProfile is configured and applicable for respective interfaces of the service, then `TimerProfile_value` is used as request timeout.
     - If TimerProfile is not configured or applicable for respective interfaces of the service, then static timeout is used as request timeout.
2. Asynchronous
   - If TimerProfile is configured for a respective interfaces on service, then use value of the `TimerProfile` request timeout.
   - If TimerProfile is not configured or applicable for respective interface on service, then set the static timeout as request timeout. While setting the static timeout value, you must ensure that the value of static timeout is greater than any timeout profile value.

The timeout value is calculated as per message instead of per interface. It allows the user to configure a different timeout, whether the UDR connector or NRF interface is sending a Get or Subscribe message. The user can calculate the timeout using UDR messages. For more information on managing the timeout, see Support for Timer Configurations.

Managing SBI Timer

Enable

Copyright © 2019, 2026, Oracle and/or its affiliates.

To enable the SBI Timer Header, set the `isSbiTimerEnabled` parameter to true, under the ingress-gateway configurations in the custom values.yaml file for Policy.

If the `isSbiTimerEnabled` parameter is 'true' then:

- `3gpp-Sbi-Sender-Timestamp`, `3gpp-Sbi-Max-Rsp-Time`, and `3gpp-Sbi-Origination-Timestamp` are used along with route level (if configured) and global level request timeout to calculate final request timeout.
- After calculating the final request timeout, the original values of `3gpp-Sbi-Sender-Timestamp`, `3gpp-Sbi-Max-Rsp-Time`, and `3gpp-Sbi-Origination-Timestamp` are published in the `Orig-3gpp-Sbi-Sender-Timestamp`, `Orig-3gpp-Sbi-Max-Rsp-Time`, and `Orig-3gpp-Sbi-Origination-Timestamp` respective custom headers.

If `isSbiTimerEnabled` is 'false', then the SBI headers are not taken into consideration even if, they are present and the custom headers are not published.

Configure

When `isSbiTimerEnabled` flag is true in Ingress Gateway and publish headers flag is enabled, Egress Gateway needs to get the original value from the corresponding orig header and set it to the 3gpp header. This can be done by adding an entry filter per route in egress gateway section of custom-values.yaml file.

Following is an example of how to configure the entry filter to ensure that the '3gpp-Sbi-Origination-Timestamp' header retains the original value stored in the 'Orig-3gpp-Sbi-Origination-Timestamp' header for the UDR route:

```
routesConfig:
    - id: udr_direct
      uri: http://dummy.dontchange2
      path: /nudr-dr/**
      order: 3
      metadata:
        # Configuration done at route level will take precedence over same
configuration done at global level
        httpsTargetOnly: false
        httpRuriOnly: false
        sbiRoutingEnabled: false
        sbiRoutingWeightBasedEnabled: false
        configurableErrorCodes:
          enabled: false
          #errorProfileName are always defined at global level
          errorScenarios:
            - exceptionType: "VIRTUAL_HOST_RESOLUTION_ERROR"
              errorProfileName: "ERR_114"
            - exceptionType: "INVALID_OAUTH_TOKEN_REQUEST"
              errorProfileName: "ERR_115"
            - exceptionType: "OAUTH_INTERNAL_ERROR"
              errorProfileName: "ERR_115"
            - exceptionType: "OAUTH_TOKEN_RETRIEVAL_FAILURE"
              errorProfileName: "ERR_115"
            - exceptionType: "OAUTH_NRF_RESPONSE_FAILURE"
              errorProfileName: "ERR_115"
            - exceptionType: "CONNECTION_TIMEOUT"
              errorProfileName: "ERR_100"
            - exceptionType: "REQUEST_TIMEOUT"
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
        errorProfileName: "ERR_200"
filterNameReqEntry:
  name: CustomReqHeaderEntryFilter
  args:
    headers:
      - methods:
          - ALL
        headersList:
          - headerName: 3gpp-Sbi-Origination-Timestamp
            defaultVal: <default_value>
            source: incomingReq
            sourceHeader: Orig-3gpp-Sbi-Origination-Timestamp
```

You can configure the parameters for SBI Timer by updating the custom-values.yaml file for Policy. For more information about configuring the parameter value, see *Late Arrival Handling Configuration* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

Observe

The `ocpm_udr_tracking_request_timeout_total`, `ocpm_udr_tracking_request_timeout_total`, `ocpm_egress_request_timeout_total`, and `ocpm_timeout_total` metrics are applicable for SBI timers. For information related to SBI Timer metrics, see CNC Policy Metrics .

4.86 Detection and Handling of Late Arrival Requests

PCF Service receives requests from Ingress Gateway with the 3GPP headers. These requests help in the detection of the response time for the SM service. Following headers are received from the Ingress Gateway:

- `3gpp-Sbi-Origination-Timestamp`- It contains the timestamp when the originating entity initiates the request.
- `3gpp-Sbi-Max-Rsp-Time`- It contains the time duration expressed in milliseconds since the absolute time is indicated in the 3gpp-Sbi-Origination-Timestamp header.
-
- `3gpp-Sbi-Sender-Timestamp`- It contains the date and time (with a millisecond granularity) at which an HTTP request or response is originated from the previous NF.

PCF must be able to read the `3gpp-Sbi-Origination-Timestamp` and `3gpp-Sbi-Max-Rsp-Time` headers to be able to respond as per the request. The following scenarios can be considered:

- If the sum of `3gpp-Sbi-Origination-Timestamp` and 3gpp-Sbi-Max-Rsp-Time is less than the current time, the PCF service must reject the message with a 504 HTTP code and the message: "TIMED_OUT_REQUEST".
- If the request does not include either `3gpp-Sbi-Origination-Timestamp`, `3gpp-Sbi-Sender-Timestamp`, or `3gpp-Sbi-Max-Rsp-Time` headers, then this request is accepted and the call flow continues as normal with the inclusion of collision detection.
- If `3gpp-Sbi-Max-Rsp-Time` receives a negative value, this header is considered invalid. In this case, the service falls back to the default behavior and accepts the request irrespective of the origination/Sender timestamp value.

Copyright © 2019, 2026, Oracle and/or its affiliates.

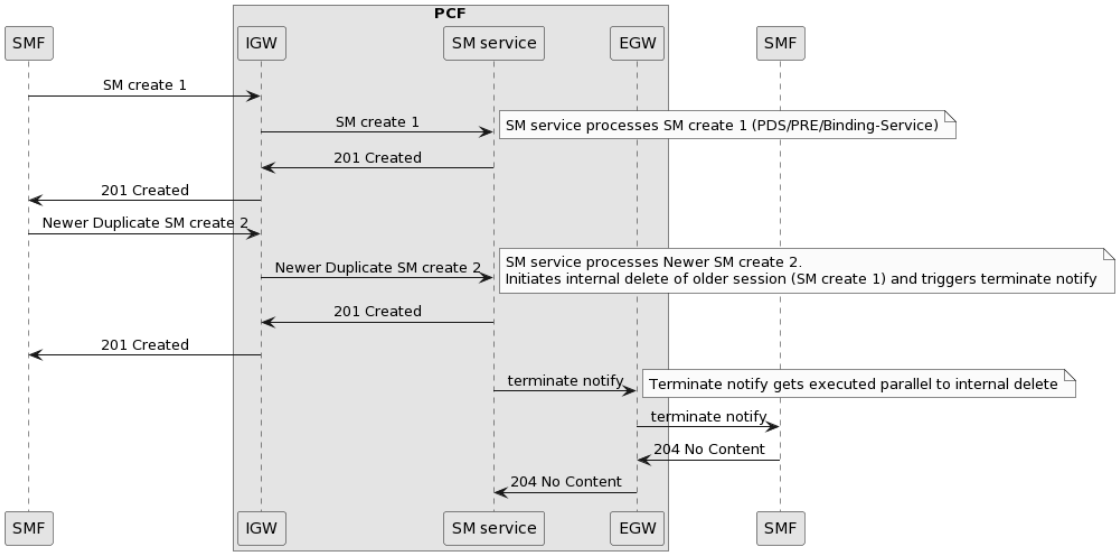
In case of collision detection, PCF needs to trigger a cleanup internally on the rest of the services so that there is only one association per user at a time.

Collision Detection of SM PDU Sessions

When SM Service receives a new SM PDU Session Create request and if the value of `SYSTEM.COLLISION_DETECTION.TERMINATE_NOTIFY.ENABLED` advanced settings key is set to `true`, SM Service detects and cleans up duplicate requests of SM Sessions (Collision Detection) and sends Terminate Notify to SMF when .

SM service deletes the older session from SMPolicyAssociation database and sends the Terminate Notify request to SMF.

Figure 4-184 Sample call flow for sending Terminate Notify when duplicate session is found (collision detection) and SM service cleans up the older session from database



1. SM service receives a SM CREATE request from SMF through Ingress Gateway.
2. SM service sends a GET request to PDS to get the subscriber details from UDR, initiates a binding session request with Binding Service and then sends a request to PRE for policy evaluation. After the session is successfully created, SM services responds to SMF with 201 created message.
3. SM service receives another CREATE request from SMF, which is a duplicate of the session that is already created.
4. SM service processes the new CREATE request and deletes the older session.
5. SM service sends a Terminate Notify message to SMF through Egress Gateway.
6. After deleting the details of the older session, SMF responds to SM service with 204 No Content message.

Managing Late Arrival requests and Collision Detection

Enable

The detection and handling of late arrival feature can be enabled or disabled using `ENABLE_LATE_ARRIVAL` parameter. For more information about configuring the parameter

Copyright © 2019, 2026, Oracle and/or its affiliates.

value, see *Detection and Handling of Late Arrival Requests* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

For collision detection, the **SYSTEM.COLLISION.DETECTION** parameter is available to the user. It is set to false, by default. When the parameter is set to true, PCF-SM checks for collision in the SMPolicyAssociation table, based on User Equipment information (that is. SUPI) and the PDU Session ID.

PCF-UE and PCF-AM checks for collision in the UEPolicyAssociation and AMPolicyAssociation table respectively, based on User Equipment information (that is. SUPI).

Configure

You can configure the parameters for late arrival handling by updating the custom values file for Policy. For more information about configuring the parameter value, see *Detection and Handling of Late Arrival Requests* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Observe

Policy provides metrics specific to late arrival requests and collision detection. For information related to late arrival requests and collision detection metrics, see Late Arrival Requests and Collision Detection Metrics .

4.86.1 PCF Support for Detection and Handling of Late Arrival Requests in BSF

Each microservice propagates the 3gpp-Sbi-Origination-Timestamp header and updates the 3gpp-Sbi-Sender-Timestamp from PCF to BSF with the current timestamp when it receives a request from SMF or SCP.

For adding Detection and Handling of Late Arrival functionality in BSF, it is necessary to make sure these headers and a new Custom header are propagated from PCF to BSF. Moreover, as required by the user, PCF supports to set the value of Custom-Sbi-Sender-Timestamp header.

To create Custom-Sbi-Sender-Timestamp it is necessary to add the following configuration to PCF ingress-gateway:

```
routesConfig:
    - id: sm_create_session_route
      uri: http://{{ .Release.Name }}-occnp-pcf-sm:
{{ .Values.global.servicePorts.pcfSmServiceHttp }}
      path: /npcf-smpolicycontrol/*/sm-policies
      order: 1
      method: POST
      readBodyForLog: true
      filters:
        subLog: true,CREATE,SM
        customReqHeaderEntryFilter:
          headers:
            - methods:
              - POST
              headersList:
                - headerName: 3gpp-Sbi-Message-Priority
                  defaultVal: 24
                  source: incomingReq
                  sourceHeader: 3gpp-Sbi-Message-Priority
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
                override: false
              - headerName: Custom-Sbi-Sender-Timestamp
                defaultVal: func:currentTime(EEE, d MMM yyyy HH:mm:ss.SSS
z,gmt)
                source: incomingReq
                sourceHeader: 3gpp-Sbi-Sender-Timestamp
                override: false
```

4.87 Support for Session Retry and Alternate Route Service

For previous releases, Policy and PCF were configured with primary and secondary NRF or SCP statically by limiting to a specific number. Starting with release 1.8.0, Policy provides the Session Retry functionality. This feature enables the alternate recovery mechanisms to mitigate the impact of any unavailable resource. The policy system provides flexible and configurable retry behavior for selected interfaces.

A retry profile specifies when and how signaling messages from one network function to another are retried or rerouted on failures. Policy supports retry and reroute mechanisms for both initial messages and subsequent messages, based on the configured retry profile.

For initial messages, Policy can retry or reroute the request based on the configured failure handling and alternate route settings. For subsequent messages, Policy must be able to identify the alternate destination from DNS-SRV resolution, binding information received in the 3gpp-Sbi-Binding header, or binding information available from the NF profile.For example, if heartbeat messages that PCF sends to NRF fail consistently, PCF can choose a different available NRF, such as a secondary or next-priority NRF, for subsequent heartbeat messages. Similarly, retry or reroute mechanisms can be applied to messages and subsequent messages towards peer NFs based on the configured retry profile.

Policy supports the session retry functionality for failed notifications. In case of a notification towards SMF fails, then the PCF sends an On-Demand discovery towards NRF based on the SetID received in the CREATE or UPDATE request from the SMF as part of the *3gpp-Sbi-Binding* header. NRF performs a SetID based resolution and sends back a list of NFs under the same SetID. PCF selects the alternate SMF based on the configurations and sends the next notification.

> **Note**
>
> For retry or reroute of initial messages, configure the retry profile and alternate route settings as required.
> For reroute of subsequent messages, at least one of the following conditions must be met:
>
> - Enable DNS Resolution is enabled and DNS-SRV records are configured for the corresponding FQDN.
> - Use Binding Information from Binding Header is enabled and the NF sends the required binding information in the 3gpp-Sbi-Binding header in the CREATE or UPDATE request.
> - Use Binding Information from NF Profile is enabled. When NF Set Resolution is configured as Cached NF Profile, the cached NF profile must include NFSetIdList. For more information about these configurations, see Managing Session Retry and Alternate Route Service.

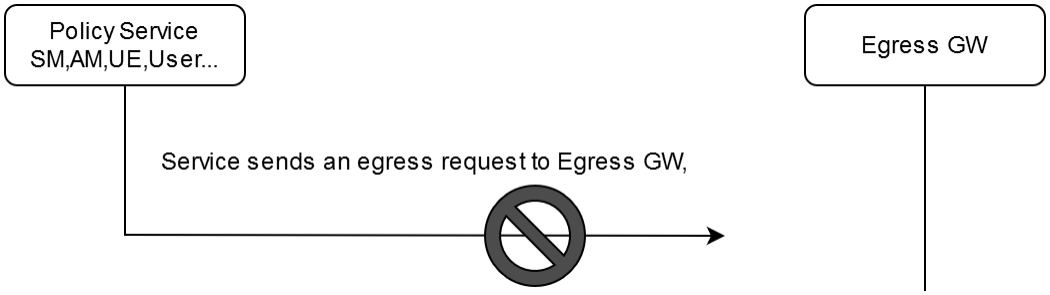
Copyright © 2019, 2026, Oracle and/or its affiliates.

Retry

Retry is initiated when PCF microservices initiate an egress request, but it fails to reach the egress gateway. The reason can be connection failure or Aspen Service Mesh failure. Session retry enables alternate recovery mechanisms to mitigate impact of any unavailable resource. Policy system provides flexible and configurable retry behavior for selected interfaces. You can configure retry profile for the following destination NFs: UDR, CHF, BSF, SMF, AMF, and AF through CNC Console.

The following figure shows a scenario when PCF microservice initiates an egress request, but it fails to reach the egress gateway:

Figure 4-185 PCF Microservice Initiates Egress Request



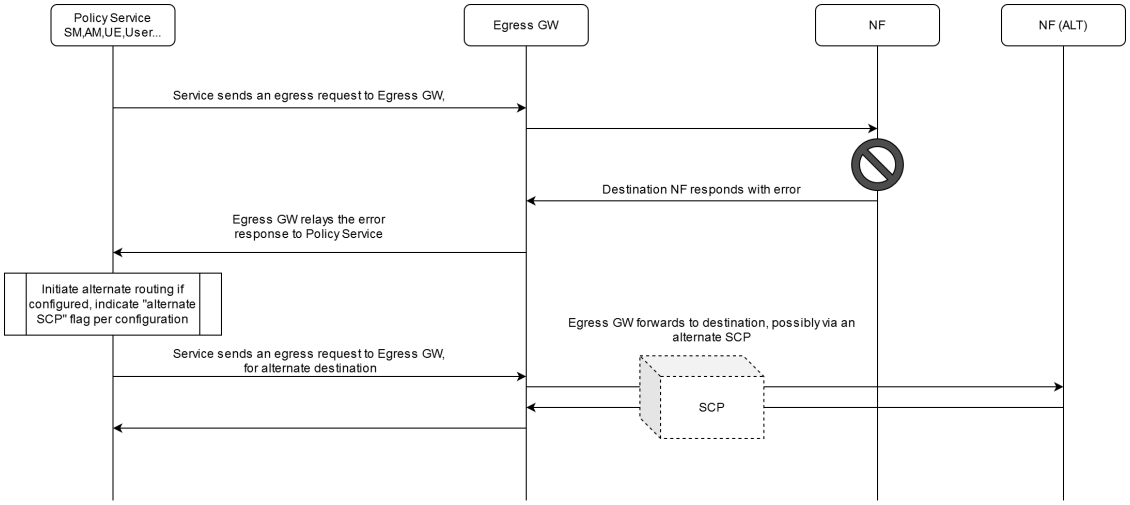
Alternate routing

Alternate routing is initiated when Egress Gateway fails to reach an external NF, an external NF returns a configured error code, or an external NF does not respond. The alternate destination can be selected by using static alternate route configuration, DNS-SRV records, binding information from the binding header, or binding information from the NF profile. For subsequent messages, Policy requires DNS-SRV resolution, binding header information, or NF profile based binding information to identify the alternate destination. For more information about static and DNS-SRV configurations, see "Configurable Parameters for Alternate Route Service Configuration" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

The following figure shows a scenario when egress gateway reaches the NF, but NF responds with an error code:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-186 Egress Gateway get Error Response



To support this behavior, PCF provides the capability to perform DNS SRV Query. The DNS SRV Query discovers the NFs, such as NRF, SCP, and alternate producers. It also notifies consumers during failures to enable the retry mechanisms. This feature provides support to configure virtual FQDNs and adds capability to perform DNS SRV or local configuration Look up to retrieve alternate failover NFs which can be maintained dynamically at the DNS Server.

With SRV Records, you can configure and maintain NF FQDN dynamically at the DNS Server, which can be further selected by Policy, when there is a NF failure. This is achieved by performing a SRV query on the virtual FQDN configured at the Policy, rather than configuring primary and secondary NRF or SCP, statically in every Policy, only during instantiation time. This option of DNS lookup for SRV records would also provide alternate NFs to the Policy during failover.

Egress Gateway

Policy supports session retry functionality at Egress Gateway. When Egress Gateway receives HTTP error response based on the matching `errorcriteria`, there is retry of failed request through an alternate SCP based on the defined `erroractionset`. The `errorcriteria` defines matching HTTP methods, status codes, and causes (optional). The `erroractionset` defines number of reattempted counts and blacklist configurations. The respective `errorcriteria` and `erroractionset` should be mapped to the `routesConfig`.

The following sample shows the mapping of `errorcriteria` and `erroractionset` with `routesConfig`:

```
routesConfig:
 - id: scp_direct2
   uri: https://dummy.dontchange2
   path: /<Intended Path>/**
   order: 3
   metadata:
    httpsTargetOnly: false
    httpRuriOnly: false
    sbiRoutingEnabled: false
   filterName1:
     name: SbiRouting
     args:
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
       peerSetIdentifier: set0
       customPeerSelectorEnabled: false
       errorHandling:
        - errorCriteriaSet: scp_direct2_criteria_1
          actionSet: scp_direct2_action_1
          priority: 1
        - errorCriteriaSet: scp_direct2_criteria_0
          actionSet: scp_direct2_action_0
          priority: 2


- id: scp_direct2_criteria_1
    method:
      - GET
      - POST
      - PUT
      - DELETE
      - PATCH
    response:
      cause:
        ignoreCauseIfMissing: false
        path: ".cause"
        reason:
         - "cause-1"
         - "cause-2"
      statuses:
        - statusSeries: 4xx
          status:
            - 400


- id: scp_direct2_action_0
   action: reroute
   attempts:2
   blackList:
    enabled: false
    duration: 60000
```

`errorcriteria` can also be configured only with the status code. Following is the sample:

```
sbiRoutingErrorCriteriaSets:
 - id: scp_direct2_criteria_1
    method:
      - GET
      - POST
      - PUT
      - DELETE
      - PATCH
    response:
      statuses:
        - statusSeries: 4xx
          status:
            - 400
            - 404
        - statusSeries: 5xx
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
status:
  - 500
  - 503
```

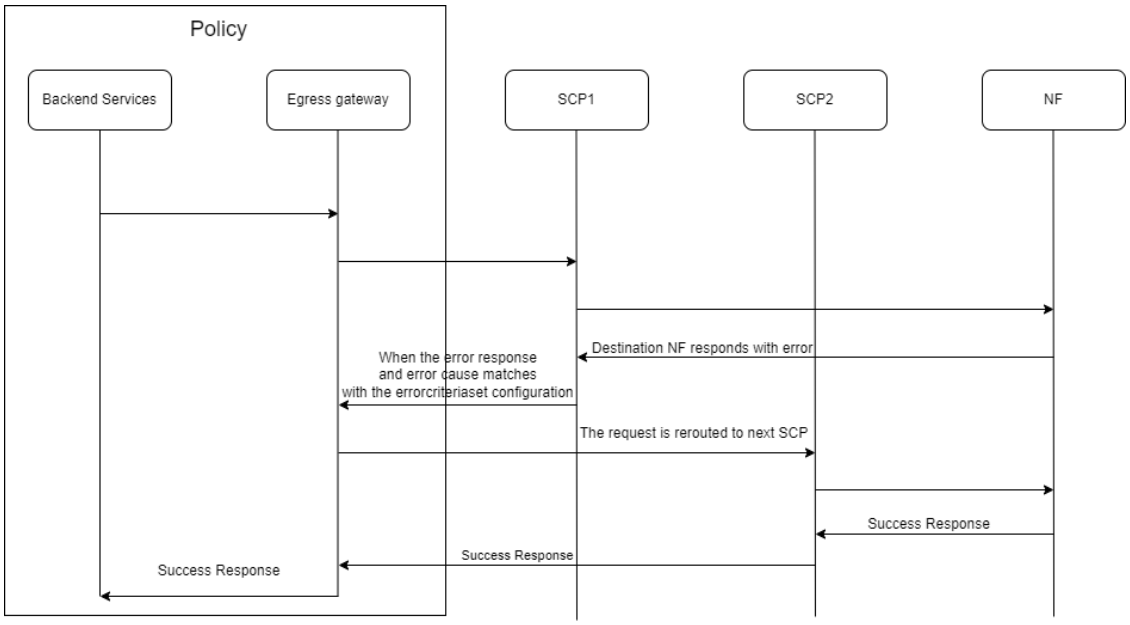
Following are the different use cases:

- When the HTTP response is received at the Egress Gateway only with the error code, then the error code is matched with the `errorcriteriaset` and rerouted to alternate SCP.
- When the HTTP response is received at the Egress Gateway with error code and error cause, then the error code and error cause is matched with the `errorcriteriaset` and rerouted to alternate SCP.
- When configured path is not found in the response and `ignoreCauseIfMissing` is `true`, then the response is received at Egress Gateway from SCP.
- When configured path is not found in the response and `ignoreCauseIfMissing` is false, then the response is sent back to Policy.
- When the cause is empty or null in the response body, `errorcriteria` is not considered as a match irrespective of `ignoreCauseIfMissing` is true or false and corresponding `erroractionset` is not executed.

For more information on configuration, see "SCP Configurations" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

The following diagram shows a scenario when the NF sends the error code and rerouting to alternate SCP is performed.

Figure 4-187 Session Retry at Egress Gateway



Policy sends the service request to the NF through SCP. When the NF sends the error code with cause to the Egress Gateway, the Egress Gateway compares the error code and error cause with `errorcriteriaset`. When it matches, it reroutes the request based on the erroractionset to the alternate SCP. If the maximum reattempts exhausts, the request is sent back to Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Using Binding Headers, NFSets, and Server Headers

Policy supports session retry and alternate routing using Binding Headers, NFSets, and Server Headers.

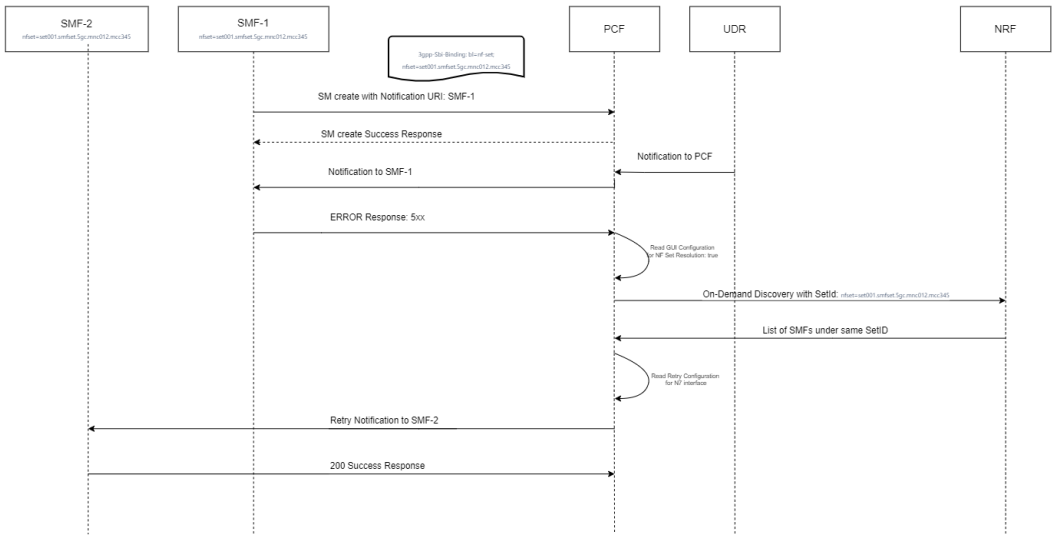
When indirect communication model is selected without delegated discovery, when the target NFs throw errors, SCP performs the task of reselecting target NFs to perform service operations. The reselection of alternate target NFs is based on various considerations such as binding headers, NFSets, and server headers sent by the HTTP client or consumer. In certain scenarios, reselection is based on error response and server headers as well. This feature also determines the action for Policy when no retry is required and all attempts are exhausted by SCP.

Session Retry for Notifications on N7 Interfaces

Policy supports the session retry functionality for failed notifications over N7 interface.

The following diagram depicts an example call flow for retry notification from UDR to SMF:

Figure 4-188 On demand NF Discovery is enabled (NF Set Resolution is set to NRF Discovery)



The call flow is explained as follows:

1. SMF 1 sends an SM Create request with the notification URI towards UDR. The request binding header contains the NFSetID.
2. After successful processing of the request, UDR sends a notification to SMF 1 through PCF.
3. On notification failure, SMF 1 sends a notification failure response with the error code to PCF.
4. PCF checks the Retry Profile configurations and if the value for the NF Set Resolution parameter under the Retry Profile configurations in Policy is set to **NRF Discovery**, then it performs an on demand discovery with SetID through NRF and receives the list of SMFs with the same SetID as SMF 1.
5. PCF retries sending the notification to SMF 2 based on the NFSetID list and receives *200 Success* response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing Session Retry and Alternate Route Service

Enable

You can enable the Retry Profile and Alternate Routing functionality using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** Enable the **Retry on Internal Send Failure** and **Enable Alternate Routing** parameters on the **Retry Profile** page. For more information about enabling the feature through CNC Console, see Retry Profiles.

  Retry Subscription Message enables the operator to choose Retry Logic for SUBSCRIBE/POST. For more information about retry subscription message, see PCF User Connector.
- **Enable using REST API:** Set the **enableRetry** and **enableAlternateRouting** parameter value to **true** in the **Retry Profile** configuration API. For more information about enabling the feature through REST API, see "Retry Profile" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the Retry Profile and Alternate Routing functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations on the **Retry Profile** page. For more information about configuring audit service, see Retry Profiles.
- **Configure using REST API:** Policy provides the following REST API for Session Retry and Alternating Routing configuration:
  API: {apiRoot}/oc-cnpolicy-configuration/v1/services/common/retryprofiles

  You can perform the POST, PUT, or GET operations to configure the feature. For more information about REST API configuration, see "Retry Profile" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

You can configure the parameter for alternate route service by updating the custom values file for Policy. For more information about configuring the parameter value, see "Alternate Route Service Configuration" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*

Observe

Policy provides the Alternate Routing request and response metrics in the User Services. For more information, see User Service Metrics.

4.88 Support for Honor retry-after Header in Egress Gateway

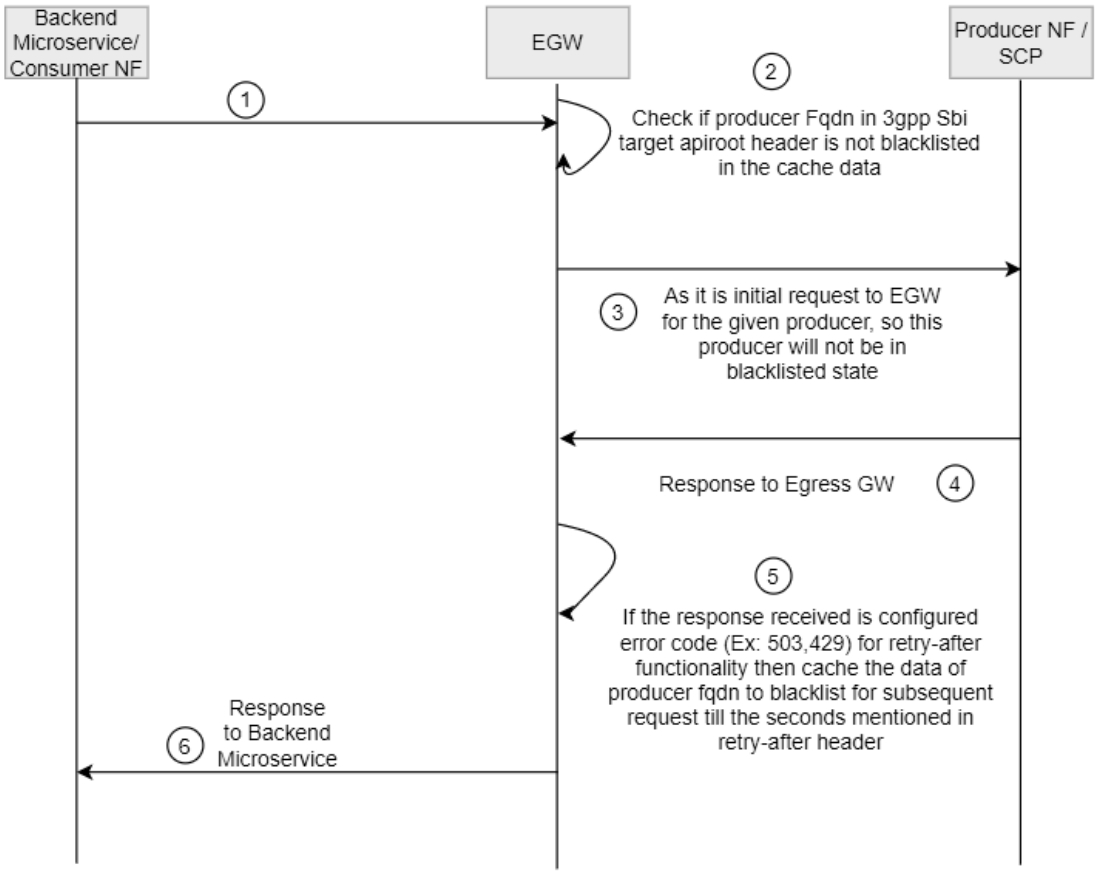
This section describes the `retry-after` header functionality in Egress Gateway. This header is received as a response, from the Egress gateway. Based on the header information, the producer data is collected to block the producer FQDN for the number of seconds mentioned in the `retry-after` header.

Initial Call for Producer FQDN

The following call flow describes the initial call to Egress Gateway from the Producer FQDN:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-189 Initial CallS for Producer FQDNs



The initial call for producer FQDN is explained as follows:

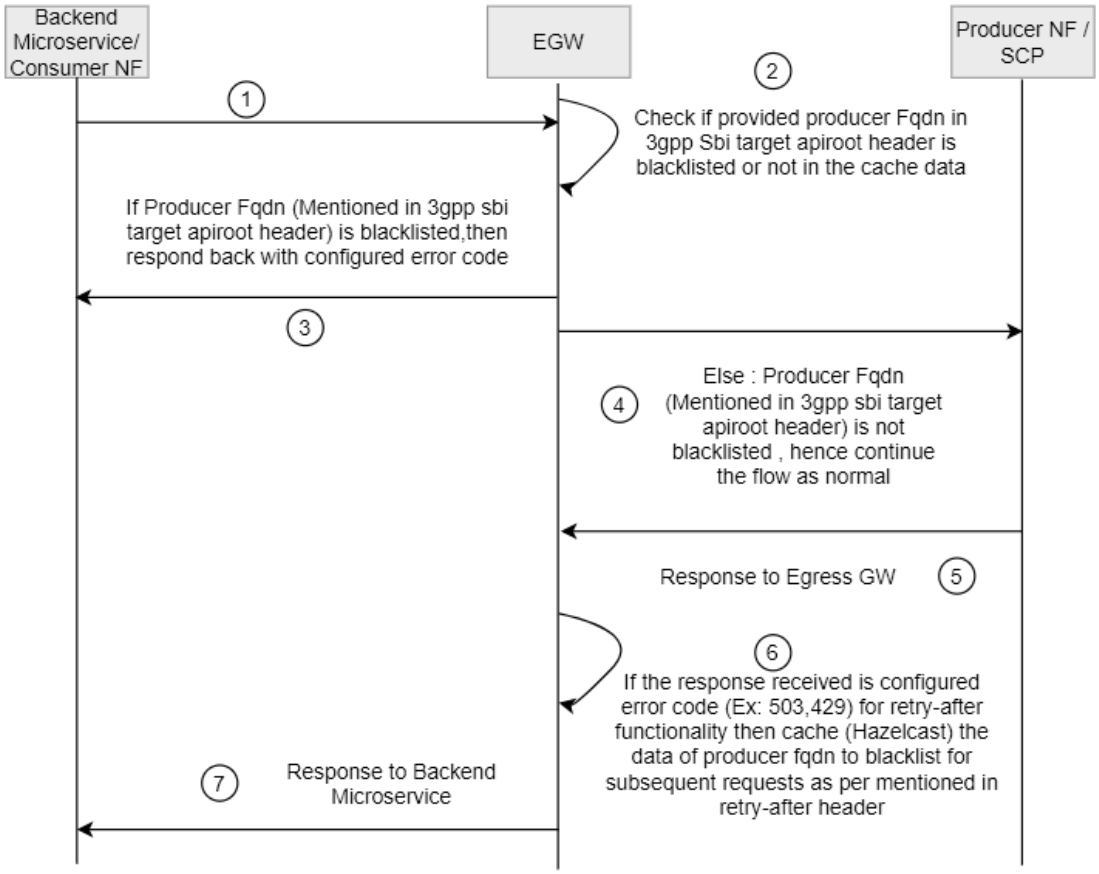
1. The backend microservice or the consumer NF sends request to Egress Gateway.
2. The Egress Gateway verifies that the producer FQDN available in 3GPP SBI target apiroot header is not blocked.
3. Since, this is an initial request to Egress Gateway for the given producer, the producer FQDN is not blocked and the request is sent to the producer NF or SCP.
4. The producer NF or SCP sends a response to Egress Gateway.
5. If the response received by Egress Gateway is a configured error code, such as 503 or 429 for retry-after functionality, then the Egress Gateway cache the producer FQDN data to blocklist. It blocks the subsequent requests for the number of seconds mentioned in the `retry-after` header.
6. Egress Gateway sends a response to back end microservice or consumer NF that includes the `retry-header`.

Subsequent Call for Producer FQDN

The following call flow describes the subsequent call to Egress Gateway from the Producer FQDN:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-190 Subsequent Calls for Producer FQDN



The subsequent call for producer FQDN is explained as follows:

1. The backend microservice or the consumer NF sends request to Egress Gateway.
2. The Egress Gateway verifies that the producer FQDN available in 3GPP SBI target apiroot header is not blocked.
   - If the producer FQDN available in 3gpp SBI target apiroot header is blocked, then the Egress Gateway responds back to the backend microservice or consumer NF with the configured returnErrorCode.
   - If the producer FQDN available in 3gpp SBI target apiroot header is not blocked, then the flow continues by sending request to producer NF / SCP.
3. The producer NF or SCP sends a response to Egress Gateway.
   - If the response received by Egress Gateway is a configured error code, such as 503 or 429 for retry-after functionality, then the Egress Gateway cache the producer FQDN data to blocklist. It blocks the subsequent requests for the number of seconds mentioned in the `retry-after` header.
   - If the response received by Egress Gateway does not have any configured error code, then no producer FQDN data is collected to be blocked.
4. Egress Gateway sends a response to backend microservice or consumer NF that includes the `retry-header`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing Honor retry-after Header in Egress Gateway

Enable and Configure

To enable this feature in Policy, set the **egress-gateway.retryAfter.enabled** parameter to **true** under the `egress-gateway` configurations in the custom-values.yaml file for Policy.

Here is a sample configuration for this feature in custom-values.yaml file for Policy:

```
egress-gateway:
   retryAfter:
    enabled: true
    errorCodesToLook: 429,503
    #Provide error code with comma separated and no space
    returnErrorCode: 425
    #Error code expected to be sent to Backend NF when 3gpp-Sbi-Target-
    Apiroot header
    is provided with producer and request route/path which is blacklisted
    in egress
    gateway for a period mentioned in retry-after header
    blacklist-period: 0 #Seconds
    #This value is used when configured response code's are received from
    producer NF
    but retry-after header is absent. If retry-after value is configured
    with any
    value greater than 0 then it is considered in the absence of retryafter
    header from
    producer NF.
```

4.89 Stale Session Handling

Policy offers the signaling services such as, SM service, AM service, UE service, Binding Management service, Policy DS and, so on. These services are stateless in nature, thereby offloading session state to the centralized Oracle MySQL database (DB) for Policy.

As the session processing microservices and the DB are different components that communicate over a network, there are chances for certain transaction failures during transit. For example, failures can occur in overload situations or as a result of code bugs. To manage such failed transactions, Policy provides a database audit mechanism that monitors the stale records and clean them up to not exhaust the database memory. The audit mechanism also notifies the microservice about the stale records so that the service can trigger signaling messages, if required. The stale session handling functionality ensures that the stale sessions are released by the consumer NFs. If applicable, the feature also releases the associated sessions from the same or other NFs. For example, deleting a stale SM association may require to delete the associated PA sessions.

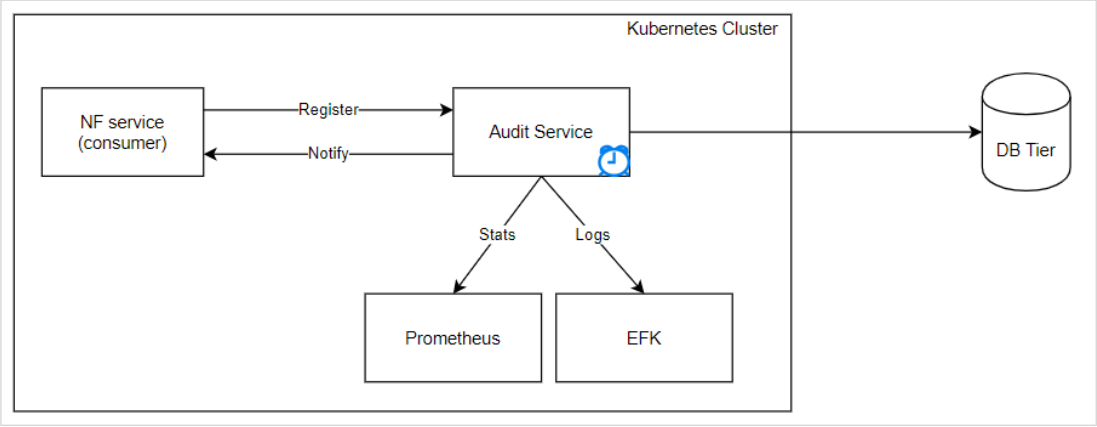
Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Policy supports the stale session handling for the following services:
>
> - SM service
> - AM service
> - PCRF Core
> - PDS
> - Binding service
> - UE Service
> - Usage Monitoring Service

Feature Design

The following diagram provides a high level design for stale session handling through session state Audit service:

Figure 4-191 High Level Design for Stale Session Handling using Audit Service



As shown in the above diagram:

1. The Policy service registers as a consumer with the Audit service and starts auditing the service database.
2. When a stale record is detected, the Audit service takes any of the following actions as requested by the Policy service during the registration:
   - Deletes the stale records from the database.
   - Sends a notification to the service about the stale records.
   - Deletes the stale records from the database and notify the service.
3. The Audit service implements a minimum wait time between consecutive audits and the consecutive notifications for the same record.

Copyright © 2019, 2026, Oracle and/or its affiliates.

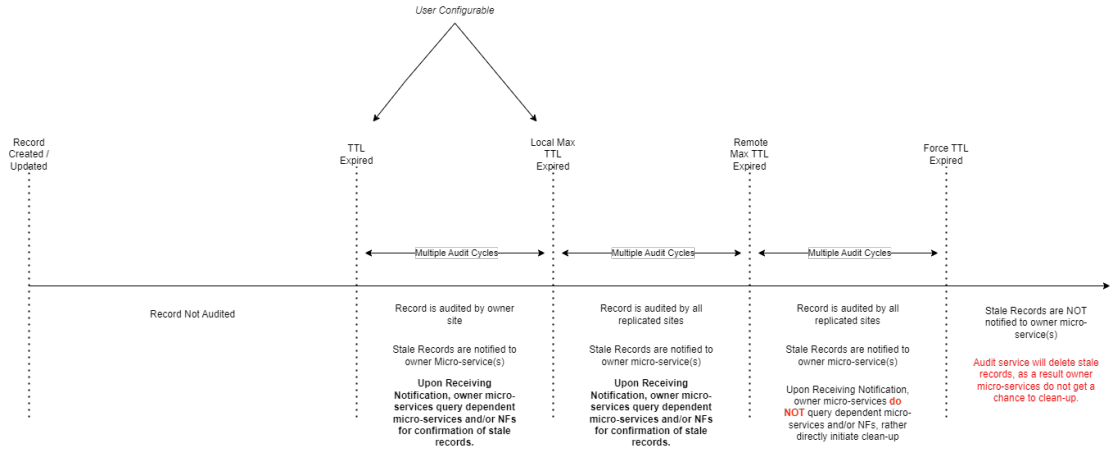
> **Note**
>
> - The Audit service stores the service registration details in the DB to be recovered after the pod restart or upgrade.
> - The audit service supports the local time zone.

Call Flow

Timeline View of Audit Service

The following figure shows a time line view of the Audit service for a record:

Figure 4-192 Timeline view of Audit Service

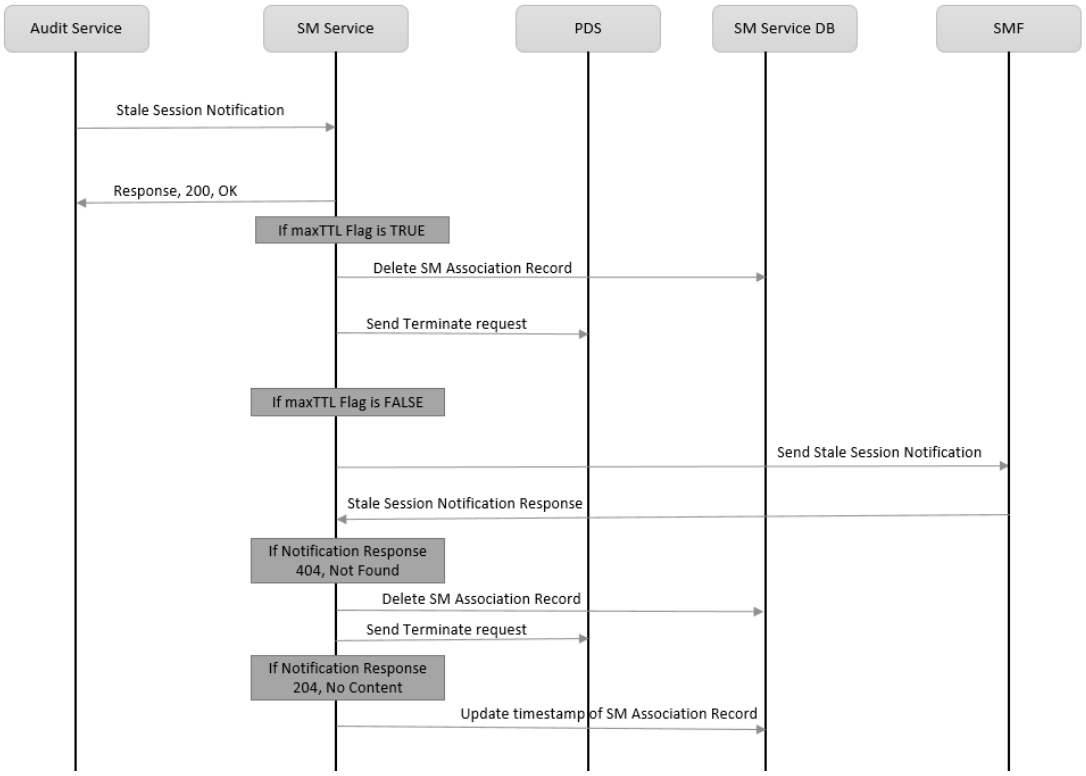


Stale Session Detection and Handling in SM Service

The following figure shows an example call flow of handling of stale session notification by the Policy SM service:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-193 Example call flow for Stale Session Detection and Handling in SM Service



As shown in the call flow, after receiving a stale session notification from Audit service, SM service checks the `maxTtl` flag status and takes the following actions :

- If the `maxTtl` flag is **TRUE** then SM service triggers the TERMINATE action and deletes the record from the database.
- If the **maxTtl** flag is **FALSE** then SM service triggers another notification towards SMF to check if the particular SM association record exists with SMF:
  - If SMF responds with `204, No Content` status code then SM will **update** the timestamp of the SM Association record.
  - Else if SMF responds with `404, Not Found` status code then SM service triggers the TERMINATE action and deletes the record from the database..

Sending Terminate Notify to SMF

SM Service sends Terminate Notify to SMF when it detects and cleans up duplicate requests of SM PDU Session Create (Collision Detection) and stale SMPolicyAssociation (Max TTL reached for session).

When Audit service sends a notification to SM service that Max TTL has reached and if the value of `AUDIT_SMPOLICY_ASSOCIATION.MAX_TTL.TERMINATE_NOTIFY.ENABLED` advanced settings key is set to `true`, the details are deleted from the SMPolicyAssociation database. Also, a Terminate Notify is sent to SMF. SMF performs the appropriate action to remove the stale SMPolicyAssociation.

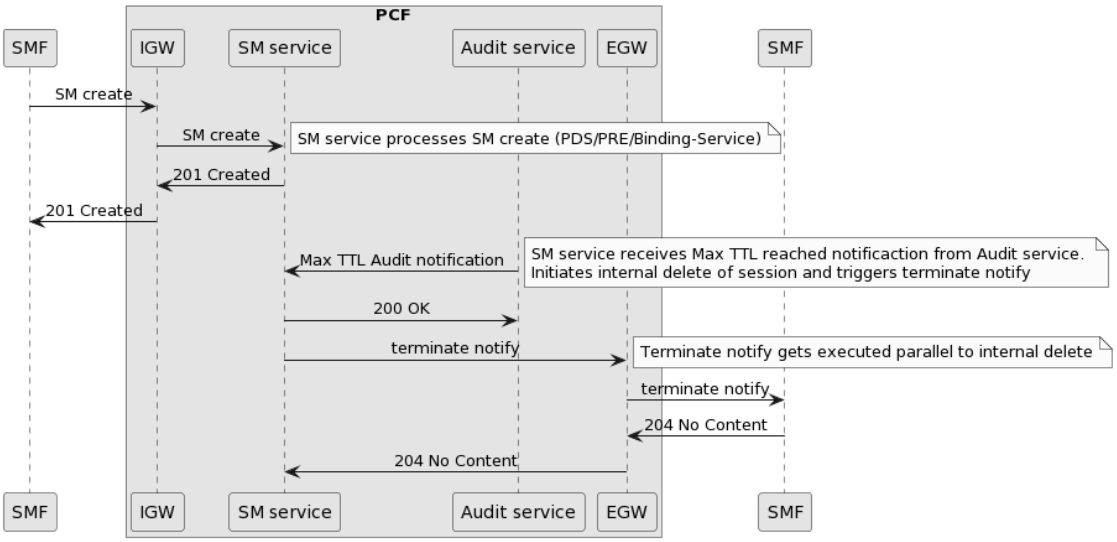
Also, when a newer session is received, SM service checks if the value of `SYSTEM.COLLISION_DETECTION.TERMINATE_NOTIFY.ENABLED` advanced settings key is set to

Copyright © 2019, 2026, Oracle and/or its affiliates.

`true`. It identifies the new session as duplicate and deletes the older session from SMPolicyAssociation database. Also, SM service sends a Terminate Notify to SMF.

For details on collision detection of duplicate Create session requests, see Detection and Handling of Late Arrival Requests.

Figure 4-194 Sample call flow for sending Terminate Notify when Max TTL notification is received from Audit service.



1. SM service receives a SM CREATE request from SMF through Ingress Gateway.
2. SM service sends a GET request to PDS to get the subscriber details from UDR, initiates a binding session request with Binding Service and then sends a request to PRE for policy evaluation. After the session is successfully created, SM services responds to SMF with 201 created message.
3. When the MaxTTL for the session is reached, the Audit service sends a MaxTTL Audit notification to SM service. SM service deletes the session details from its local SMPolicyAssociation database and then sends a Terminate Notify message to SMF through Egress Gateway.
4. After deleting the details of the older session, SMF responds to SM service with 204 No Content message.

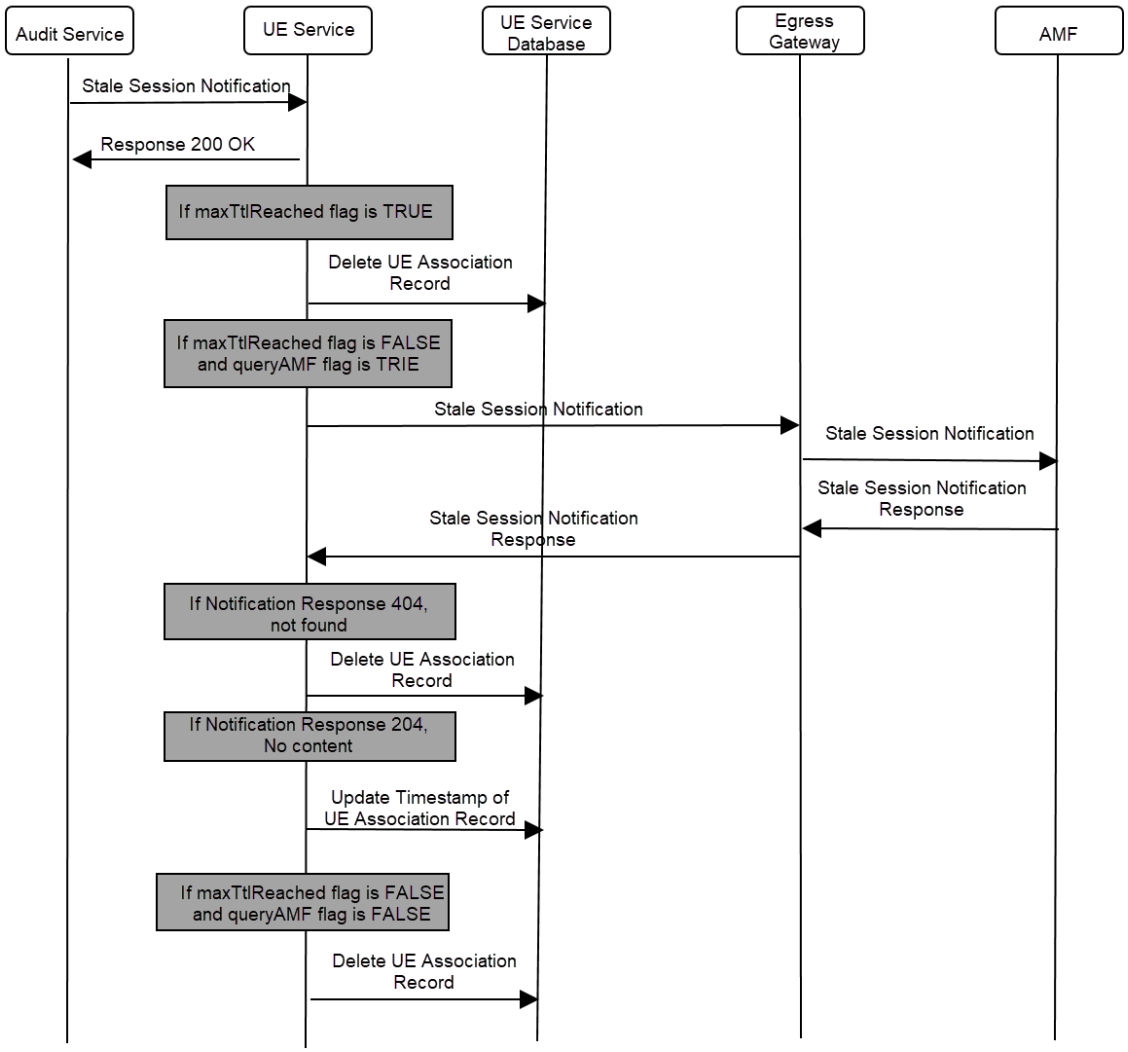
Stale Session Detection and Handling in UE Service

A UE Policy Association on PCF is considered as stale when the association exists in PCF, but has no corresponding session on the AMF.

When a UE Policy Association is detected as stale, the UE service deletes the association from the database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-195 Example call flow for Stale Session Detection and Handling in UE Service



As shown in the call flow, after receiving a stale session notification from Audit service, UE service checks the status of `maxTtlReached` and `queryAMF` flags and takes the following actions:

- If the `maxTtlReached` flag is `TRUE`, the UE service triggers the TERMINATE action and deletes the record from the database.
- If the `maxTtlReached` flag is `FALSE` and `queryAMF` flag is `TRUE`, the UE Service sends the stale session notification to AMF via the Egress Gateway to check whether this particular UE Association record exists with AMF.

  The AMF replies with a stale session notification response to UE service.

  - If the stale session notification response includes a `404 Not Found` status code, the UE Service triggers the TERMINATE action and deletes the record from the database.
  - If the stale session notification response includes a `204 No Content` status code, the UE Service updates the timestamp of the UE Association record in the database.

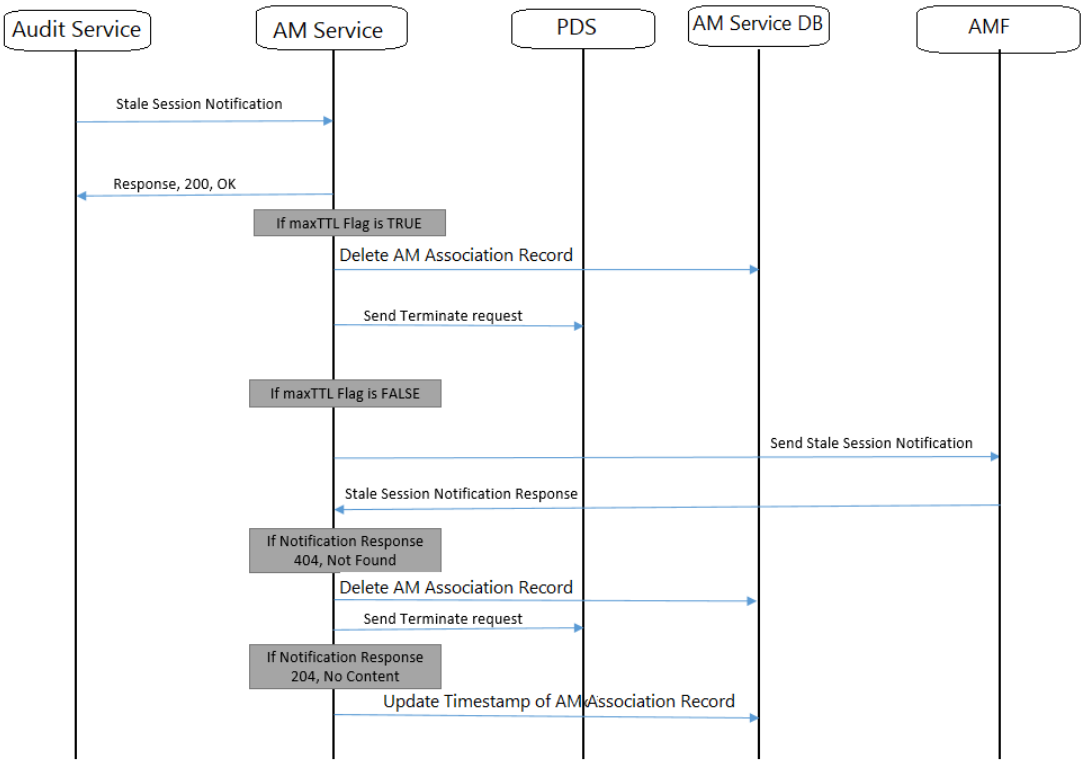
Copyright © 2019, 2026, Oracle and/or its affiliates.

If either AMF does not respond, or is not reachable, no action is taken until `maxTtlReached` is reached.

- If the `maxTtlReached` flag is `FALSE` and `queryAMF` flag is `FALSE`, the UE Service triggers the TERMINATE action and deletes the record from the database.

Stale Session Detection and Handling in AM Service

Figure 4-196 Example call flow for Stale Session Detection and Handling in AM Service:



.

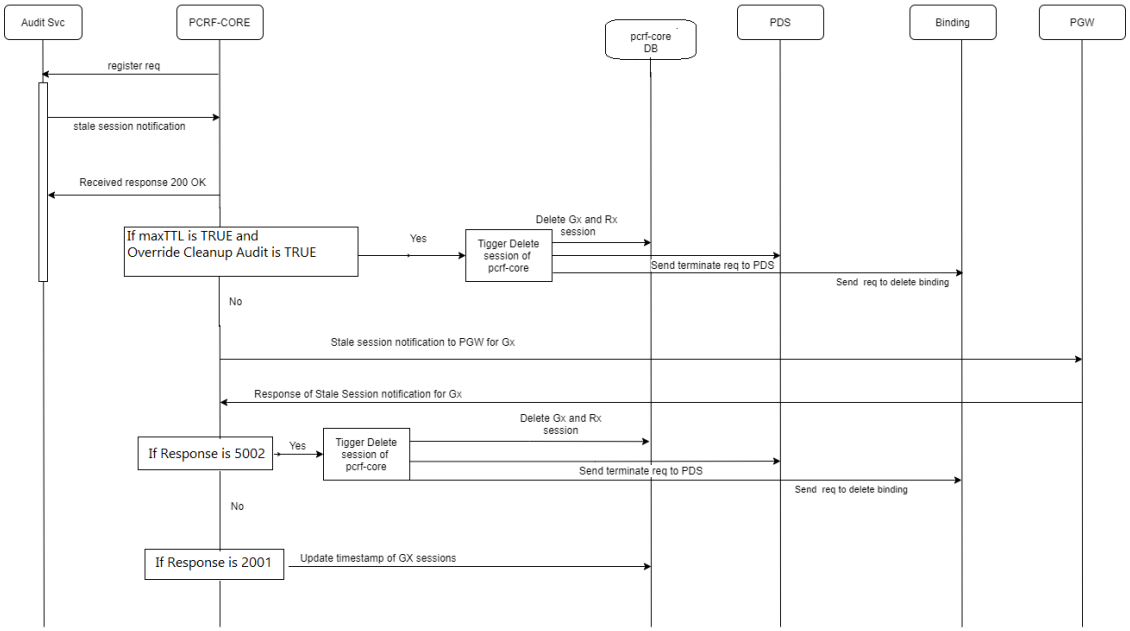
As shown in the call flow, after receiving a stale session notification from Audit service, AM service checks the maxTtl flag status and takes the following actions:

- If the **maxTtl** flag is **TRUE** then AM service will trigger it's **TERMINATE** leg.
- If the **maxTtl** flag is **FALSE** then AM Service will check the status of **queryAMF** flag.
- If **queryAMF** flag is set to true AM Service will trigger another notification towards AMF to check whether this particular AM Association record exists with AMF or not.
- If AMF responds with **204** No Content status code then AM will **update** the timestamp of the AM Association record.
- Else if AMF responds with **404** Not Found status code then AM Service will trigger its **TERMINATE** leg.
- Otherwise, if **queryAMF** flag is set to false then AM service will trigger it's **TERMINATE** leg.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Stale Session Detection and Handling in PCRF Core Service

Figure 4-197 Example call flow for Stale Session Detection and Handling in PCRF Core Service



Audit service audits the Gx sessions, Rx sessions and Sd sessions.

> **Note**
>
> PDS takes care of cleaning the Sy sessions.

Depending on the status of **maxTTL** flag, the Audit service send the notification to PCRF Core and initiates the stale session cleanup activity.

- For Rx session: If the **maxTTL** flag is **TRUE**, Rx sessions are cleaned.

  > **Note**
  >
  > The cleanup functionality is not implemented for Rx sessions, if the **maxTTL** flag is **false**.

- For Gx session:
  - **DIAMETER.Cleanup.OverrideCleanupAudit** Advance settings key will also be checked along with **maxTTL** flag.
  - If both **maxTTL** and **DIAMETER.Cleanup.OverrideCleanupAudit** are **TRUE**, the Gx sessions are cleaned without querying the PGW. Dependent Rx sessions will also be deleted as part for cleanup.
  - If the **maxTTL** flag is **FALSE**,

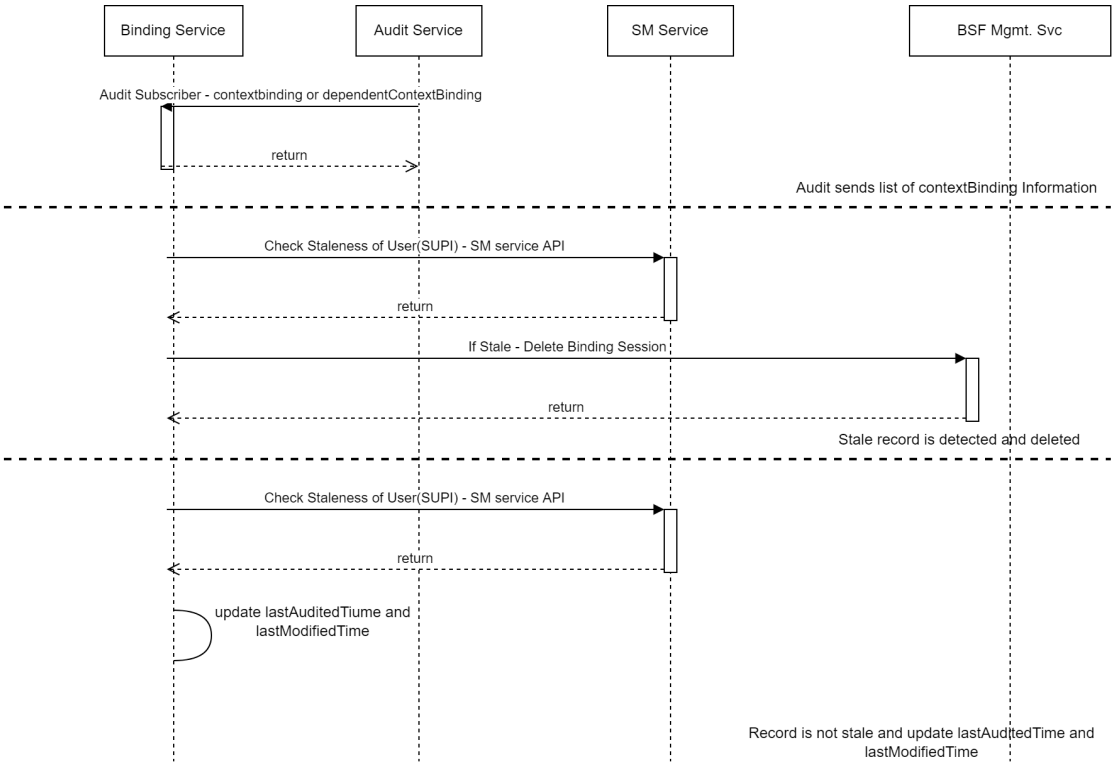
Copyright © 2019, 2026, Oracle and/or its affiliates.

    * pcrf-core service will trigger notification towards PGW to check whether this particular Diameter Session exists in the PGW or not.
    * If PGW responds with **2001 DIAMETER_SUCCESS** then pcrf-core will **update** the timestamp of the diameter session record.
    * Else, if PGW responds with **5002 DIAMETER_UNKNOWN_SESSION_ID** then pcrf-core Service will trigger its **TERMINATE** (CCR-T) leg.

- For Sd session: If the **maxTTL** flag is **TRUE** then Sd sessions are cleaned.

Stale Session Detection and Handling in Binding Service

Figure 4-198 Example call flow for Stale Session Detection and Handling in Binding Service



Audit Service uses the lastAuditedTime to check the staleness of the record.

1. For every **Minimum Audit Passes Interval** (frequency), Audit Service queries the database to get all the records that are older than the defined *TTL*.
2. If the records older than *TTL* have not yet reached *MaxTTL*, the Audit Service sends a audit notification to Binding Service with *maxTTL=false*. The Binding Service validates the staleness of the record with the contextOwner by sending request to core services.
    a. If the ContextOwner, has a valid session (Status code 200) - the binding service updates the *lastAuditedTimestamp*.
    b. Else, if the ContextOwner, does not have a valid session (Status code 404 from PCM-SM, 204 from PCRF-Core) - the Binding service deregisters the session as mentioned in the point 3.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. If the records older than *TTL* and have reached *MaxTTL*, but not yet reached *maxTTLforceInterval*, the Audit Service sends a stale session notification to Binding Service.
   In case of ContextBinding, the Binding Service sends a deregister request to BSF, deletes the record in the Binding Service database and marks the dependent session (if any) as stale.

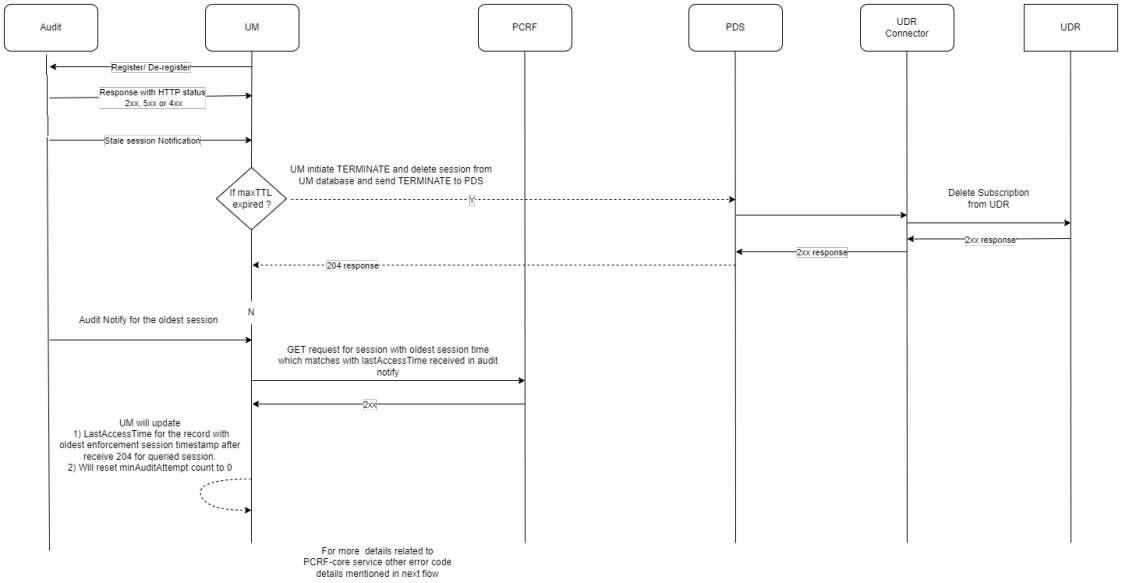
   In case of dependentcontextbinding, deletes the record from Binding Service database.
4. If the records older than the *TTL* and have reached *MaxTTL*, as well as *maxTTLforceInterval*, the Audit Service deletes the records in binding tables directly and no notification is sent.

> **Note**
>
> *maxTTLforceInterval* is configurable from deployment file of audit service. The Default value is of *maxTTLforceInterval* is 3 days (259200 seconds).

Stale Session Detection and Handling in Usage Monitoring Service

Usage Monitoring service identifies the stale sessions based on **lastAccessTime**.

Figure 4-199 Example call flow for Stale Session Detection and Handling in Usage Monitoring Service



1. The Usage Monitoring service sends register/de-register request to Audit service and takes necessary action on notifications received from Audit service.
2. Usage Monitoring service receives stale UM session notification from Audit service.
3. Usage Monitoring service checks the status of **maxTTL** flag.
4. If the value of **maxTTL** flag is `TRUE`, Usage Monitoring service initiates a UM session TERMINATE request for the oldest session to PDS to delete the session from UMContext database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Usage Monitoring service deletes the record from its UmContext database only when it is the last session for that record.

5. Usage Monitoring service sends a GET request to PCRF Core to check if the Usage Monitoring session exists with PCRF Core service.
6. If PCRF Core service responds with **2xx** status code, the Usage Monitoring service updates the timestamp of the Usage Monitoring session for that subscriber, updates the **lastAccessTime** with the oldest session timestamp and resets the value of **Minimum Audit Attempt** field to 0.
7. If PCRF Core service responds with **404 Not Found** status code and the MaxTTL is expired, the Usage Monitoring service triggers **TERMINATE** and also sends a DELETE request to PDS.
8. If PCRF Core service responds with **4xx**/**5xx** , except **404** , the Usage Monitoring service increments the value of **Minimum Audit Attempt** count in the database.
9. Also, Usage Monitoring service sends a DELETE request to PDS, which in turn sends a DELETE request to UDR through UDR Connector to delete the subscription.

If **forceTTL** is triggered from Audit service, Audit service will delete the entire subscriber entry from Usage Monitoring (UMContext) database. Usage Monitoring service will not send the TERMINATE and unsubscribe request in that case.

For example, when there is a Usage Monitoring session for a subscriber that is qualified for forceTTL and the session is stale. In the interim, if Usage Monitoring service receives a new session with a different AVP for the same subscriber prior to the forceTTL being triggered, even then Audit service deletes the entire record for the subscriber.

Managing Stale Session Handling

Enable

You can enable the Stale Session Handling functionality using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** To enable this feature, set the **Audit Enabled** parameter value to **true** on the **Audit Service** page. For more information about enabling the feature through CNC Console, see Audit Service.
- **Enable using REST API:** Set the **auditEnabled** parameter value to **true** in the **Audit Service** configuration API. For more information about enabling the feature through REST API, see "Audit Service" in *Oracle Communications Converged Policy REST API Specification Guide*.

Configure

You can configure the Stale Session Handling functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** To configure stale session handling feature for various services, perform the feature configurations under the **Audit** group on the respective service configurations page. For more information, see the following sections:
  - PCF Session Management
  - PCF Access and Mobility
  - Settings (for PCRF Core)
  - PDS Settings
  - PCF UE Policy Service

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - Configuring Usage Monitoring

  .

- **Configure using REST API:** Policy provides the following REST API for Stale Session Handling configuration:
  SM service: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm

  AM service: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam

  PCRF Core: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcrfcore/settings

  PDS: {apiRoot}/oc-cnpolicy-configuration/v1/services/pds/pdsSettings

  UE service: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfue

  You can perform the PUT operation to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.
- Usage Monitoring service: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfum

Observe

Policy provides metrics and alerts specific to Audit Service. For information related to Audit Service metrics, see Audit Service Metrics.

Maintain

The Stale Session Handling functionality provides audit logging. At the end of each audit pass, an audit log is published on the Grafana dashboard with the following details of the pass:

- Database and Table audited
- Number of records found to be stale
- Number of records removed (for the DELETE action)
- Number of notifications sent (for the NOTIFY action)
- Time taken to complete the audit pass
- Any exceptions occurred

The following is a sample of the audit report for SM service:

```
Audit Report {
"database" : "pcf_smservice_161",
"table" : "SmPolicyAssociation",
"staleRecords" : 18869,
"recordsDeleted" : 0,
"timeToCompletePass" : 20,
"recordsEnqueuedForNotification" : 18869,
"exceptions" : [ ]
}
```

The following is a sample of the audit report for PDS:

```
Audit Report:
{
     "database" : "occnp_policyds",
     "table" :  "pdssubscriber",
     "staleRecords" : 1,
     "recordsDeleted" : 0,
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    "timeToCompletePass" : 0,
    "recordsEnqueuedForNotification" : 1,
    "exceptions" : [ ]
 }
Audit Report:
 {
   "database " :  "occnp_policyds ",
   "table " :  "pdsprofile ",
   "staleRecords " : 1,
   "recordsDeleted " : 0,
   "timeToCompletePass " : 0,
   "recordsEnqueuedForNotification " : 1,
   "exceptions " : [ ]
}
```

The following is a sample of the audit report for UE Service:

4.90 Support for 3GPP NF Sets and Binding Headers

Policy supports the 3GPP NF Sets and binding headers in Model-B (Direct communication) and Model-C (Indirect communication). The support for 3GPP NF Sets and binding headers allows Policy to use the related headers and attributes for successful call processing.

> **Note**
>
> PCF can act both as an HTTP Server and HTTP Client.

NF Set: NF set is a group of interchangeable NF instances supporting similar services and network slices. In an NF set, the NF instances can be geographically distributed, but have access to the same context data. The NF instances can be deployed in such a pattern so that several instances are present within an NF set to provide distribution, redundancy, and scalability as a set. The NF instances of an NF set are equivalent and share the same MCC, MNC, NID (for SNPN), NF type, and NF Set ID.

Binding headers: The binding headers indicate the suitable target NF producer instance for NF service instance selection, reselection, and routing of subsequent requests associated with a specific NF producer resource or context. It allows the NF producer to indicate that the NF consumer, for a particular context, must be bound to an NF service instance, or NF set depending on local policies. Binding can also be used by the NF consumer to indicate the suitable NF consumer instances for notification target instance reselection and routing of subsequent notification requests, associated with a specific notification subscription.

PCF as a consumer sends binding headers to producer NFs such as UDR, CHF, BSF (customized), and AMF during explicit subscription. When **Send PCF Service Name in Binding Header** field under **NF Communication Profiles** page on CNC Console is enabled, the binding header includes `servname` along with other details such as `nfinst` and `nfset`.

When a notification request from any of the producer NFs such as UDR, CHF, BSF (customized), or AMF to PCF fails, the producer NFs use the details in the binding header to select alternate PCF. Using the service name included in the binding header, producer NFs can select alternate PCF with service level details.

Whenever there is an update in binding level and value, PCF includes the service name in the updated binding header sent to producers in Subscription Update or Notification Response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Also, PCF sends binding header with `scope` as `callback`.

Support for N1N2 Message Transfer

PCF allows to configure sending of the binding header, routing binding header and the discovery header for N1N2 transfer using the below mentioned fields available under **AMF** group in **PCF UE Policy Service** page on CNC Console.

- Send SBI Binding Header For N1N2 Transfer Requests
- Send Routing Binding Header For N1N2 Transfer Requests
- Send Discovery Header For N1N2 Transfer Requests

Whenever there is a change in the binding information, UE Policy service sends the SBI binding in the transfer message. It can be configured whether N1N2Transfer must be sent with routing binding header or discovery header.

For N1N2 transfer requests UE Policy service sends the binding header as N1N2 transfer contains the implicit subscription for N1N2 failure notification.

- When NFSet and binding feature is enabled, PCF sends binding header in N1N2Transfer request at NFSet or NFInstance level, as configured by user.

  The user can configure to send SBI binding header for N1N2 Transfer requests by selecting one of the following values for **Send SBI Binding Header For N1N2 Transfer Requests** field:

  – **When binding information changes**: To send the binding header in the HTTP request only whenever there is a change in the binding information.

  – **Always**: To send the binding header in all the N1N2 Transfer requests.

  – **Never**: Not to send the binding header in any of the N1N2 Transfer requests.

  This configuration will override the values being set towards **NF Communication Profile** under Non-access stratum (NAS).

  > **Note**
  >
  > The NF Communication Profile for NAS is mandatory to be set in UE service configuration.

- The user can configure to send the routing binding header in N1N2Transfer requests by selecting one of the following values for **Send Routing Binding Header For N1N2 Transfer Requests** field.

  – **Always**: To send the routing binding header in all the N1N2 Transfer requests.

  – **Never**: Not to send the routing binding header in any of the N1N2 Transfer requests.

- The binding header includes the discovery header when the N1N2 message transfer does not include the routing binding information. That is, UE Policy service adds 3gpp-Sbi-Discovery-target-nf-set-id when 3gpp-Sbi-Routing-Binding is not included in the binding information.

  The user can configure to send the discovery header in N1N2Transfer requests by selecting one of the following values for **Send Discovery Header For N1N2 Transfer Requests** field when the routing binding header is not present. This configuration is applicable to retransmissions as well.

  – **Always**: To send the discovery header in all the N1N2 Transfer requests when the routing binding header is not present.

Copyright © 2019, 2026, Oracle and/or its affiliates.

– **Never**: Not to send the discovery header in any of the N1N2 Transfer requests.

For more details on how to configure the binding header, routing binding header, and discovery header for N1N2Transfer, see PCF UE Policy Service.

> **Note**
>
> It can be configured to include 3gpp-Sbi-Discovery-target-header in N1N2Transfer request explicitly and not in any other subsequent messages to AMF like Unsubscription of N1N2Subscription.

Table 4-133 Supported Headers

Header Name	Description
3gpp-Sbi-Binding	This header is used to communicate the binding information from an HTTP server for storage and subsequent use by an HTTP client. This header contains a comma-delimited list of Binding Indications from an HTTP server for storage and use of HTTP clients. The absence of this parameter in a Binding Indication in a service request is interpreted as "callback".
3gpp-Sbi-Callback	This header indicates if a HTTP request is a callback. For example, Notifications. This header is included in HTTP POST messages to request notifications or callbacks towards NF service consumers in indirect communication. This header is used by the SCP to differentiate the notification and callback requests from other service requests. For example, the authorization (access token is not used in notification or callback. This header contains the type of notification and the name of the notify service operation.
3gpp-Sbi-Discovery-*	The discovery parameter can be set using the CNC Console for Policy or the Policy REST API. The headers beginning with the prefix `3gpp-Sbi-Discovery-`, are used in indirect communication mode for discovery and selection of a suitable producer by the SCP. Such headers can be included in any SBI message and include information that allows an SCP to find a suitable producer, according to the delegated discovery parameters provided by the consumer. The name of each NF service discovery factors header are constructed by concatenating the string `3gpp-Sbi-Discovery-` with the name of the conveyed discovery parameter. For example, `3gpp-Sbi-Discovery-<discovery parameter>`. Policy supports the `target-nf-set-id` discovery parameter. Thus, the supported discovery header is `3gpp-Sbi-Discovery-target-nf-set-id`.
3gpp-Sbi-Routing-Binding	This header is used in a service request to send the binding information (3gpp-Sbi-Binding header) to direct the service request to an HTTP server, which has the targeted NF Service Resource context. This header enables alternate routing for subsequent requests at SCP. It contains a routing binding Indication to direct a service request to an HTTP server, which has the targeted NF service resource context.

Policy supports the NF Set and binding header functionality in SM, AM, UE, and PA function interfaces. You can configure NF communication profiles for the following PCF interfaces:

Copyright © 2019, 2026, Oracle and/or its affiliates.

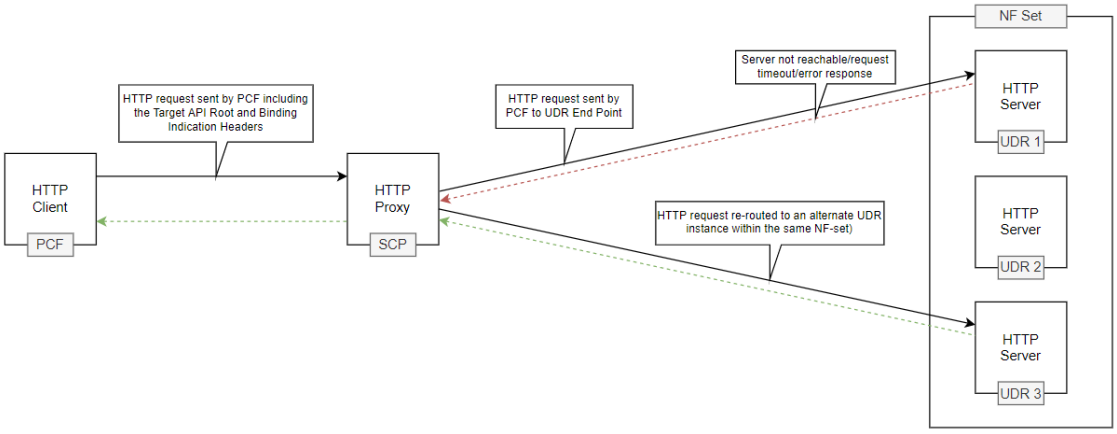
- N7/Npcf interface for notifications towards SMF
- N36/Nudr for requests and responses towards UDR
- N28/Nchf for requests and responses towards CHF
- Nbsf interface towards BSF
- N15/Namf interface for notifications towards AMF
- Npcf interface for notifications towards UE
- Npcf interface for notifications towards PA

You can configure the PCF to support binding header on the selected interface either as an HTTP client or server. If PCF is not configured to support the binding header for an interface, then it ignores the binding header and the information.

Example

The following diagram depicts an example of indirect communication between PCF and other NF, based on NF set and binding header:

Figure 4-200 Example of NF Set and Binding Header based Indirect Communication



The above architecture diagram describes a scenario of indirect communication between PCF and UDR. The PCF acts as an HTTP Client and UDR is the HTTP server. SCP acts as the HTTP proxy that redirects the requests coming from PCF.

In indirect communication, PCF sends the HTTP requests and the binding indication headers to SCP. The request contains the following details:

- 3gpp-Sbi-Target-Apiroot: The target API root that indicates the destination NF endpoint (Target UDR instance).
- 3gpp-Sbi-Discovery header: Contains information about the NF Set of the destination UDR instance. This header is used by SCP in case the first message does not reach the original UDR instance.
- 3gpp-Sbi-Routing-Binding: In case of an insertion request, PCF sends this header. It contains the routing binding indication to direct a subsequent service request to UDR.
- 3gpp-Sbi-Binding (PCF): Contains the NF Set information of PCF. This header is sent by PCF with request message and stored by UDR for subsequent communication.

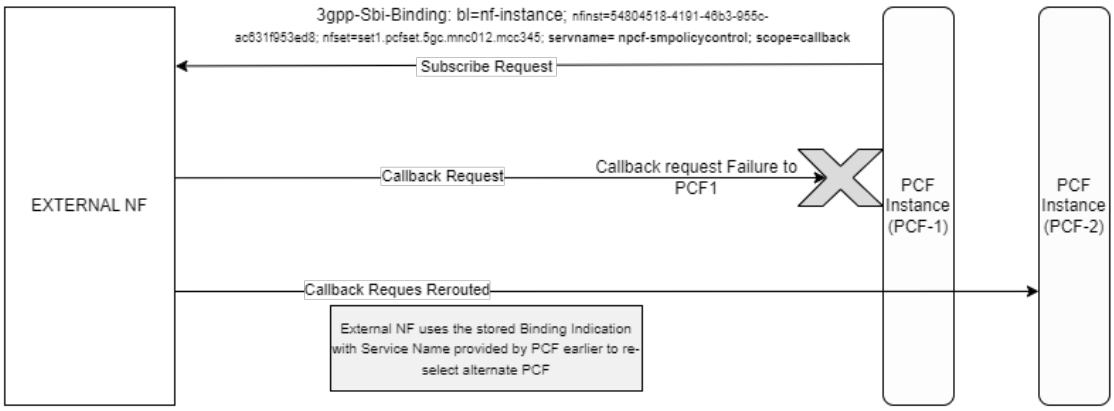
Copyright © 2019, 2026, Oracle and/or its affiliates.

- 3gpp-Sbi-Binding (UDR): Contains the NF Set information of UDR in the response message. This header is sent by UDR in response message and stored by PCF for subsequent communication.

Once the HTTP request is received at SCP, it is then redirected towards the NF instance indicated in the API root. In case of any failure, SCP redirects the request to an alternate destination belonging to the same NF set or a different NF set, as indicated in the *3gpp-Sbi-Binding* header.

The values can be set while configuring NF Communication Profile through CNC Console for Policy or REST APIs.

Support for Rerouting Notification from External NFs to Alternate PCF When the Notification Request Fails



PCF supports including the service name in the binding header sent to NFs such as UDR, CHF, AMF, and BSF (customized) when **Send PCF Service Name in Binding Header** parameter in the **NF Communication Profile** page is enabled.

The `servname` parameter in the binding header contains the name of the 3GPP defined PCF service (or aggregate service name applicable only towards CHF), which is invoking the Subscribe request or handling the notification. Invoking or Handler service name to be sent in the binding header is internally identified by PCF for UDR,AMF, and BSF interfaces and no external configuration is required except for the binding header sent towards CHF where the service name to be sent in the binding header is defined using CNC Console for Policy.

For example, the explicit Subscribe request sent towards nUDR on SM Create request for SM data contains `servname= npcf-smpolicycontrol` in the binding header as SM service is the handler service here.

Below is a sample Binding Header:

```
3gpp-Sbi-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed8;
nfset=set1.pcfset.5gc.mnc012.mcc345; scope=callback;servname= npcf-
smpolicycontrol;
```

The service name to be forwarded in the binding header sent towards CHF is configured based on the value of **PCF Service name in Binding header** parameter under **CHF** group in **PCF User Connector** page under **Service Configurations**. The service name in the binding header sent to CHF contains:

- 3GPP defined PCF Service name: As PCF requests the policy counter information from CHF only once and can share with other services, PCF can contain the service name of the first service (for example, npcf-am-policy-control), which is requesting policy counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

information from CHF. The service level information such as scheme and port that the first service can be used to represent other services in the same PCF deployment as subsequent notifications from CHF will be consumed by all the services which is sharing the data.

Below is a sample binding header with 3GPP defined PCF service name sent towards CHF:

```
3gpp-Sbi-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed8;
nfset=set1.pcfset.5gc.mnc012.mcc345; scope=callback;servname= npcf-am-policy-
control;
```

- Aggregate/custom service name representing a group of PCF services with aggregated service level information.

  As PCF (PCF1) requests the policy counter information from CHF only once and can share with other services, PCF can contain aggregate service name approach for sending `servname` in the binding header. The aggregate service level information is used to represent group of service with aggregate service name.

  For example, npcf-custom-service can represent npcf-am-policy-control, npcf-smpolicycontrol, and npcf-ue-policy-control.

  Below is a sample binding header with aggregate/custom service name sent towards CHF:

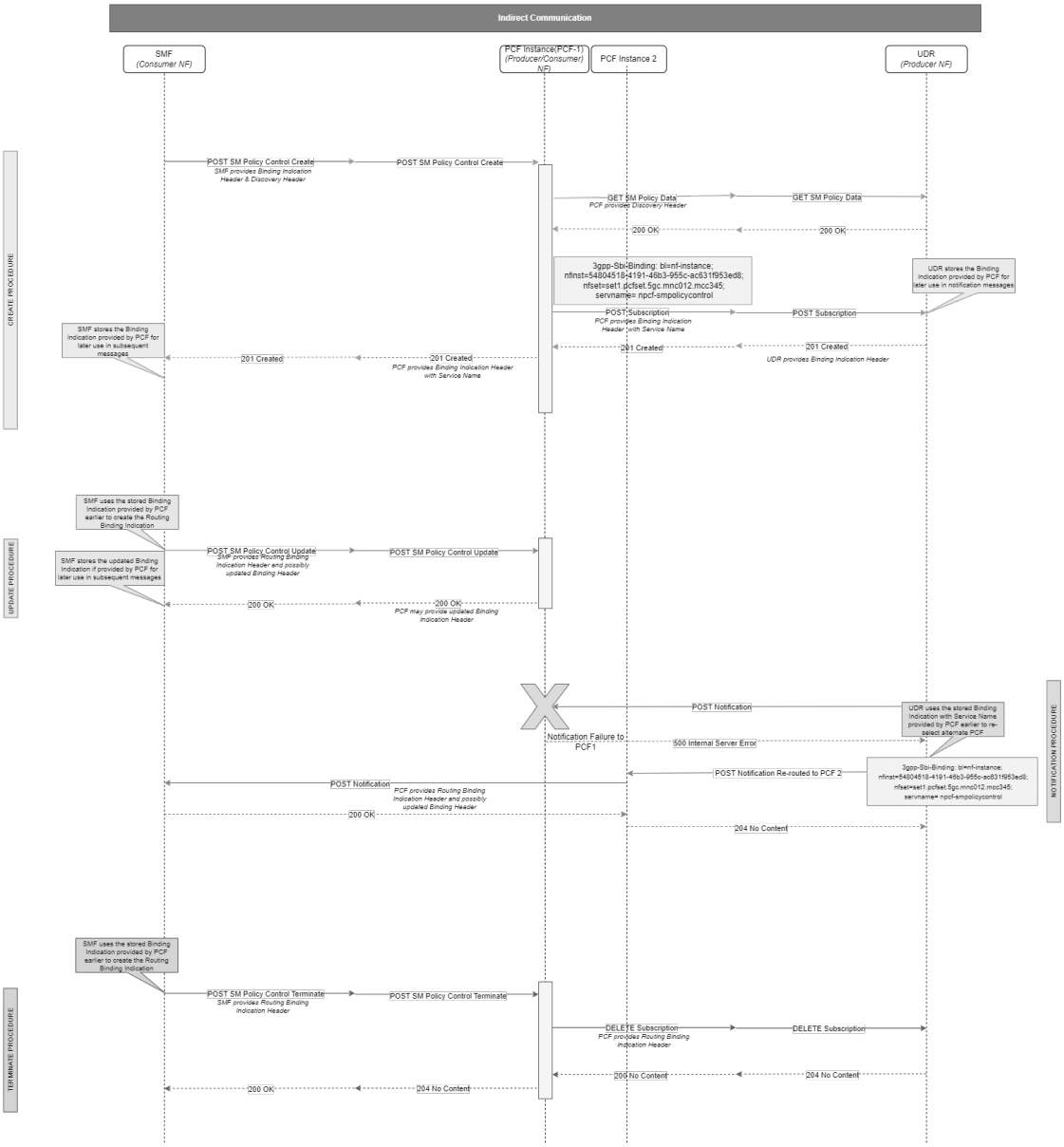
  ```
  3gpp-Sbi-Binding: bl=nf-instance; nfinst=54804518-4191-46b3-955c-ac631f953ed8;
  nfset=set1.pcfset.5gc.mnc012.mcc345; scope=callback;servname= npcf-custom-
  service;
  ```

  > **Note**
  >
  > Before defining the aggregate/custom service name towards CHF, it is mandatory to register this custom service having aggregated service level information while doing PCF registration with NRF.

Call flow for rerouting a notification message from UDR to an alternate PCF using service name in Binding Header

Here is a sample call flow that depicts rerouting a notification message from UDR to an alternate PCF using service name in the binding header when the NOTIFICATION request from UDR fails to reach PCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

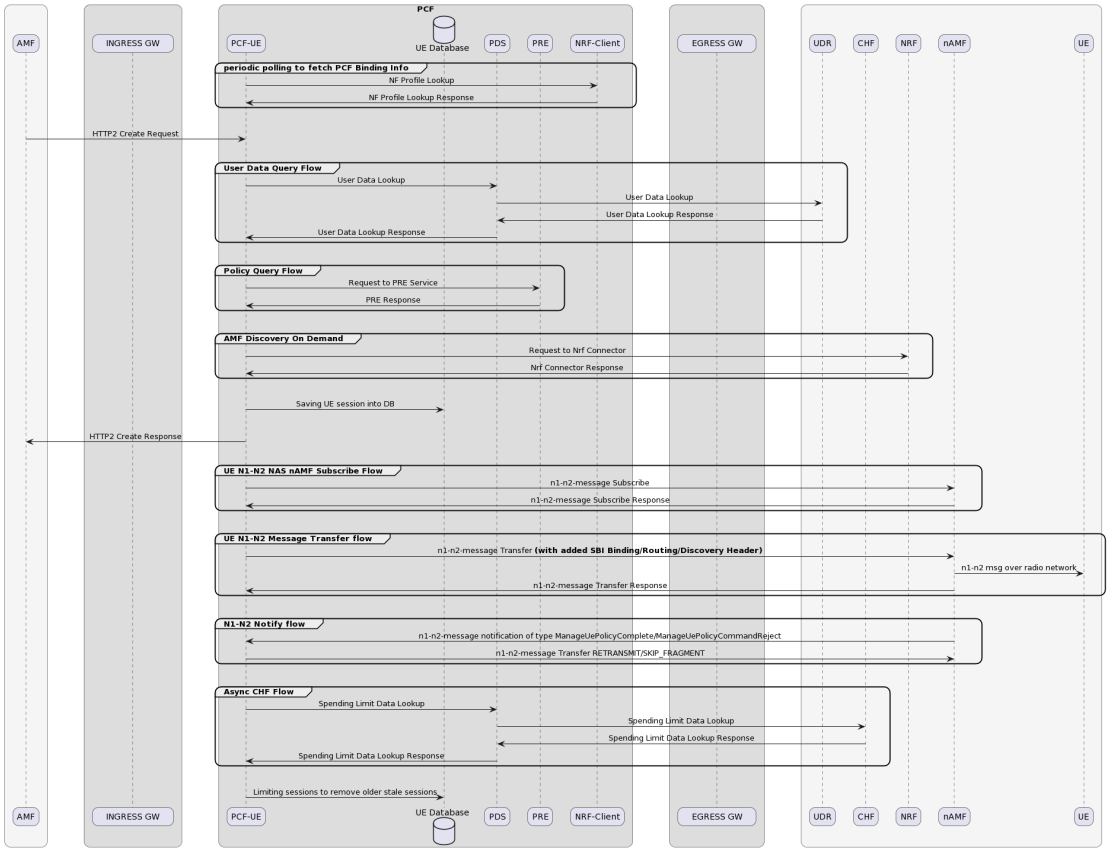


1. An instance of PCF, PCF1 receives the binding indication header and the discovery header in an SM Policy Control Create request from SMF (Consumer NF).
2. PCF1 queries UDR to get the corresponding SM Policy Data.
3. UDR sends a 200 ok message to PCF1.
4. Also, PCF1 sends the binding header and discovery header (3gpp-Sbi-Binding) in the Subscription request to UDR that includes `svcname` along with other parameters such as `nfinst` and `nfset`. UDR saves this binding information in its database, which will be used while sending any notification from UDR to PCF1.
5. When an update notification from UDR to PCF1 fails with a 500 internal server error, UDR identifies an alternate PCF2 using the service name provided by PCF in the previous binding header.
6. UDR reroutes the notification message to PCF2 and receives a response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Support for Binding Header and Routing Binding Header in N1N2Transfer Request

Here is a sample UE Policy create call flow depicting Binding Header in N1N2Transfer request.



1. UE Policy service periodically polls the NRF through NRF client to fetch the updated NF profile.
2. Whenever UE Policy service receives a create request from AMF, it queries the UEPolicy Association database to fetch the UE Policy association details.
3. UE Policy service queries the UDR to fetch the user profile.
4. UE Policy service sends a request with the given details to PRE for Policy evaluation.
5. UE Policy service sends a request to NRF through NRF Client to discover the NF instances using amf-set-id and amf-region-id.
6. UE Policy service saves the updated UE Policy Session details in the UEPolicy Association database.
7. UE Policy service responds to AMF with a successful message.
8. UE Policy service sends a subscription request to nAMF for N1N2 message transfer and receives a response.
9. UE Policy service sends N1N2 message Transfer(with added SBI Binding/Routing/ Discovery Header) to nAMF for N1N2 message transfer, which in-turn forwards the details to the UE.

Copyright © 2019, 2026, Oracle and/or its affiliates.

10. Whenever the UE Policy service receives an N1N2 notification of type ManageUePolicyComplete/ManageUePolicyCommandReject from nAMF, the UE Policy service tries to retransmit the message to nAMF.
11. Asynchronously, the UE Policy service contacts the PDF to fetch the Spending Limit data.
12. PDS contacts CHF through CHF Connector to subscribe for the policy counters.
13. After receiving the information from CHF, PDS sends a notification to UE Policy service with the Spending Limit data.
14. UE Policy service processes this information and if needed it sends an update notify to AMF service and also saves the details in UEPolicy Association database.

Managing NF Sets and Binding Header Support

Enable and Configure

The NF Sets and Binding header support can be enabled for SM, AM, UE, and PA service interfaces. An NF communication profile must be configured and assigned to the respective interface to enable this feature.

You can enable and configure the NF Communication Profiles using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations under:
  - **NF Communication Profiles** page under **Common Data** for **Service Configurations**. For more details, see NF Communication Profiles
  - **AMF** group in **PCF UE Policy** page for **Service Configurations**. For more details, see PCF UE Policy Service.
  - Configure **NF Communication Profile** parameter for each of the services. For details, see:
    - PCF Session Management
    - PCF Access and Mobility
    - PCF Policy Authorization
    - Binding Service
    - PCF UE Policy Service
  - Configure the parameters under **UDR** and **CHF** groups under **PCF User Connector**. For more details, see PCF User Connector.
- **Configure using REST API:** Perform the NF Communication Profile configurations under the following REST APIs:
  - {apiRoot}/oc-cnpolicy-configuration/v1/services/common/nfcommprofiles
  - {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm
  - {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam
  - {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfpa
  - {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfue
  - {apiRoot}/oc-cnpolicy-configuration/v1/services/binding
  - {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfuser

  You can perform the POST, PUT, or GET operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observe

Policy uses the Ingress and Egress metrics for the NF bindings used by PCF. The following metrics contains the information about NF bindings used by PCF:

- For SM, PA, AM, UE, and Binding service:
  - ocpm_ingress_response_total
  - ocpm_egress_request_total
- For UDR Connector service: `ocpm_udr_tracking_request_total`
- For CHF Connector service: `ocpm_chf_tracking_request_total`

For more information, see the following sections:

- SM Service Metrics
- User Service Metrics

Maintain

The Policy logs includes the NF binding information received or sent by PCF. The logs include information about the following headers:

- `location`
- `3gpp-sbi-target-apiroot`
- `3gpp-sbi-binding`
- `3gpp-sbi-routing-binding`
- `3gpp-Sbi-Discovery-target-nf-set-id`
- `3gpp-sbi-callback`

4.91 Georedundancy Support

The Cloud Native Core architecture supports Geographical Redundant (Georedundant) Policy (PCF, PCRF, and converged Policy) deployments to ensure high availability and redundancy. It offers a two, three, or four-sites georedundancy to ensure service availability when one of the Policy sites is down.

The specifications for georedundancy feature are as follows:

- All the georedundant sites must have helm and REST based configurations except NF Instanced Id, Policy Endpoint, and port.
- The georedundant Policy sites must be reachable from NFs or Peers on all the sites.
- The same NFs or Peers must not communicate to other georedundant Policy sites at the same time for the same session.
- When Policy is deployed as georedundant PCF instances, then:
  - All the sites register with NRF independently and works in active state.
  - All Policy instances share the **Session State** data by using the replication service of DB tier. This enables service continuity during failure of any of the site.
  - The NFs in a given site can discover Policy instances through NRF. However, local configurations, such as DNS SRV or static configuration are required to determine the primary and secondary or alternate Policy configuration. When the primary instance is available, the NFs send service requests to the primary instance.

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - NRF always reflects current functional status of a given PCF or BSF instance. Thus, during failure of a given PCF or BSF instance, the value of `NfStatus` is updated to **SUSPENDED** by either NRF or PCF or BSF instance. Therefore, when NF detects failure of primary instance due to error response or status notification from NRF, the NF redirects its traffic to the secondary instance, while the primary instance remains unavailable and until it becomes available again.

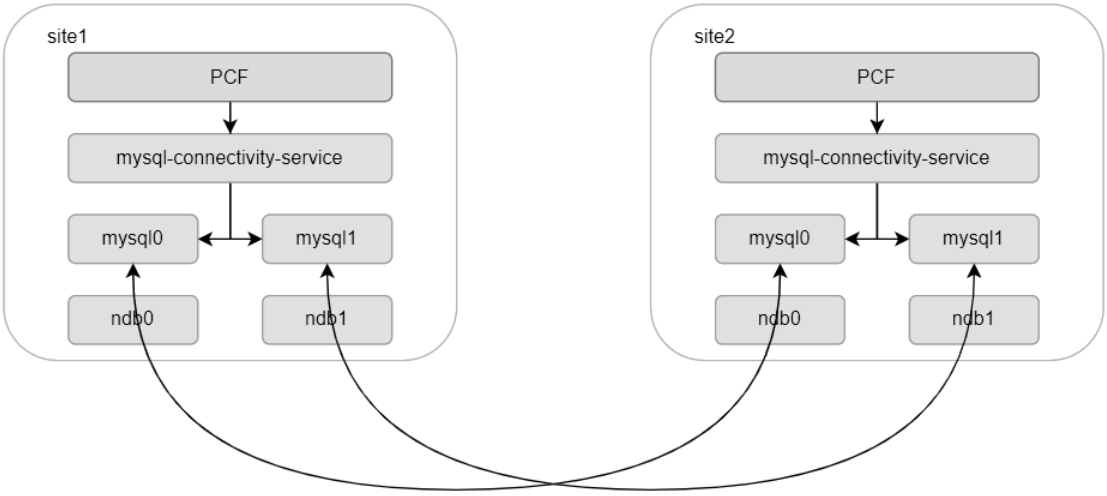
- When Policy is deployed as georedundant PCRF instances, then:
  - All the sites works in active state.
  - All instances share "Session State" data using DB tier's replication service to enable service continuity during site failure.
  - When peer detects failure of primary instance, the peer redirects its traffic to the secondary instance while the primary instance remains unavailable and until it becomes available again.

Policy supports the following types of georedundant deployment:

Two-Site Georedundancy Deployment

The following diagram depicts the topology for two-site georedundant PCF deployment:

Figure 4-201 Two-Site Georedundancy Deployment



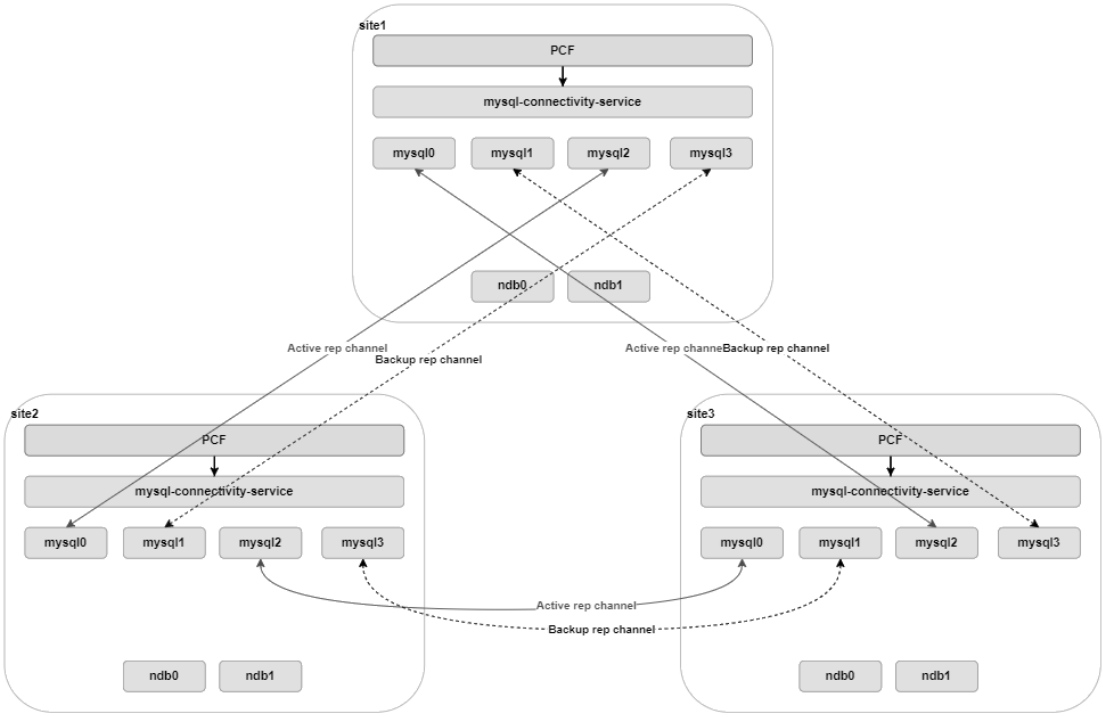
The two-site georedundancy is established, when the second site instance of the cnDBTier is created. The DB Tier provides bi-directional replication between both the sites. When the two-sites are correctly replicated, then any update done at one site is replicated to the other remote site in real-time. The changes include creating, changing, or deleting a record.

Three-Site Georedundancy Deployment

The following diagram depicts the topology for three-site georedundant PCF deployment:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-202 Three-Site Georedundancy Deployment



In case of three-site georedundancy, bi-directional replication is established from each site to the two other sites. The database updates from each site are replicated to the other two-sites over the replication channel.

The advantages of three-site georedundancy is:

- In case of a single site failure, the remaining two-sites keep establishing the bi-directional replication.
- No action is required in case of a site failure.
- Requires 4 SQL pods and 2 replicated svc (db-rep-svc) at each site

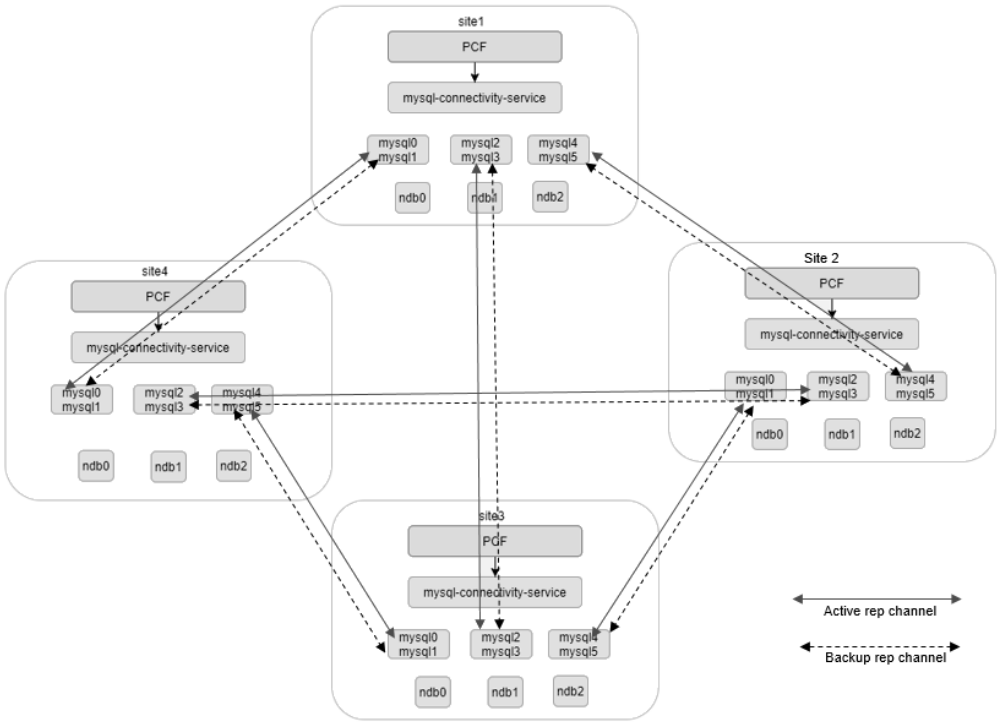
When the three-sites are correctly replicated, then any update done at one site is replicated to the other two remote sites in real-time. The changes include creating, changing, or deleting a record.

Four-Site Georedundancy Deployment

The following diagram depicts the topology for four-site georedundant PCF deployment:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-203 Four-Site Georedundancy Deployment



cnDBTier supports the four-site georedundancy deployment. In case of four-site georedundancy, each site participates in a 4-way replication. The database updates from each site are replicated to the other three-sites over the replication channels.

The advantages of four-site georedundancy is:

- In case of a single site failure, the remaining three-sites keep establishing the bi-directional replication.
- No action is required in case of a site failure.
- Requires 6 SQL pods and 3 db-rep-svc at each site.
- Each site uses two SQL nodes for active and standby replication channels for high availability of the replication channels.

When the four-sites are correctly replicated, then any update done at one site is replicated to the other three remote sites in real-time. The changes include creating, changing, or deleting a record.

Managing Georedundancy

Deploy

To deploy Policy in a georedundant environment:

1. Set up the replicated cnDBTier version 1.8.0.0.3 or above, on two or three-sites, as required. For information about installing cnDBTier, see "Installing cnDBTier" in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade and Fault Recovery Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Deploy Policy over the replicated (two or three) cnDBTier sites. For information about installing and deploying Policy, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*

Configure

To configure georedundancy:

You need to configure the georedundancy functionality while deploying the Policy instances on the replicated sites. The following parameters must be updated in the custom values file for Policy:

Table 4-134 Georedundancy Parameters

Parameter	Description
global.envMysqlHost	The database instance for each site. PCF communicates to the database at the same site only.
global.nfInstanceId	The ID for the site
config-server.envMysqlDatabase	The database for the config server. The two-sites should use different database names for config server
cm-service.envCommonConfigMysqlDatabase	The common configuration database. It should be different on the sites
nrf-client.configmapApplicationConfig.profile	Configuration data for nrf client. The `appProfile` and the `nfInstanceId` parameters must be aligned with `global.nfInstanceId`
nrf-client-nfdiscovery.dbConfig.dbName	The common configuration database. It should be different on the sites
nrf-client-nfmanagement.dbConfig.dbName	The common configuration database. It should be different on the sites
appinfo.dbConfig.dbName	The common configuration database. It should be different on the sites
perf-info.dbConfig.dbName	The common configuration database. It should be different on the sites
policyds.envMysqlDatabaseConfigServer	The database for the config server. The two-sites should use different database names for config server
ingress-gateway.dbConfig.dbName	The common configuration database for ingress gateway. It should be different on the sites
egress-gateway.dbConfig.dbName	The common configuration database for egress gateway. It should be different on the sites
alternate-route.dbConfig.dbName	The common configuration database for alternate route. It should be different on the sites

For more information about configuring the parameter value, see "Alternate Route Service Configuration" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*

Observe

cnDBTier generates critical alerts in case of application or database failure. For more information, see *Oracle Communications Cloud Native Core, cnDBTier User's Guide*.

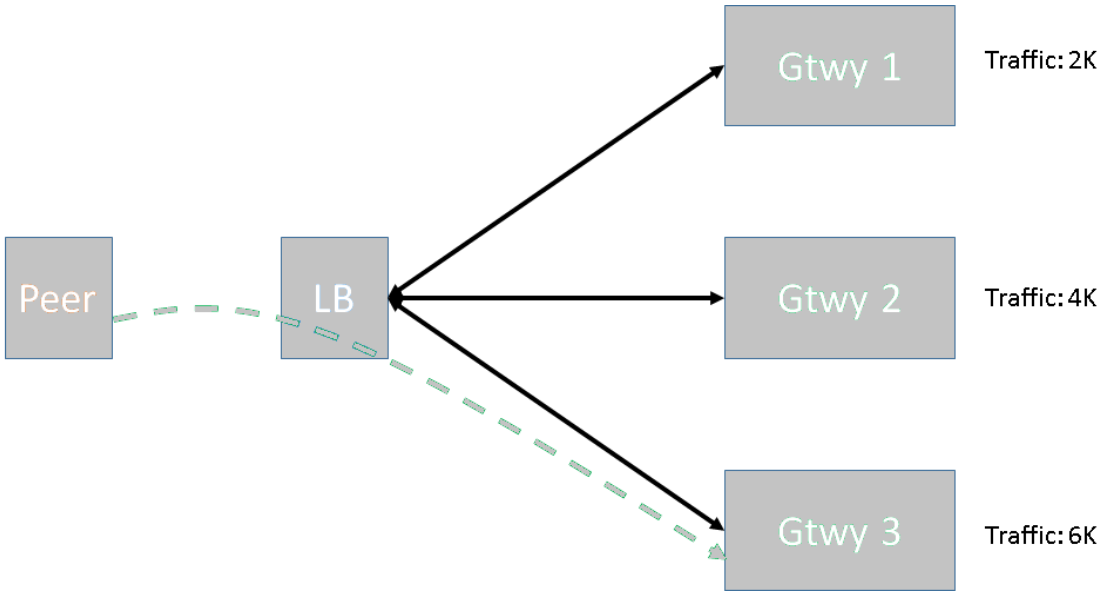
Maintain

Copyright © 2019, 2026, Oracle and/or its affiliates.

Policy allows you to monitor the georedundancy deployment through cnDBTier alerts. Access the Prometheus GUI to check for new App alerts.

4.92 Diameter Pod Congestion Control

The Diameter Gateway is a diameter proxy agent for Policy. Being a front-end microservice for diameter traffic for both Ingress Gateway and Egress Gateway, the Diameter Gateway can get congested due to higher traffic and higher CPU usage. Thus, it is imperative to have suitable congestion control features in place for Diameter Gateway pods to avoid adverse impact on latency and performance. Another reason for the need of congestion control mechanism for Diameter Gateway is the nature of diameter connections. These connections are long lived and are distributed by external LoadBalancer. As shown in the following image, when LoadBalancer routes an incoming request from network to Diameter Gateway pod, it does not take into account health or load of the pod. As a result, uneven distribution of traffic may happen and gateway pods experience congestion.



Congestion control helps to identify such conditions and invoke load shedding rules to address these situations when these load conditions persist. With Diameter Gateway service supporting the congestion control mechanism feature, it helps to protects its pods from congestion and ensures consistent service availability to its consumer.

The pod congestion control mechanism involves:

1. Determining Pod Congestion State
2. Triggering Pod Congestion Control

Determining Pod Congestion State

At any given point of time, a pod can be in any one of the following states:

- Normal
- Danger of Congestion (DOC)
- CONGESTION_L1
- CONGESTION_L2
- CONGESTED

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-204 Different Pod Congestion States



To decide the state of a pod, the following points are taken into consideration:

1. **CPU**: The CPU usage for congestion state is calculated by comparing the CPU usage of the container (monitored using cgroup parameter, `cpuacct.usage`, which provides current cpu usage in nanoseconds) with the configured threshold.
2. **Queue**: For the DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED pod states, compare the number of pending messages in the queue with the configured pending messages threshold.

To avoid switching between these states due to traffic pattern, it is required for the pod to be in a particular state for a given period before transitioning to another state. Periodically, the state of the pod's congestion gets determined. The following configurations are used to define the period that the pod has to be in a particular state for:

- `stateChangeSampleCount`: This specifies after how many continuous intervals, the pod state can be changed. The default value is 5. This value can range from 1 to 2147483647. This parameter can be configured to using Policy CNC Console or REST API.
- `stateCalculationInterval`: This specifies the time duration or interval, after which the pod congestion state will be re-verified. The default value is 200ms. This interval is configured in milliseconds and can range from 50 to 2147483647. This parameter can be configured to using Policy CNC Console or REST API.

For more information about these congestion control configurations, see Congestion Control Settings section in CNC Console.

CPU and Queue Threshold

A pod's state changes when its resources, namely the CPU and Queue buffer usage exceeds the predefined congestion threshold, checked at regular intervals. An active CPU and Queue default threshold profile can be viewed using CNC Console at *Policy → Overload and Congestion Control → Congestion Control → Thresholds* section. The user can create new threshold profile with the congestion states being in the order of CONGESTED → CONGESTION_L1 → CONGESTION_L2 → CONGESTED states, and make it active. The Diameter Gateway service pod's congestion states and their default congestion parameters, CPU, and Queue counts are provided in the following table:

Table 4-135 Diameter Gateway service Congestion States

Congestion States	CPU Count	Queue (Pending Request)
DANGER_OF_CONGESTION (DOC)	60	6300
CONGESTION_L1	70	7200
CONGESTION_L2	75	8100
CONGESTED	80	9000

For more information about these CPU and Queue count thresholds configurations, see Congestion Control Thresholds section in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Triggering Congestion Control

With Congestion Control feature enabled, every time a message is fetched for processing, the system checks the current congestion state of the pod. If the current state is either in `DOC`, `CONGESTION_L1`, `CONGESTION_L2`, or `Congested` state, then the congestion control mechanism is triggered. After verifying that the message type is a request, a request priority is assigned to it. If the request priority is greater than or equal to the discard priority, then the message is rejected, otherwise it is accepted.

Congestion Control Load Shedding using Discard and Request Priority

Diameter Gateway pods performs load shedding by considering the load rule configured for the current congestion state. The load shedding rule is based on message priority configuration. A default load shedding rule is active and the messages are discarded based on it. You can configure these load rules with the congestion states being in the order of CONGESTED → CONGESTION_L1 → CONGESTION_L2 → CONGESTED states, using the Overload and Congestion Control menu in CNC Console. The Diameter Gateway discards the requests based on either:

- Priority
- Priority and Percentage

Table 4-136 Priority based Message Discards

Congestion State	Discard Priority
DANGER_OF_CONGESTION	27
CONGESTION_L1	19
CONGESTION_L2	17
CONGESTED	15

Table 4-137 Priority and Percentage based Discards

Congestion State	Discard Priority Range	Discard Percentage
DANGER_OF_CONGESTION	27-31	50
CONGESTION_L1	19-26 27-31	50 75
CONGESTION_L2	17-18 19-26 27-31	50 75 100
CONGESTED	15-31	100

For more information about these `Priority` or `Priority and Percentage` discards configurations, see Congestion Control Load Shedding Profiles page in CNC Console.

Propagation of Message Priority from and to Diameter Gateway

The following points needs to be known while assigning request or message priority to an request API:

- When the Diameter Gateway sends a message that includes `OC-Message-Priority` AVP, it is sending the priority value to the downstream services. The downstream services namely the Diameter Connector and PCRF Core services consider this value as having the highest precedence. This means that, instead of considering the configured message priority rules,

Copyright © 2019, 2026, Oracle and/or its affiliates.

these services will directly use the priority in `OC-Message-Priority` AVP when theirs pods are in congestion state.

- Similarly, when the downstream services namely the Diameter Connector and PCRF Core services sends messages that includes `OC-Message-Priority` AVP, it is sending the priority value to Diameter Gateway. The Diameter Gateway considers this value as having the highest precedence only if the diameter message priority rule has enabled the `OC-Message-Priority` option. If the option is not enabled then it will use the configured message priority from the selected Message Priority Profile.

The following two AVP's are added in Pre-Defined AVP Conditions in Diameter Gateway Message Priority Rules configurations at *Policy → Overload and Congestion Control → Diameter → Message Priority Profiles* in CNC Console.

Table 4-138 Pre-Defined AVP Conditions

Pre-Defined AVP Conditions	Type Operator	Values
DRMP	• Equals • Not Equals • Less Than • Less Than Equals • Greater Than • Greater Than Equals	The Diameter Routing Message Priority (DRMP) AVP allows Diameter Gateway to indicate the priority of diameter messages. This will take numeric values. Allowed numeric value in the range of 0-15.
OC-Message-Priority	• Equals • Not Equals • Less Than • Less Than Equals • Greater Than • Greater Than Equals	The header attribute allows Diameter Gateway to indicate the priority of diameter messages. This will take numeric values. Allowed numeric value in the range of 0-31.

In the Message Priority Profiles for Diameter Gateway, if both `DRMP Priority` and `OC-Message-Priority` is selected, then `OC-Message-Priority` shall be considered as highest priority for message priority rule selection. The message priority range for OC-Message-Priority is 0-31, and for DRMP AVP it is 0-15.

For more information about configuring message priority profiles, see Message Priority Profiles section in CNC Console.

Congestion Response Code

After defining load rules Overload and Congestion Control menu, the response to reject the request can also be configured using the advanced settings in Diameter configurations. The following are the advanced settings key and value:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-139 Advance Setting

Key	Value	Description
CONGESTION_DIAMETER_RESPONSE_CODE	3004	This is to configure the diameter result code for the congestion control discards and its value shall be numerical. The value can be set to either 3xxx, 4xxx, or 5xxx response codes. If this value is not configured, then default congestion result code shall be *3004 (DIAMETER_TOO_BUSY)*. **Default Value**: 3004 **Examples**: CONGESTION_DIAMETER_RESPONSE_CODE=5065 CONGESTION_DIAMETER_RESPONSE_CODE=3004
CONGESTION_DIAMETER_VENDOR_ID	0	This is to configure the diameter vendor id for the congestion control discards and its value shall be numerical. If the value is non-zero, then the *CONGESTION_DIAMETER_RESPONSE_CODE* shall be considered as the experimental result code. If value is zero or it is not configured, then *CONGESTION_DIAMETER_RESPONSE_CODE* shall be considered as the normal result code. **Examples**: CONGESTION_DIAMETER_VENDOR_ID=10415 CONGESTION_DIAMETER_VENDOR_ID=21274

If above advance settings keys are not configured, then Diameter Gateway will discard the messages with default diameter result code `3004 DIAMETER_TOO_BUSY`. Diameter Gateway will continue to use the diameter result code `3004 DIAMETER_TOO_BUSY` for the message received from backend services namely, the Diameter Connector and PCRF Core services.

For more information about different response codes that can be configured, see Congestion Control Discard Message Response Code section.

Call Flow

To best understand how the diameter congestion control feature works, consider a scenario where the sample message priority profiles rules are configured as described in the following table:

Table 4-140 Message Priority Profiles

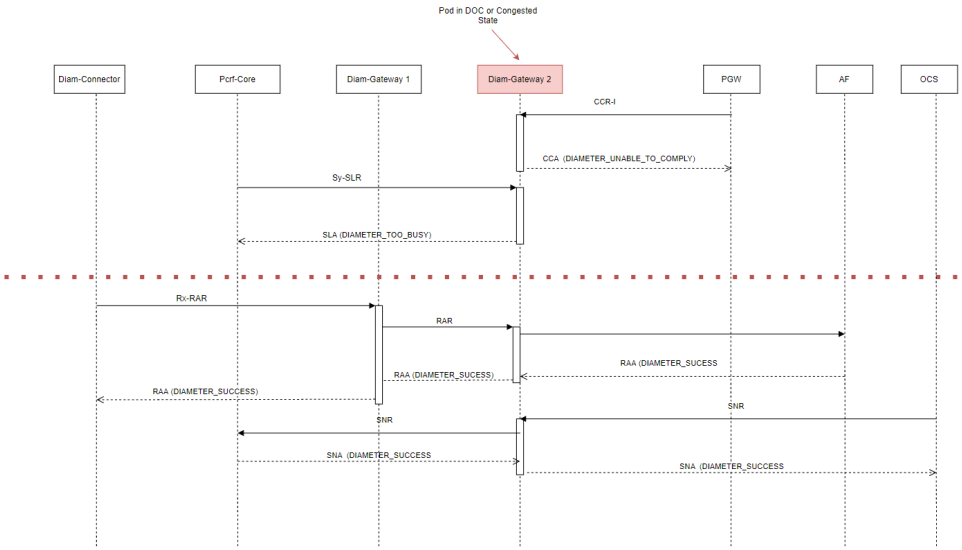
Message	Priority
Default	24
Rx RAR	18
Gx CCR-I	24
Sy SLR	24

> **Note**
>
> The default message profile is only for the purpose of understanding the feature. No default message priority profiles are configured for Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The discard priority congestion states will be in order like CONGESTED → CONGESTION_L1 → CONGESTION_L2 → CONGESTED states. For this call flow, the discard priority are configured with DOC as 22, and Congested as 20. The result code for rejecting request messages is set as DIAMETER_UNABLE_TO_COMPLY (applicable only for external peers).

Figure 4-205 Call flow diagram for Diameter Congestion Control



- When Diameter Gateway 2, currently is either in DOC or Congested state, receives CCR-I request, the priority is compared against discard priority. As both message priority and discard priority values are same, the message is rejected with result code – DIAMETER_UNABLE_TO_COMPLY.
- When Diameter Gateway 2, currently is either in DOC or Congested state, receives Sy-SLR request, the priority is compared against discard priority. As message priority is low in priority than discard priority, the message is rejected with result code – DIAMETER_TOO_BUSY.
- When Diameter Gateway 2, currently is either in DOC or Congested state, receives Rx RAR request, the priority is compared against discard priority. As message priority is higher than discard priority, the message is accepted with result code – DIAMETER_SUCCESS.
- When Diameter Gateway 2, currently in DOC or Congested state, receives SNR request, the priority is compared against discard priority. Since no priority rule is configured for this message request, the message is accepted with result code – DIAMETER_SUCCESS.

Feature Upgrade Impact

With upgrade of Policy application from any of the previous release versions to 25.1.200, the Diameter Gateway pod Congestion Control feature can be updated to use the common Congestion Control mechanism available in 25.1.200. In order to do this, there are some considerations to address, especially due to the difference in configuration data. Diameter Gateway's pod congestion control configurations from the previous version should be migrated to use the current version configurations. The data migration process is manual and one-time activity that user has to perform, by using either the CNC Console or Congestion Control migration APIs.

Feature Transition

Copyright © 2019, 2026, Oracle and/or its affiliates.

Diameter Gateway Congestion Control feature transition between older version to the Policy 25.1.200 Congestion Control mechanism is based on migration status of the Policy application during the upgrade. The migration status can be either in "False" or "True".

False (Before Migration): After upgrading to Policy version 25.1.200, the Diameter Gateway pod congestion control feature still operates under the configurations and designs of the pre-upgrade version until the user actively migrates the setup. In this "Before Migration" state, the users will only see:

- Old Configurations: The Diameter Gateway Congestion Control configurations from the previous application version.
- Previous CNC Console pages: User will have access to the older user interface rather than the new screen designed for Congestion Control feature.
- Legacy REST APIs: Calls to APIs will still work with the previous version's endpoints.

To enable the common Congestion Control mechanism for Diameter Gateway, users will need to complete the data migration process. For more information related to Diameter Gateway Congestion Control configuration migration, see "Migration of Congestion Control Configuration Data" section in Congestion Control Settings page in CNC Console.

True (After Migration): After the upgrade to Policy version 25.1.200, perform the data migration for Diameter Gateway pod Congestion Control feature. With this, the migration status will be "After Migration" and Diameter Gateway services will be able to use the updated Congestion Control mechanisms.

Impact on Bulk Import and Export

There will be impact on import and export of configuration data after this congestion control transition to common congestion control feature and following are the various scenarios of import and export impact of configuration data:

Import Scenarios:
Diameter Gateway congestion control configurations will be imported based on the exported data, system type, and migration status as follows:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-141 Impact for Import Scenarios

Import Scenario	System Type	Migration Status	Result	Details
Congestion Control configuration data exported from old version system and imported to current version system	Fresh Install	NA	Import Successful / Import Partial Successful	Imported configuration data will reflect in the CNC Console in the common congestion control screens. System will be in common congestion control behavior and Load Shedding profiles will be imported in common congestion control topic and message priority profile will be imported to respective DGW message priority topic. **Note**: Result will be *Import Partial Successful* when old congestion configurations diameter settings data contains the congestion load shedding profile as this specific diameter congestion load shedding profile select option is removed from diameter settings in current version and it's moved to common congestion configurations and same old configurations will be reflected for the same and there in no feature impact of this case.
Rx RARCongestion Control configuration data exported from old version system and imported to current version system	Upgrade	Before Migration	Import Successful	Imported configuration data will reflect in the CNC Console in the DGW old congestion control screens. System will be in old congestion control behavior and Load Shedding profiles will be imported in old congestion control topic and message priority profile will be imported to respective DGW message priority topic.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-141 (Cont.) Impact for Import Scenarios

Import Scenario	System Type	Migration Status	Result	Details
Congestion Control configuration data exported from old version system and imported to current version system	Upgrade	After Migration	Import Successful / Import Partial Successful	Imported configuration data will reflect in the CNC Console in the common congestion control screens. System will be in common congestion control behavior and Load Shedding profiles will be imported in common congestion control topic and message priority profile will be imported to respective DGW message priority topic. ***Note***: Result will be *Import Partial Successful* when old congestion configurations diameter settings data contains the congestion load shedding profile as this specific diameter congestion load shedding profile select option is removed from diameter settings in current version and it's moved to common congestion configurations and same old configurations will be reflected for the same and there in no feature impact of this case.
1. Congestion Control configuration data exported from current version system (fresh install) 2. Imported to current version system (upgraded) and data migration not done	1st System: Fresh Install 2nd System: Current Version (Upgraded + Not Migrated)	NA	Import Partial Successful	Import will be partial successful as the congestion configuration data is different in old and new congestion system so that diameter-gateway new congestion control data will not be importing successfully as the current system will be in old congestion control behavior.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-141 (Cont.) Impact for Import Scenarios

Import Scenario	System Type	Migration Status	Result	Details
1. Congestion Control configuration data exported from current version system (fresh install) 2. Imported to current version system (upgraded) and data migration done	1st System: Fresh Install 2nd System: Current Version (Upgraded + Migrated)	NA	Import Successful	Imported configuration data will reflect in the CNC Console in the common congestion control screens as system will be in common congestion control behavior.
1. Congestion Control configuration data exported from current version system (fresh install) 2. Imported to old version system	1st System: Fresh Install 2nd System: Old Version	NA	Import Partial Successful	Import will be partial successful as the congestion configuration data is different in old and new congestion system so that Diameter Gateway new congestion control data will not be importing successfully as the current system will be in old congestion control behavior.

Export Scenarios:
Diameter Gateway congestion control configurations will be exported based on the system type, and migration status as follows:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-142 Export Scenarios

System Type	Migration Status	Result	Details
Fresh Install	NA	Export Successful	Data will export from common congestion feature and threshold and load shedding rules data consist of all four congestion states DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED.
Upgrade	Before Migration	Import Successful	Data will export from old congestion feature and threshold and load shedding rules data consist of only two congestion states DOC and CONGESTED.
Upgrade	After Migration	Import Successful	Data will export from common congestion feature and threshold and load shedding rules data consist of all four congestion states DOC, CONGESTION_L1, CONGESTION_L2, and CONGESTED.

Load-Shedding Profile Storage and Validation

On freshly installed or migrated systems, Diameter Gateway congestion control uses load-shedding profiles from `common.congestioncontrol.loadsheddingrules.diameter-gateway` instead of `common.public.diamloadshedding`.

When you import an older Diameter Settings configuration that specifies an active congestion load-shedding profile, such as LSP-1, the system performs the following actions:

1. Validates the profile against `common.congestioncontrol.loadsheddingrules.diameter-gateway`.
2. If the profile exists, set it as the active load-shedding profile on the **Common Congestion Control** screen for Diameter Gateway.

On upgraded systems, users must manually migrate Diameter Gateway congestion control first. Until migration is complete, profile validation continues to use `common.public.diamloadshedding`.

Unified Message Priority Profile Behavior

From 25.1.100 release onward, congestion control and overload control use a single unified `messagePriorityProfile`.

During imports from earlier releases, the system determines the unified profile as follows:

1. If the congestion MPP and overload MPP are the same, the system uses that profile as the unified profile, such as `MPP-1`.
2. If the congestion MPP and overload MPP are different, the system uses `DEFAULT` as the unified profile because the configuration is ambiguous.
3. If only a congestion MPP is present, the system uses the congestion MPP as the unified profile.
4. If only an overload MPP is present, the system uses the overload MPP as the unified profile.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Conversion of Legacy Diameter Gateway Load Shedding Profiles

On freshly installed or migrated systems, Diameter Gateway load-shedding profiles imported from earlier releases are automatically converted from the legacy two-state format to the new four-state format.

Managing Diameter Gateway Pod Congestion Control

Enable

By default, the Pod Congestion Control is disabled for Diameter Gateway. You can enable this feature using CNC Console or REST API for Policy.

Feature Migration

If the Policy application is upgraded to 25.1.200, then you can enable this feature by performing the migration process. For more information how to perform the data migration, see "Migration of Congestion Control Configuration Data" section in Congestion Control Settings page using CNC Console.

Configure

You can customize the configurations related to this feature using the CNC Console or REST APIs for Policy:

- **Configure using CNC Console:**
  To enable the feature using CNC Console, set the **Enable** parameter in **Settings** page under **Congestion Control** for **Overload and Congestion Control Configurations** for Diameter Gateway Service.

  To configure Diameter Gateway service pod congestion control feature in CNC Console, see Congestion Control section.
- **Configure using REST API:**
  To enable this feature using REST API, perform the feature configurations as described in "Congestion Control" APIs section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

  If the Policy application is upgraded to 25.1.200, then you can enable this feature by performing the migration process. For more information how to perform the data migration using Congestion Control Migration APIs, see "Congestion Migration" APIs section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics:

Diameter Gateway service uses the pod congestion metrics for this feature.The following common service Pod Congestion Metrics are used to provide information about this feature:

- `occnp_pod_congestion_state`
- `occnp_pod_resource_stress`
- `occnp_pod_resource_congestion_state`
- `occnp_pod_cong_state_report_total`
- `occnp_pod_resource_congestion_state_report_total`
- `occnp_congestion_diam_pending_request_active_counter`
- `occnp_congestion_diam_pending_request_end_to_end_id_map_size`

Copyright © 2019, 2026, Oracle and/or its affiliates.

- occnp_congestion_DiamMsgBuffer_queue_msg_count

The following Diameter Gateway Metrics are used to provide information about this feature:

- occnp_pod_resource_congestion_state_report_total
- occnp_congestion_diam_pending_request_active_counter
- occnp_congestion_diam_pending_request_end_to_end_id_map_size
- occnp_congestion_DiamMsgBuffer_queue_msg_count
- occnp_diam_pending_requests
- occnp_diam_congestion_message_reject_total

Alerts

The following alerts are generated for this feature:

- POD_CONGESTED
- POD_CONGESTION_L2
- POD_CONGESTION_L1
- POD_DANGER_OF_CONGESTION
- POD_PENDING_REQUEST_CONGESTED
- POD_PENDING_REQUEST_CONGESTION_L2
- POD_PENDING_REQUEST_CONGESTION_L1
- POD_PENDING_REQUEST_DANGER_OF_CONGESTION
- POD_CPU_CONGESTED
- POD_CPU_CONGESTION_L2
- POD_CPU_CONGESTION_L1
- POD_CPU_DANGER_OF_CONGESTION

Maintain

Error logs are generated when the system is congested and the actions taken to bring the system back to normal. Warning logs are generated to indicate the congestion level. However, error logs are not generated when messages are rejected to avoid additional resource usage to write error logs.

The following is a sample error log:


```
{
  "instant": {
    "epochSecond": 1629306402,
    "nanoOfSecond": 438895435
  },
  "thread": "Thread-10",
  "level": "INFO",
  "loggerName": "ocpm.cne.common.configclient.ConfigurationAgent",
  "message": "Configuration changed, class ConfigurationItem {\n    key:
common.congestionthreshold.diam-gateway\n    value:
{\"stateCalculationInterval\":10000,\"stateChangeSampleCount\":3,\"thresholds\
":[{\"state\":\"DANGER_OF_CONGESTION\",\"resourceUsageLimit\":
{\"cpu\":40,\"memory\":40,\"queue\":20}},
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
{\"state\":\"CONGESTED\",\"resourceUsageLimit\":
{\"cpu\":80,\"memory\":80,\"queue\":50}}]}\n    version: 8\n    topicInfo:
class TopicInfo {\n        id: 6\n        name:
common.congestionthreshold.diam-gateway\n        description: Created by
config server.\n        modifydate: Wed Aug 18 17:06:42 UTC 2021\n
version: 10\n    }\n    labels: null\n}",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 77,
  "threadPriority": 5,
  "messageTimestamp": "2021-08-18T17:06:42.438+0000"
}
```

4.93 Overload Control

Overload means when 100% of the planned capacity is exhausted. It can be due to uneven distribution of traffic towards a given policy service instance, network fluctuations leading to traffic bursts or unexpected high traffic volume at any given point of time.

During overload conditions, the service response times may grow to unacceptable levels, and exhaustion of resources can result in downtime or services exhibiting unexpected behavior. Overload management is a critical requirement for any telecom node, server, and service to protect against downtime and ensure serviceability during extreme overload conditions. Thus, the goal of overload management is to prevent service performance from degrading in an uncontrolled manner under heavy load. When policy service starts approaching its saturation or planned limit, response times typically grow high and throughput can degrade substantially. Under such conditions, it is desirable to shed load based on the operator's configuration, instead of causing all messages and signaling flows to experience unacceptable response times, failures, or downtime.

Policy allows to configure a percentage of messages to be rejected. That is, messages are discarded based on configured percentage. This enables system's overload and congestion control to manage gauge system's load with better accuracy. Also, it allows the user to provide less rejections instead of providing 100% rejections.

Percentage of message rejections for each load level is configurable. Also, the rejection percentage for each message priority can be configured.

For example, if the discard value for CCR-I messages is 50%, when system is under load, only alternate CCR-I requests are processed rejected the rest. That is, 1st CCR-I is rejected and 2nd is accepted.

> **Note**
>
> All CCR-Ts are accepted.

Enable

Follow the below procedure to enable the overload control functionality:

1. Set value for the parameter, **perf-info.overloadManager.enabled**, as `true` in the `custom-values.yaml` file for Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Then, configure the values for the following parameters in the `custom-values.yaml` file:

```
perf-info:
  envMysqlDatabase: ''
  overloadManager:
    enabled: false
    ingressGatewaySvcName: occnp-ingress-gateway
    ingressGatewayPort: *svcIngressGatewayHttp
    # nfType is used to query configuration from common cfg server
    nfType: PCF
    # diam Gateway overload management feature configurations
    diamGWPort: *svcDiamGatewayHttp
```

For more information about setting the parameter values, see *Overload Manager Configurations* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

2. Set value for the field, **Enable Overload Control**, as `true` in **Discard Policy Mapping page** under **SBI** in CNC Console. For more information about this field, see Discard Policy Mapping.

Configure

You configure the overload control feature either using CNC Console, or through REST API.

- **Configure using REST API:** Policy provides `overloadLevelThreshold` and `overloadLevelThresholdProfiles` API end points to configure overload control feature. You can perform the POST, PUT, or GET operations to configure the feature. For more information about REST API configuration, see *Overload Level Threshold* section in *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide*.
- **Configure using CNC Console**: Using CNC Console, you can configure the threshold values based on profiles. For more information, see Overload Control Threshold.

Overload Threshold Values

When Overload control feature is enabled, the load on each service is monitored using the following counters:

- CPU: Indicates the maximum CPU usage in terms of percentage.
- Pending message count: Indicates the number of requests from the gateway to the Policy service for which the response is not yet received.
- Failure count: Failed request count for each service. Indicates the number of error responses that the Policy service receives in error series such as 4XX or 5XX. Different routes mapped to the Policy service can have different set of configured error codes and exception list for tracking the failure counts.
  The error codes set must be configured in the routes configuration. The below table lists the route IDs for each of the services for which the error codes set must be configured.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-143 Supported Route IDs

Service	Routes
SM Service	– sm_create_session_route – sm_delete_session_route – sm_update_session_route – pa_create_session_route – pa_delete_session_route – pa_update_session_route – pa_events_subscription_route
AM Service	– am_create_session_route – am_delete_session_route – am_update_session_route
UE Policy Service	– reverse_ue_service – reverse_ue_service_notify
UDR	– udr_notify_route – reverse_user_udr_notify_service – reverse_user_udr_notify_service
CHF	– chf_terminate_route – chf_notify_route – reverse_user_chf_notify_service
NRF Client	– reverse_nrf_discovery_service – reverse_nrf_management_service – reverse_nrf_notify_service
SOAP Connector	– reverse_soapconnector_service

For details on configuring the route IDs, see *Route Level Configuration* section in *Oracle Communications Cloud Native Core, REST Specification Guide*.

Default Overload Threshold Values

This section describes the recommended default overload threshold values for Diameter Connector, PCRF Core, SM Service, AM Service, UE Policy Service, UDR Connector, and CHF Connector. To calculate threshold values, you must consider the resource values for microservices. The following table lists the default resource values for Diameter Connector, PCRF Core, SM Service, AM Service, UE Policy Service, UDR Connector, and CHF Connector:

Table 4-144 Default Resource Values

Resources	Diameter Connector	PCRF Core	SM Service	AM Service	UE Policy Service
CPU (Limits)	4	8	7	8	8
CPU (Requests)	3	7	7	7	7
Maximum CPU Usage	2.5	4.35	5.4	3.39	3.39
Maximum CPU Usage (%)	63	54	68	42	42
Maximum Replicas	8	8	8	8	8
Maximum TPS	2500	2100	880	675	300

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-144 (Cont.) Default Resource Values

Resources	Diameter Connector	PCRF Core	SM Service	AM Service	UE Policy Service
Maximum TPS (all replicas)	20000	16800	7040	5400	2400
Worst RTT (assumed)	250 ms	250 ms	250 ms	250 ms	250 ms
Maximum Pending Transactions	5000	4200	1760	1350	600

Based on the values in Table 4-144 table, you can calculate the onset and abatement values for load levels - L1, L2, and L3, as shown in the Table 4-145 table.

> **Note**
>
> The values shown in Table 4-144 table are the default values and can be changed depending on the deployment model used.

Table 4-145 Formulas to Calculate Default Overload Threshold Levels

Load Level	CPU (%)	Pending Message Count (Absolute Value)	Failure Count (Absolute Value)
L1 - Onset	80% * C	60% * P	05% * T
L1 - Abatement	75% * C	50% * P	03% * T
L2 - Onset	90% * C	75% * P	10% * T
L2 - Abatement	85% * C	70% * P	08% * T
L3 - Onset	95% * C	90% * P	15% * T
L3 - Abatement	91% * C	85% * P	12% * T

Abatement value is the lower range where as the onset value is higher range for that particular level.

Note:

C denotes the maximum CPU utilization per pod of each of the services shown in Table 4-146 table.

T denotes the maximum incoming TPS of a given service listed in Table 4-146 table.

P denotes the maximum pending transaction size value based on worst RTT and maximum incoming TPS (T).

For example, if Maximum TPS (all replicas) (T) =20000 and Worst RTT (assumed) =250, then Maximum Pending Transactions (P) is calculated as (20000/1000) * 250 = 5000.

> **Note**
>
> You can configure the memory for each of these services.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-146 Messages to be accounted for calculating Service level Ingress TPS

Service Name	Message Types	Metrics Used
SM Service	• SM (Create, Update, Delete) • PA (Create, Update, Delete, events subscription, events un-subscription)	• ocpm_ingress_request_total • ocpm_ingress_response_total For more details on these metrics, see SM Service Metrics.
AM Service	AM (Create, Update, Delete)	• ocpm_ingress_request_total • ocpm_ingress_response_total For more details on these metrics, see AM Service Metrics.
UE Service	• UE (Create, Update, Delete) • N1 Message Notify	• ocpm_ingress_request_total • ocpm_ingress_response_total • ue_n1_transfer_request • ue_n1_transfer_response • ue_n1_transfer_ue_notification_total For more details on these metrics, see UE Service Metrics.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-146 (Cont.) Messages to be accounted for calculating Service level Ingress TPS

Service Name	Message Types	Metrics Used
Pcrf-Core	• Gx CCR (I/U/T) • Rx (AAR, STR)	• occnp_diam_request_local_total (CCR-I) • occnp_diam_response_local_total (CCA-I) • occnp_diam_request_local_total (CCR-U) • occnp_diam_response_local_total (CCA-U) • occnp_diam_request_local_total (CCR-T) • occnp_diam_response_local_total (CCA-T) • occnp_diam_request_local_total (AAR-I) • occnp_diam_response_local_total (AAA-I) • occnp_diam_request_local_total (AAR-U) • occnp_diam_response_local_total (AAA-U) • occnp_diam_request_local_total (RAR Gx) • occnp_diam_response_local_total (RAA Gx) • occnp_diam_request_local_total (RAR Rx) • occnp_diam_response_local_total (RAA Rx) • occnp_diam_request_local_total (STR) • occnp_diam_response_local_total (STA) For more details on these metrics, see PCRF Core Metrics.
Diameter Connector	• Rx (AAR, STR) • Sy SNR	• ocpm_ingress_request_total • ocpm_ingress_response_total For more details on these metrics, see Diameter Connector Service Metrics.
UDR Connector	Policy Data Change Notification	• ocpm_udr_tracking_request_total • ocpm_udr_tracking_response_total For more details on these metrics, see UDR Metrics.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-146 (Cont.) Messages to be accounted for calculating Service level Ingress TPS

Service Name	Message Types	Metrics Used
CHF Connector	• Spending limit report notify • Subscription Termination	• ocpm_chf_tracking_request_total • ocpm_chf_tracking_response_total For more details on these metrics, see CHF Metrics.

The following table lists the default overload threshold values for Diameter Connector:

Table 4-147 Default Overload Threshold Values - Diameter Connector

Load Level	CPU (%)	Pending Message Count	Failure Count
L1 - Onset	68	3250	1000
L1 - Abatement	63	2700	600
L2 - Onset	76	4050	2000
L2 - Abatement	72	3800	1600
L3 - Onset	81	4850	3000
L3 - Abatement	77	4600	2400

The following table lists the default overload threshold values for PCRF Core:

Table 4-148 Default Overload Threshold Values - PCRF Core

Load Level	CPU (%)	Pending Message Count	Failure Count
L1 - Onset	68	1200	840
L1 - Abatement	63	1000	504
L2 - Onset	76	1500	1680
L2 - Abatement	72	1400	1344
L3 - Onset	81	1800	2520
L3 - Abatement	77	1700	2016

> **Note**
>
> On performing fresh installation of Policy, the system is loaded with only CPU threshold values. Using the sample configurations as a reference, you can set the threshold values for pending count and failure count according to the system's capacity.

The following table lists the default overload threshold values for UDR Connector:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-149 Default Overload Threshold Values - UDR Connector

Load Level	CPU (%)	Pending Message Count	Failure Count
L1 - Onset	68	2650	352
L1 - Abatement	63	2200	208
L2 - Onset	76	3300	704
L2 - Abatement	72	3050	560
L3 - Onset	81	3950	1056
L3 - Abatement	77	3700	848

The following table lists the default overload threshold values for CHF Connector:

Table 4-150 Default Overload Threshold Values - CHF Connector

Load Level	CPU (%)	Pending Message Count	Failure Count
L1 - Onset	56	2150	352
L1 - Abatement	52	1800	208
L2 - Onset	62	2700	704
L2 - Abatement	59	2500	560
L3 - Onset	67	3200	1056
L3 - Abatement	63	3050	848

Recommended Overload Threshold Values - SM, AM, and UE Services

The following table lists the default overload threshold values for SM, AM, and UE Services:

Table 4-151 Recommended Overload Threshold Values - SM, AM, and UE Services

Load Level	Service	CPU (%)	Pending Message Count	Failure Count
L1 - Onset	SM Service	68	1100	352
	AM Service	63	1750	270
	UE Policy Service	64	200	120
L1 - Abatement	SM Service	63	900	208
	AM Service	58	1450	160
	UE Policy Service	60	175	72
L2 - Onset	SM Service	75	1350	704
	AM Service	71	2200	544
	UE Service	71	250	240
L2 - Abatement	SM Service	71	1250	560
	AM Service	66	2050	432
	UE Policy Service	68	225	192
L3 - Onset	SM Service	80	1600	1056
	AM Service	75	2600	808
	UE Policy Service	76	300	360
L3 - Abatement	SM Service	76	1550	848

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-151 (Cont.) Recommended Overload Threshold Values - SM, AM, and UE Services

Load Level	Service	CPU (%)	Pending Message Count	Failure Count
	AM Service	70	2450	648
	UE Policy Service	72	275	288

> **Note**
>
> These are the recommended values. It can be modified as per the customer requirements.
>
> The pending message count, and failure counts depend on the deployment capacity. The values shown in the above tables are calculated for the default deployment size. These values must be recalculated as per the deployment requirements.

Observe

Policy provides the following metrics specific to Overload Control feature:

- service_resource_stress
- service_resource_overload_level
- load_level
- system_overload_threshold_config_mode
- active_overload_threshold_fetch_failed

For more information, see PerfInfo Metrics section.

Alerts

- Policy provides the following alerts for overload control feature on SBI interface:
  - `ServiceOverloaded` - This alert is raised whenever a given service is in overload state - L1, L2, and L3.
  - `ServiceResourceOverLoaded` - This alert is raised when a given service is in overload state - L1, L2, or L3 due to resource types such as memory, CPU, pending count, and failure count.
- Policy provides `PERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED` alert for overload control threshold configuration. This alert is raised when the service is unable to fetch the current active overload threshold data.

Maintain

Error logs are generated when the system is overloaded and the actions taken to bring the system back to normal. Warning logs are generated to indicate the change in load level.

4.93.1 Overload Control- Diameter

For Diameter Gateway, Policy provides the following means for overload management:

- Pre-defined threshold load levels.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Tracks number of pending messages of PCRF core and Diameter Connector from Diameter Gateway.
- Tracks CPU and memory usage of PCRF core and Diameter Connector.
- Enforce load shredding during various overload levels based on priority and percentage discard value for each priority. The priority and percentage discard value are configurable.

Configure

To configure the threshold values (REST API only), discard priority, percentage discard value, and error codes for each defined level for overload control, you can use CNC Console as well as REST API.

- **Configure using CNC Console:** Perform the feature configurations on the Load Shedding Profiles and Message Priority Profiles page. For more information about the configurations, see Load Shedding Profiles.
- **Configure using REST API:** Policy provides the following REST API for configuring diameter gateway overload control feature:
  Load Shedding Profiles: {apiRoot}/oc-cnpolicy-configuration/v1/diameter/loadsheddingprofiles

  Message Priority Profiles: {apiRoot}/oc-cnpolicy-configuration/v1/diameter/messageprioritypprofiles

  You can perform the POST, PUT, or GET operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

The following are the recommended configurations for load shedding profile and message priority profile respectively for overload control:

```
{
  "name": "default_overload_control_msg_priority_profile",
  "priorityRules": [{
    "ruleName": "Gx_CCR_I",
    "messagePriority": 14,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Gx",
      "message": "CCR",
      "preDefinedAVPConditions": [{
        "conditionName": "CC-Request-Type",
        "conditionCCRTValue": ["INITIAL_REQUEST"]
      }]
    }
  }, {
    "ruleName": "Rx_AAR_I",
    "messagePriority": 13,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Rx",
      "message": "AAR",
      "preDefinedAVPConditions": [{
        "conditionName": "Rx-Request-Type",
        "conditionRxRTValue": ["INITIAL_REQUEST"]
      }]
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    }
  }, {
    "ruleName": "Gx_CCR_U",
    "messagePriority": 12,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Gx",
      "message": "AAR",
      "preDefinedAVPConditions": [{
        "conditionName": "CC-Request-Type",
        "conditionCCRTValue": ["UPDATE_REQUEST"]
      }]
    }
  }, {
    "ruleName": "Gx_CCR_T",
    "messagePriority": 8,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Gx",
      "message": "CCR",
      "preDefinedAVPConditions": [{
        "conditionName": "CC-Request-Type",
        "conditionCCRTValue": ["TERMINATION_REQUEST"]
      }]
    }
  }, {
    "ruleName": "Sy_SNR",
    "messagePriority": 6,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Sy",
      "message": "Sy-SNR",
      "preDefinedAVPConditions": []
    }
  }, {
    "ruleName": "Rx_STR",
    "messagePriority": 7,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Rx",
      "message": "STR",
      "preDefinedAVPConditions": []
    }
  }, {
    "ruleName": "Rx_AAR_U",
    "messagePriority": 11,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Rx",
      "message": "AAR",
      "preDefinedAVPConditions": [{
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
        "conditionName": "Rx-Request-Type",
        "conditionRxRTValue": ["UPDATE_REQUEST"]
      }]
    }
  }]
}


{
  "name": "default_overload_control_load_shedding_profile",
  "type": "Overload Control",
  "overloadLoadSheddingRules": [{
    "level": "L1",
    "discardPriority": 13,
    "ansWithResultCode": "DIAMETER_TOO_BUSY"
  }, {
    "level": "L2",
    "discardPriority": 11,
    "ansWithResultCode": "DIAMETER_TOO_BUSY"
  }, {
    "level": "L3",
    "discardPriority": 6,
    "ansWithResultCode": "DIAMETER_TOO_BUSY"
  }]
}
```

Observe

Policy provides the following metrics specific to Overload Control feature for diameter gateway:

- diam_overload_message_reject_total

For more information, see Diameter Gateway Metrics section.

4.93.2 Overload Control- SBI

For HTTP signaling, Policy overload management provides following means for overload management:

- Tracks number of pending messages for an exposed policy service in its NF Profile.
- Tracks number of failed responses (configurable as error code by operator) generated by exposed policy service in its NF Profile.
- Determine the overload level of system using data collected from point 1 and 2, against planned threshold levels (based on planning).
- Enforce load shredding during various overload levels.

Configure

To configure the discard policies, discard policy mapping, and error code profiles for overload control, you may use CNC Console as well as REST API.

> **Note**
>
> Currently, threshold values can be configured using REST API only.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Configure using CNC Console:** Perform the feature configurations on the Discard Policy Mapping, Discard Policy, and Error Code Profiles pages. For more information about the configurations, see Overload and Congestion Control Configurations.
- **Configure using REST API:** Policy provides the following REST API for configuring overload control feature on SBI interface:
  OC Policy Mapping: {apiRoot}/PCF/nf-common-component/v1/igw/ocpolicymapping

  OC Discard Policies: {apiRoot}/PCF/nf-common-component/v1/igw/ocdiscardpolicies

  Error Code Profiles: {apiRoot}/PCF/nf-common-component/v1/igw/errorcodeprofiles

  You can perform the GET, PUT, or PATCH operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

The following are the recommended configurations for default message priority values for overload control:

Table 4-152 Default Message Priority

Message Type	Priority
Create SM Policy Association	24
Delete SM Policy Association	16
Update SM Policy Association	18
UDR Notify	18
CHF Terminate	18
UDR Notify	18
CHF Notify	18
Create PA Application Session	24
Delete PA Application Session	16
Update PA Application Session	18
Subscribe PA Events	18
Unsubscribe PA Events	18
Create AM Policy Association	24
Delete AM Policy Association	16
Update AM Policy Association	18
Create UE Policy Association	24
Delete UE Policy Association	16
Update UE Policy Association	18

Note

when creating SBI Error code Profile for SBI overload control that has to be associated with discard policy, ensure that the created profile has Error Cause, Error Title, and Error Description fields. If these fields are not present, then the Ingress Gateway will return 500 error instead of configured error code in profile. Similarly, when creating error code profile through {apiRoot}/PCF/nf-common-component/v1/igw/errorcodeprofiles API, these fields must be populated in JSON request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.93.3 Enhancement to Overload Control Handling in SM Service

At SBI Gateway side, to handle the load shedding conditions, messages are either rejected based on the priority of a message or 'n' percentage of messages are rejected. With this limited capability even messages which are important but may not be carrying higher priority can get discarded.

To handle overload situation, Policy supports the following two actions at SM service:

- Reject action
- Assume Positive
- **Reject action**: In addition to overload control actions at SBI Gateway, Policy also supports load shedding at the Policy micro service's level (SM service).

  Policy microservices perform overload threshold actions like accept and reject, which can be controlled based on message attributes and message type. Message attributes include DNN and S-NSSAI for N7 (Create/Update/Delete) requests and Message Attributes include DNN and ServiceURN for Diameter Rx messages request.

  Here is a sample use case of rejection of messages:

  For a SM Create request with DNN as IMS and with the reject rule setup as 50% at L3 load level. After SM service reaches overload level L3, 50% of the SM Create requests that SM service receives are rejected.
- **Assume Positive action**: Assume Positive is a fail-fast mechanism for overload handling. Assume Positive action allows to suppress flows for a request, but still resulting in a success response. That is, the system still returns a success response even after suppressing the flows. The fail-fast mechanism provides a short-circuiting processing paths to protect capacity and latency.

  Assume Positive action suppresses the following interactions for a message when the system is in overload state:

  – User Data interaction
  – Spending Limit Data Interaction
  – Policy Evaluation

  A request message received at the Microservice interacts with a few services for certain features as configured and excludes the interaction with other services for other features.

  For example, when SM service is in certain overload state, it handles the different SM Association related requests over N7 Interface with minimal processing and responds back to SMF with success. If a underlying feature interaction for Policy evaluation is skipped, even then the return response for that can be considered as a success and attempts to return with default policy rules are made. These default Policy rules are also extended and can be configured to return different Policy rules based on various message attributes.

  In order to apply the Assume Positive action, Service Profiles must be created and associated with the overload configuration. The Service Profiles enable to specify which feature interactions to include or exclude. For details on configuring service profiles, see Service Profiles.

  Currently, Policy supports applying the Assume Positive action for the following feature interactions:

  – **User Data Interaction**: to control interaction related to user data or to control interaction for any operator specific data. Also, determines if SM service should interact with PDS for User data and subscription.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Interaction related to user data refers to interaction with data sources such as UDR (including SSV interaction), LDAP or any other user data source. Disabling user data interaction disables all the communication related user data sources.

SSV GET or Update towards UDR are also restricted.

- **Spending Limit Data Interaction**: to control interaction related to spending limit data. Also, determines if SM service should interact with PDS for CHF data and subscription.

> **Note**
>
> Interaction related to spending limit data refers to interaction with data sources such as CHF or OCS.

- **Policy Evaluation**: to control interaction with PRE service for Policy evaluation.

Default Processing

There can be a situation when Policy decisions are not evaluated by the PRE service due to various reasons, but it is still necessary to return default Message Processing responses, such as default PCC Rules and Session Rules to the consumer NF (like SMF) on session creation. In such a situation, it is necessary to determine whether the message should interact with Producer NFs like BSF for binding registration or CHF for retrieving policy counters as well. For all these Message Processing response actions, there must be a way to configure different action responses based on interface type, message type and message attributes of a received message. To enable this capability, a new Default Processing Profile must be configured and then associated with the Overload Configuration profile. This allows responses to be generated and sent to the SMF even when PRE does not evaluate the response. Response generation is configurable within the SM service based on message attributes such as DNN, SNSSAI, and message type.

The configured Default Processing Profile drives the PCC and session rule to be returned in response towards SMF.

The Default Profile configured also controls the Binding and Async CHF flows.

Default Processing Profiles can be used under the following cases:

- When Policy Evaluation is disabled from PCF Session Management screen.
- When Policy Evaluation is disabled from Service Profiles screen.
- When an error response comes from PRE or service exceptions while sending request to PRE.

For details on configuring the Default Processing Profiles, see Default Processing Profiles.

The following are the supported default processing actions:

- PCC rules to return in responses
- Session rules to return in responses
- BSF registration along with mode of registration (Synchronous/ asynchronous)
- CounterIDs to fetch from CHF (ALL/Specfic)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Returning the default processing responses takes priority over the current default Message processing response that exists and can co-exist depending on the configuration

Default PCC and session rules configured with the Default Processing Profile is applicable only during session creation. Installation of PCC or session rules on subsequent triggers (such as Update) is conditional and can be performed only through PRE evaluation.

If the Default Processing Profile configuration provides any default PCC or session rules for Update or Delete operations, such PCC or session rules are ignore.

`MSG_PROCESSING_DEFAULTS.ENABLED_ON_PRE_FAILURE` advanced settings key for PCF Session Management can be used to apply the default PCC rules and session rules configured using Default Processing Profile on Session creation in case of PRE failure (non 2xx response / exceptions). For more details on configuring `MSG_PROCESSING_DEFAULTS.ENABLED_ON_PRE_FAILURE`, see PCF Session Management.

If BSF interaction mode selected during session creation is changed through Default Processing Profile during subsequent triggers such as Update, the same behavior is applicable that was present with Default Processing Profile during session creation. This behavior is similar to how PRE handles BSF registration.

Policy Counters ID to be fetched, if configured with Default Processing Profile are applied during Create operation only.

Default Processing Profile is not applied during Deletion operation.

Policy Evaluation Precedence for Default Processing Profile

For PCF Session Management, Policy Evaluation must be enabled at both the PCF Session Management configuration level and the associated Service Profile level for policy evaluation to be performed. If Policy Evaluation is disabled at either level, PCF-SM does not perform policy evaluation for the request and uses the configured Default Processing Profile, where applicable. When Policy Evaluation is disabled in PCF Session Management but enabled in the associated Service Profile, the PCF Session Management setting takes precedence and the Default Processing Profile is used.

Application of Reject and Assume Positive Actions

The overload actions are applied based on message properties like interface type, message type, priority, and message attributes like DNN, S-NSSAI, and ServiceURN, which are included in the incoming request .

Rejection and Assume Positive actions are applied during overload conditions when the system reaches a configured Load Level. Supported load levels are L1 to L10. Rejection and Assume Positive action rules can be configured independently, or both actions can be combined within a single rule.

Rejection of messages or application of Assume Positive action within Policy microservice during overload state supports the following logical schemes:

- Priority-based rejection or Assume Positive action: Reject and/or apply Assume Positive action to all requests with message priority greater than or equal to the configured message priority threshold rule.
  For example, threshold rule 7 rejects message with priorities 7 and above.
- Percentage-based rejection or Assume Positive action: Reject and/or apply Assume Positive action to a configured percentage of incoming requests, regardless of message priority.
  For example, a 30% rejection rate drops approximately 3 out of 10 requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Priority and percentage-based rejection or Assume Positive action: Apply percentage-based rejection and/or Assume Positive action only to requests that satisfy the configured priority threshold.
  For example, threshold 5 with 40% rejection drops approximately 40% of requests with priority >= 5; 60% of request with priority>=5 are accepted; requests with priority < 5 are accepted.

Decision regarding rejection action or Assume Positive action is configurable based on message:

- Interface Type
- Message Type
- Message Priority
- Message Attributes

Table 4-153 Enhanced Overload Actions (Reject and Assume Positive Actions) Supported per Interface Type, Message Type, and Message Attributes

Interface Type	Message Type	Message Attributes	Enhance Overload Action Supported
Npcf_SMPolicyControl	• Create • Update • Delete	• DNN • S-NSSAI	• Reject • Assume Positive
• Diameter Rx • NPcf_PolicyAuthorization	• Create • Update • Delete	• DNN • SERVICE_URN	Reject
Other	BSF_Audit_Notificaiton	N/A	Reject

Load Level Information in SM Service

Every single pod of the SM service obtains information about the overload level of the microservice. For this purpose, pods of the microservices polls the Perf-info through Perf-info API at regular intervals to read overload level information.

The load level for SM service, as calculated by Perf-info and used for overload actions in SM service, do not include ‘Failure Counts’ in its calculation. Instead, only CPU usage and Pending Message Count are considered when assessing load levels. As a result, the load levels reported by SM service can differ from those reported by Ingress Gateway. This does not impact the load level calculations that Perf-info performs for Ingress Gateway.

Overload Configurations

The following must be configured for this feature:

- Configure the message attributes to configure master data to DNN, S-NSSAI, and Service Urn:
  - Configure Data Network Name (DNN) profiles as explained in DNN.
  - Configure S-NSSAI profiles as explained in S-NSSAI.
  - Configure Service URN profiles as explained in Service URN.
- Configure the message profiles as explained in Message Profiles.
  Configuring message profiles involves assigning message priority and message identity (Message ID) to a request. There can be multiple message rules to group the incoming traffic at SM service based on `Interface Type`, `Message Type`, and setting conditions to

Copyright © 2019, 2026, Oracle and/or its affiliates.

message attributes to assign `Rule priority`, and `MessageID` to a request. These `MessageIDs` are used to configure the overload control rules in **Overload Configurations** page. The supported interface types are `Npcf_SMPolicyControl`, `Npcf_Policy_Authorization`, `Diameter_Rx`, and `Other` (for BSF Audit Notification).

For an overload action, there may be scenarios where multiple Message IDs could match the incoming message attributes. In such cases, the MessageID with the highest rule priority among the configured overload rules in the overload profile will be considered as the primary match. If no overload rule is found corresponding to the primary match, then next matched Message ID according to rule priority is considered for overload rule matching.

If no overload rule exists for the current overload condition, then the system should select the overload rule configured at the nearest lower load level based on the Message ID.

A rule Priority with the lowest natural number is consider as the highest priority. This is applicable to the `Rule Priority` definition for `MessageIDs` in `Message Profiles`, and `Rule Priority` definition in `Overload Configuration`.

- Configure the Service Profiles as explained in Service Profiles section.
- Configure the Default Processing Profile as explained in Default Processing Profiles.
- Perform the Overload configurations using message profiles as explained in Overload Configurations.
  Configure the overload control rules for each message ID and overload level. Overload configurations allows to reject messages or apply Assume Positive action based on message priority, reject percentage, or on both message priority and reject percentage.
- Before enabling overload control at SM service, enable the feature at the SBI gateway. For details, see *Enable* section in Overload Control.

  Enable **Enhanced Overload Control Level** for SM service and configure **Overload Configuration Profile** to specify the load level and the name of the overload configuration profile to be assigned. For more information, see PCF Session Management.

  By default, the overload control feature for the microservice is disabled with the value of **Enhanced Overload Control Level** as `DISABLED` and no profile selected for **Overload Configuration Profile**.

For more details on rule mapping, see Overload Rule Mapping.

The incoming SBI messages at SM service are rejected or subjected to Assume Positive action in the following scenario:

- Overload reject actions and Assume Positive actions are performed for any new SM Create, Update, Delete session requests only when the feature is enabled and the Overload configurations present are matched with the received requests interface type, message types and message attributes along with condition that SM service is in overload state as well.

  The overload reject actions are also performed for any new PA requests, Rx requests (for SM-Rx call flows) and BSF Audit notifications when the feature is enabled and the Overload configurations present are matched with the received requests interface type, message types and message attributes along with condition that SM service is in overload state as well.

> **Note**
>
> The overload control feature can be enabled using **Enable Overload Control** field on **Discard Policy Mapping** page under **Overload Control** on CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Overload reject action and Assume Positive action is performed for SM Update, and Delete requests, when the feature is enabled, the system is in overload state, Overload rules are present, and during the SM Create the feature was enabled but system was not in Overload state.

  Overload reject action is also performed for PA Create requests, when the feature is enabled, the system is in overload state, Overload rules are present, and during the SM Create the feature was enabled but system was not in Overload state.

Recommended Configuration

- When configuring a Service Profile for a message request with a specific DNN, SNSSAI, or both, disabling User Data and Spending Limit Data interactions will completely stop SM-service communication with PDS. This helps reduce downstream interactions and supports load recovery during overload. However, it can also result in stale records in PCF and in producer services such as UDR and CHF. Therefore, it is recommended to disable these interactions only under very high load conditions, typically driven by elevated Failure Count and Pending Message Count.
- It is recommended to enable either User Data or Spending Limit Data interactions when Policy Evaluation is not restricted. However, if Policy Evaluation interaction is disabled, there is no advantage in enabling User Data and Spending Limit Data.
- If User Data interactions is skipped as part of an Assume Positive action, there will be no interaction with UDR. As a result, SSV-related updates will also not be sent towards UDR, and stale records may remain at UDR.
- If the **Validate User** field needs to be enabled, it is recommended not to use the Assume Positive action, as the two are contradictory. **Validate User** relies on User Data and Spending Limit Data checks before sending a response to the SMF, whereas Assume Positive prevents interactions with external NFs such as UDR and CHF.
- For message requests with a DNN such as IMS, binding creation should always be performed and must not be skipped.
- Since load-level rejections can be configured both at the Gateway and within SM service, the following is recommended:
  - Configure reject actions at the Gateways primarily for higher load levels.
  - Configure DNN-based rejections at lower load-level for DNNs that do not contribute to traffic flow and do not impact internet or IMS traffic call flows (for example, App/Admin DNNs can be rejected at lower load levels, while Internet and IMS traffic should be allowed to pass through).
- Assume Positive actions are recommended to be configured for the intermediate range of load levels.
- If overload control configurations are changed during runtime:
  - It is recommended that DNN Profiles, S-NSSAI Profiles, Service URN Profiles, Message Profiles, and Overload configuration must be configured during downtime or offline hours for a site and specifically when the system is not in overload state.
  - It is also recommended that updating configuration for DNN, S-NSSAI , Service URN must be performed during downtime or offline hours for a site.
  - It is recommended that, to remove any DNN, S-NSSAI , or Service URN from the system, the respective configuration of DNN, S-NSSAI , Service URN mapped with in Message Profiles must be removed first before removing these configuration from their respective Profile pages. Currently, Policy does not support Referential Integrity.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Updating the DNN, S-NSSAI , Service URN profile configurations during Overload state can impact the Overload actions:
  * If the Overload reject actions were originally written for a DNN, for example DNN1. If the value of DNN1 is changed to DNN2 within the DNN Profile, then the existing overload configuration written for DNN1 is not changed to reflect DNN2 (due to referential integrity issue present in CM GUI).
  * If an Overload reject action written for Create, Update, or Delete for DNN1. During an overload state, if the value of DNN1 is changed to DNN2 within the DNN Profile and there are overload actions written for DNN2 and DNN1 actions are removed as well, although expectation with this use case can be that for DNN1 Update or Delete should not be performed, but in this use case Update or Delete action is performed for DNN1.
  * The attribute IDs (dnnId/SnssaiId/ServiceUrnId) used for initial message (such as, N7_create or N5_create) is applicable to all the corresponding subsequent messages (such as N7_update and N7_delete).
  * If the DNN profile is changed (that is, DNN for a given ID is changed or DNN profile is removed) but the **Message Profile** is not updated accordingly, the subsequent messages continue to use the initial attribute ID and matches to the message rule if that attribute ID is still present on message profile.

  To avoid these discrepancies, it is recommended to create the overload configurations when the system is not in Overload state and manually maintain the referential integrity across the configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

- The Assume Positive action by Policy supports only signalling flows over the N7 interface. Currently, Assume Positive action over N5, Diameter Rx, User Data, Spending Limit Data Notification, and AF update/terminate notifications are not supported.
- Assume Positive actions and rejections at the SM level are not applicable to internal session termination/deletion and clean up requests initiated by the SM service itself. These overload actions must only be applied to external requests, and explicitly excluded for internally generated requests.
- – Currently, Assume Positive feature do not restrict binding or BSF flows. In scenarios where Policy Evaluation Interaction is limited, the Binding Registration can be managed using the Default Processing Profile capability introduced.
  - Currently, Regex support for DNN and Service URN are not supported. However, the configuration does allow for an Assume Positive action to be applied to all DNNs within a single rule.
  - Currently, Policy supports load levels from L1–L10 only for PCF Session Management and Diameter Connector when configuring overload control thresholds, as enhanced overload control is implemented exclusively for the N7 and Diameter Rx interfaces. For all other flows, Policy supports load levels from L1-L3.
  - The overload state that triggers the Assume Positive action is determined solely by the load level of the SM service.
  - Currently, Policy does not support handling stale PDS records resulting from the Assume Positive action, such as marking records for audit clean up without checking with the core service.

Handling of BSF Audit Notification and Session queries:

SM service currently does not distinguish between BSF Audit Notification session queries and manual session queries originating from CNC Console. Therefore, any enhanced overload processing configured for BSF Audit Notification is applied to all SM session queries.

If required to apply specific handling only to BSF Audit Notification session queries, ensure that the message priority is assigned at the Ingress Gateway for BSF Audit Notification requests. The BSF message profile **Priority Override** is set to `Never`.

If a non-default Overload Threshold profile is Active and is exported, and then imported again (with or without changes to the threshold values), and the import file contains the same profile name with Active status, the update is not permitted. The import completes with a partial success result, and the import report includes the message: "`Cannot update an active profile`".

When the Replace option is used during import, an Active profile included in the import ZIP can replace the currently active threshold profile if the imported active profile name is different from the name of the current active profile.

Specific error response propagation towards BSF for Audit notification

For BSF Audit Notification request rejection, PCF Binding service masks non-404 error responses from internal services (in this case, Query service to SM service) and sends a generic error 500 towards the BSF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Handling Emergency Calls

Configuring multiple MessageIDs for the same DNN can lead to unintended Reject or Assume Positive (AP) behavior. Therefore, it is recommended to define Message Profile rules using specific DNN values rather than leaving the DNN filter empty (which would match all values). This is especially important for Emergency handling. Messages with Emergency DNNs should be configured using a dedicated rule and assigned the highest priority to ensure that they are not inadvertently rejected.

Multi-site Configuration

It is recommended that DNN, SNSSAI, ServiceURN, Message Profiles, and Overload Profiles configurations should be the same across multi-site deployment. For this purpose, it is recommended to configure at one site and use export and import features to perform configurations at other sites.

Upgrade and Rollback Impact

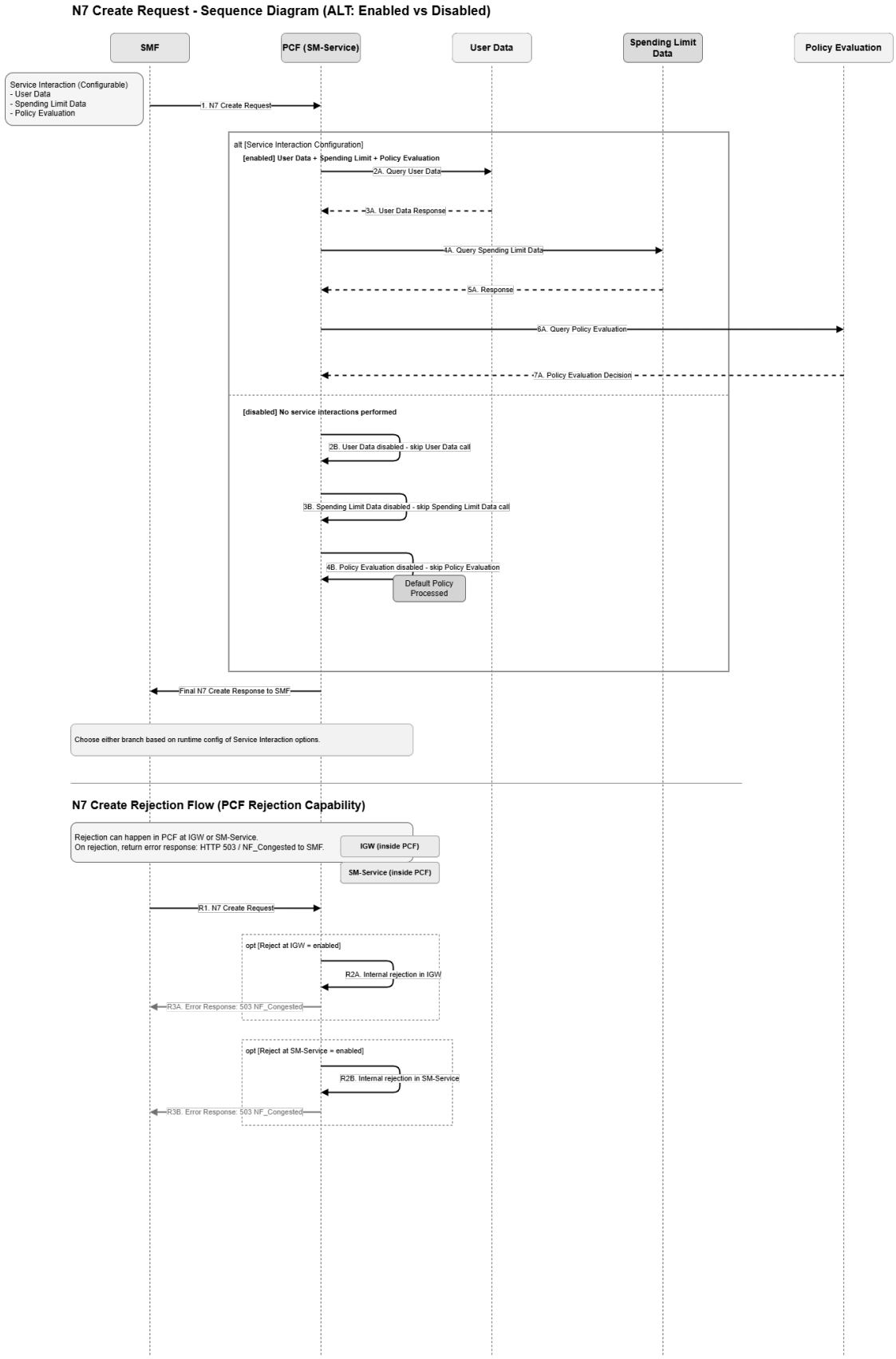
Subscriber sessions created in the release supporting this feature will not work if release version is rolled back to a version that is not supported. If the enhanced overload control feature was turned on and the sessions were created, and later the release was rolled back to an older version which does not support this feature, sessions will fail for the next update or delete requests. Therefore, it is recommended to enable this feature only when the rollback of the release is not required.

Call Flow

The following diagram depicts the sample scenarios for Assume Positive action during overload situation:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-206 Assume Positive Scenarios



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Assume Positive action starts with SM service determining its service load level.
2. Once the current load level is determined , when SM service receives an external request, it maps the corresponding Service Profile to the incoming message and load level.

   Service Profile contains applicable Assume Positive restrictions which can be mapped to specific DNN/SNSSAI/SERVICE_URN, Message Type and Interface Type.
3. SM service determines the applicable Assume Positive restriction based on the mapped Service Profile and applies the restrictions in its communication with internal services for load recovery.

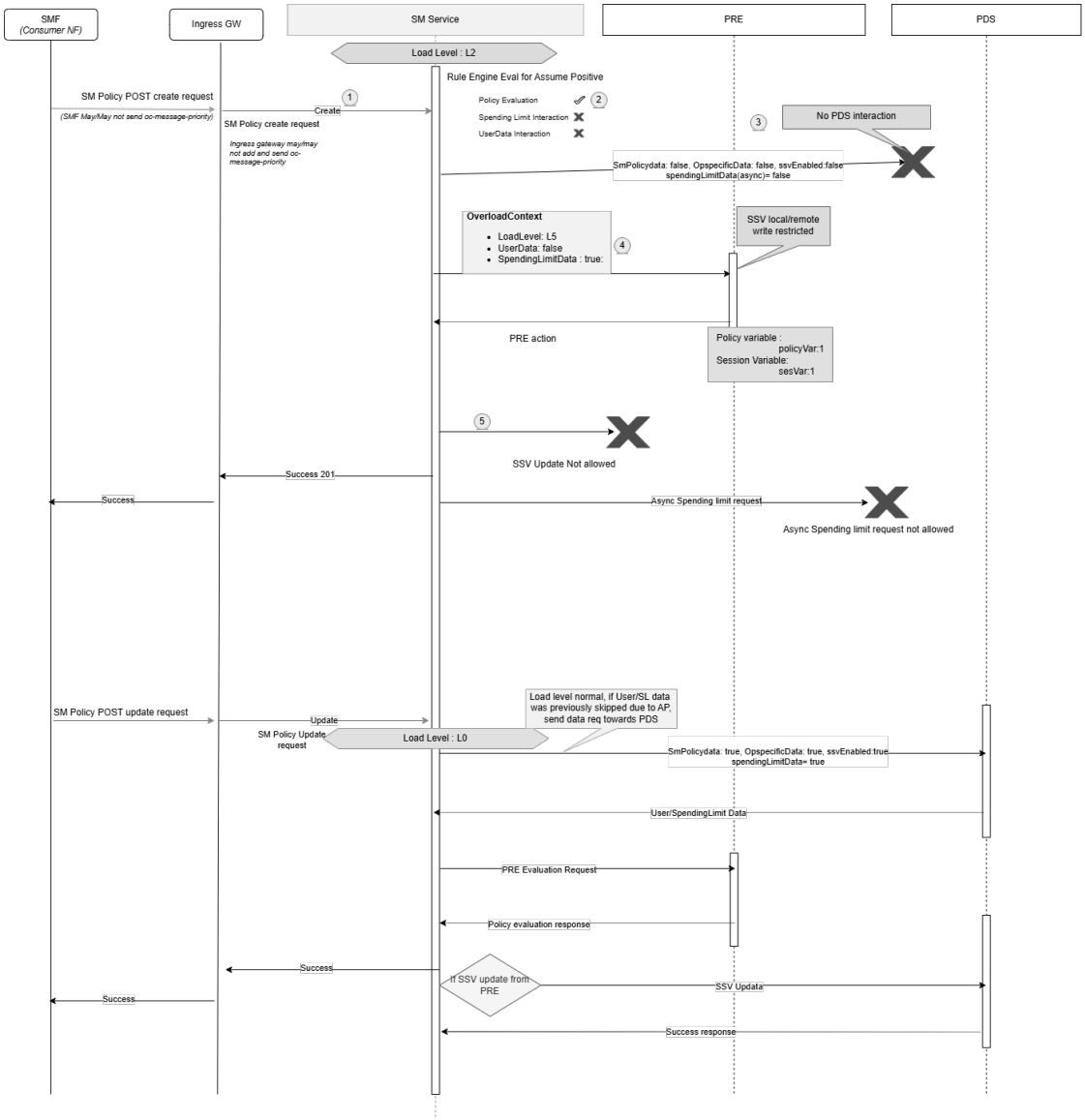
   Service Profile has configuration to limit interactions to PDS(for User Data, SpendingLimit Data) and PRE(Policy Runtime Engine).

   At comparatively higher levels, the SM service can choose to apply both UserData and SpendingLimitData restrictions which can limit the complete interaction with PDS.

> **Note**
>
> Restricting UserData inherently disables SSV interaction flow with PDS for local and Remote SSV.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-207 Assume Positive Action with Restricted Interaction with PDS

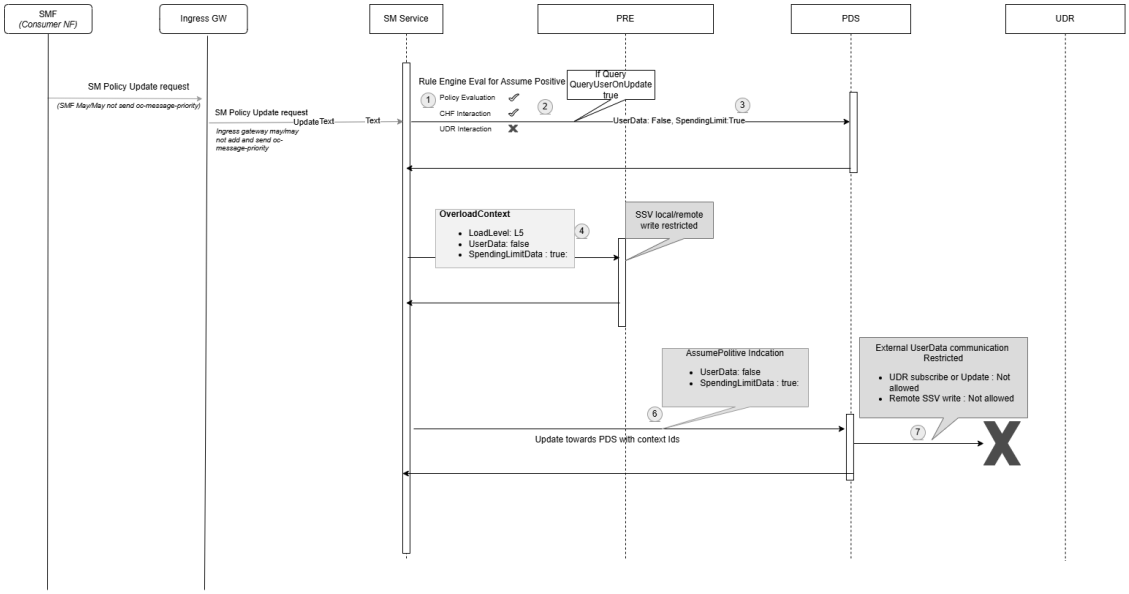


1. SM service, operating in a configured overload state at L2, determines and maps the appropriate Service Profile corresponding to each incoming request.
2. Based on the selected Service Profile with only Policy evaluation enabled, and Spending Limit interaction and UserData interaction are disabled at a specific configured percentage, SM service flags an incoming request for assumePositive-based UserData and spending limit data restriction.
3. SM service disables the access to UserData (SmData and Operator-Specific data) and Spending Limit Data, including SSV fetch from PDS.
4. An indication representing the Assume Positive restriction on UserData is forwarded to PRE to ensure policy evaluation considers the restriction applicable to SSV GET/UPDATE.
5. Any SSV UPDATE request received under the Assume Positive UserData restriction is discarded, and no SSV update call is issued to PDS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

6. An SM Update request is received and when the load level is normal at L0, and there is no restriction on UserData or SpendingLimit data, SM service forwards the corresponding indication to PDS.
7. PDS processes the request normally and responds to SM service.

Figure 4-208 Assume Positive Action with Restricted Interaction with UDR



1. SM service, when operating in a configured overload state at L2, determines and maps the appropriate Service Profile corresponding to each incoming request.
2. Based on the selected Service Profile with interaction with PRE for Policy evaluation and interaction with CHF for Spending Limit data are enabled, interaction with UDR for UserData interaction is disabled at a specific configured percentage, SM service flags an incoming request for assumePositive-based UserData.
3. SM service disables the access to UserData (SmData and Operator-Specific data), including SSV fetch from PDS.
4. An indication representing the Assume Positive restriction on UserData is forwarded to PRE to ensure policy evaluation considers the restriction applicable to SSV GET/UPDATE.
5. PDS interaction with UDR for UserData is restricted, and no remote SSV update call is issued to UDR.
6. PDS interaction with CHF for spending limit data is enabled.
7. SM service sends Update request towards PDS with context IDs and receives a response.

> **Note**
>
> If the Assume Positive feature is disabled/unsupported when an SM Create is processed for a session, enabling the feature later, either in the same Policy version or after upgrading to a newer Policy version does not cause the feature to be applied to subsequent SM Update or SM Delete messages for that session.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing Overload Control Handling in Policy Microservices

Enable and Configure

The Perf-info service manages the overload level information for Policy microservices. Overload Manager feature must be enabled at Perf-info and also in the SBI gateway for making the load level info available.

For details on enabling overload control at the SBI gateway, see *Enable* section in Overload Control.

To enable and configure overload control at SM service using CNC Console or REST API follow the below sections.

Using CNC Console

Enable **Overload Control** flag to `true` in **Discard Policy Mapping** screen.

- Configure the message attributes to configure master data to DNN, S-NSSAI, and Service Urn. For more information, see:
  - DNN
  - S-NSSAI
  - Service URN
- Configure the Message Profiles. For more information, see Message Profiles.
- Configure the Service Profile. For more information, see Service Profiles.
- Configure the Default Processing Profile. For more information, see Default Processing Profiles.
- Perform the Overload configurations using message profiles. For more information, see Overload Configurations.
- Enable **Enhanced Overload Control Level** for SM service and configure **Overload Configuration Profile** to specify the load level and the name of the overload configuration profile to be assigned. For more information, see PCF Session Management.

  Browse to **PCF Session Management** page for **Service configurations** on CNC Console:
  - Select a load level for **Enhanced Overload Control Level** field. By default, the value of this field is `DISABLED`.
  - Select the Overload configuration profile under **Overload Configuration Profile** field. By default, no profile is selected for this field.
  - Configure the **Default Processing** for SM service.

  For more information, see PCF Session Management.

Using REST API

This feature can be configured using the following APIs:

- DNN API to create DNN profiles.
- Service URN API to create Service URN.
- SNSSAI API to create S-NSSAI profiles.
- Message Profile API to create Message profiles.
- Overload Configurations API to perform advanced overload control configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Service Profile API to create service profiles.
- Default Processing Profile API to create default processing profiles.

Also, configure the following parameters in Session Management Service API to enable the feature for SM service:

- overloadConfiguration.enhancedOverloadControlLevel
- overloadConfiguration.overloadConfigurationProfile
- defaultProcessing.smdpProfile

Enable the feature by configuring `overloadConfiguration.enhancedOverloadControlLevel` parameter in Session Management Service API.

For more information, see *Session Management Service* section in *Oracle Communications, Cloud Native Core, Converged Policy REST Specification Guide*.

For more information, see *Oracle Communications, Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

Metrics

The following metrics are used to support the overload control mechanism at SM service.

- occnp_enhanced_overload_reject_total
- occnp_service_load_level
- occnp_load_level_polling_request_total
- occnp_load_level_polling_response_total
- occnp_load_level_polling_exception_total
- occnp_polled_load_level_total
- occnp_enhanced_overload_service_interaction_total
- occnp_enhanced_overload_ssv_update_skipped_total

For more information, see SM Service Metrics.

Alerts

The following alerts are used to support the overload control mechanism at SM service:

- SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_CRITICAL
- SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR
- SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MINOR
- SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_CRITICAL
- SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MAJOR
- SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MINOR

For more information, see Common Alerts.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Logging

For all the rejected message are captured as 'ERROR' messages having information related to message filter Attributes(DNN, SNSSAI, ServiceURN), overload levels, and MessageType.

The messageIds matching the incoming request are also printed including message_id, rule priority, interface type, attribute name and its value.

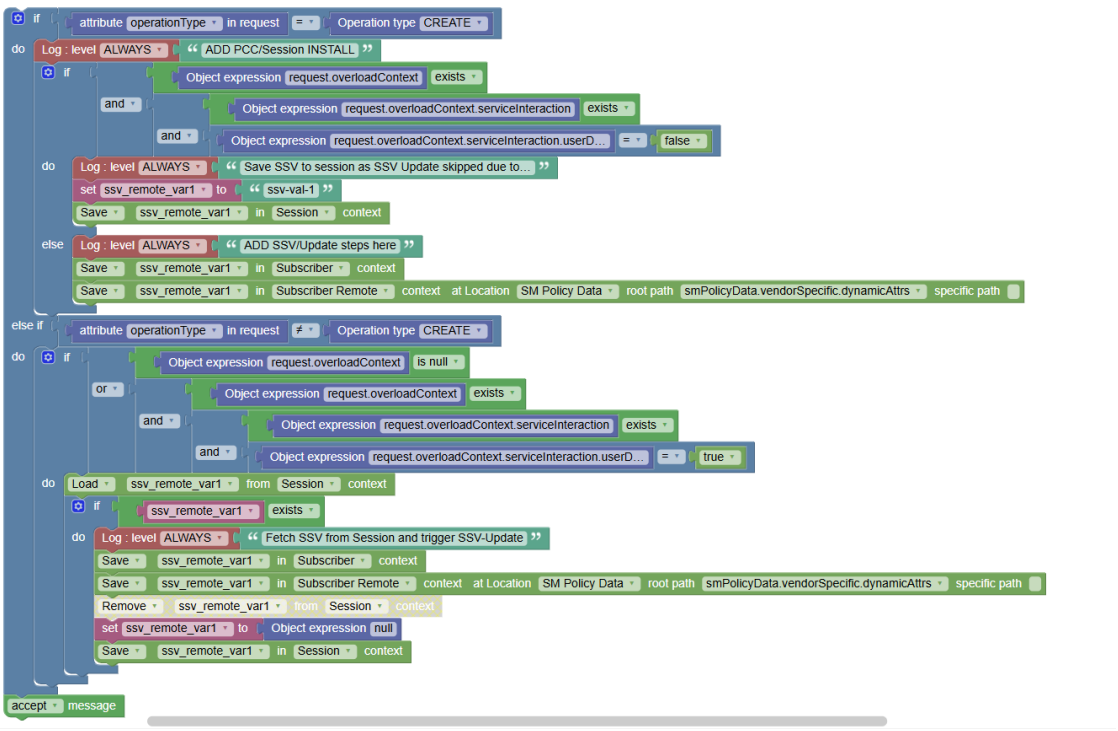
Publishing SM Overload level as a Custom Attribute in PRE for Policy Evaluation

In overload scenarios, subscriber updates may not be completed immediately during initial request handling due to Assume Positive restrictions being applied. The objective is to keep policy behavior consistent, prevent loss of update intent under constrained conditions, and ensure deferred data is synchronized when conditions permit. As a reference model, it helps operators design predictable state handling across CREATE and follow-up/update flows.

The following is a sample policy flow intended for reference and adaptation. It demonstrates how create and update SSV handling can be implemented using Overload context parameters available through object expressions.

> **Important**
>
> This example is not a strict requirement specification. It is a reusable reference pattern for implementation.

Figure 4-209 Sample Policy Project for Publishing SM Overload level as a Custom Attribute in PRE



- The sample evaluates request.operationType as the primary branching condition.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- In the CREATE branch, it checks for overload context for service interaction for user-data flag.
- If user data interaction is disabled (...userData... = false), it stores ‘ssv_remote_var1’ in Session context to defer update.
- Otherwise, it performs immediate update by saving ‘ssv_remote_var1’ to Subscriber and Subscriber-Remote contexts.
- In the next UPDATE flow, it loads deferred value from Session context and, if present, updates Subscriber and Subscriber-Remote contexts, clears Session value, and resets it to null.

Overload Rule Mapping

In case of overload rule selection priority, overload rule selection is driven by the overload rule ordering. When a request matches multiple message profile rules and those message IDs can match multiple overload rules, the selected overload rule is determined using the following precedence:

- Overload rule load level rules configured for the highest applicable load level are evaluated first.
- Overload rule priority within the selected load level, the rule with the lowest numerical *rulePriority* value has higher precedence.
- Message profile rule priority is considered only after overload rule load level and overload rule priority. Because, overload rule priorities are expected to be unique for each overload rule, message rule priority is not expected to influence the final overload action selection in normal configurations.
  That is, for a request matching multiple message IDs, the overload rule engine selects the overload rule based primarily on the configured overload severity (loadLevel) and overload rule priority, making the overload configuration the authoritative source for action precedence.

Table 4-154 Scope and Definitions for Applying Overload Actions

Item	Description
Load Level	L1 to L10 (L10 is highest).
Message Profile Attachment	One Message Profile is attached to the Overload configuration.
Message Profile Rules	Inside the attached Message Profile, rules (for example MP1, MP2) derive messageId from incoming message type (for example N7 Create/ Update/Delete).
messageId Usage	Derived messageId is used for overload rule matching.
Action Types	Reject and Assume Positive use the same selection flow.
Assume Positive Attributes	Service Interaction and Service Interaction Percentage.
Combined Rule Support	A single overload rule can contain both Reject Percentage and Service Interaction Percentage.
Percentage Constraint	Reject Percentage + Service Interaction Percentage <= 100.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-155 Overload rule Selection Procedure

Action	Result
Read current system load level.	Start evaluation at current level.
Find configured overload rules at that level.	If present, continue.
If multiple candidates remain at the identified level, compare Rule Priority (1 is highest precedence).	Lowest numeric value wins.
If no rules exist at current level, check lower levels one by one (L-1 to L1).	First lower level with rules is used. Rule Priority ordering applies if multiple rules are identified.
Use attached Message Profile to derive MessageId from incoming message via Message Profile rules (MP1.MP2,etc).	MessageId is available for matching.
Filter overload rules by MessageId match.	Candidate rule identified. MessageIds are ordered as per Message Profile rule priority. MessageID with highest rule priority will be searched first.
Apply selected rule action values.	Reject and/or Assume Positive applied per selected rule.

Figure 4-210 Overload rule selection and action

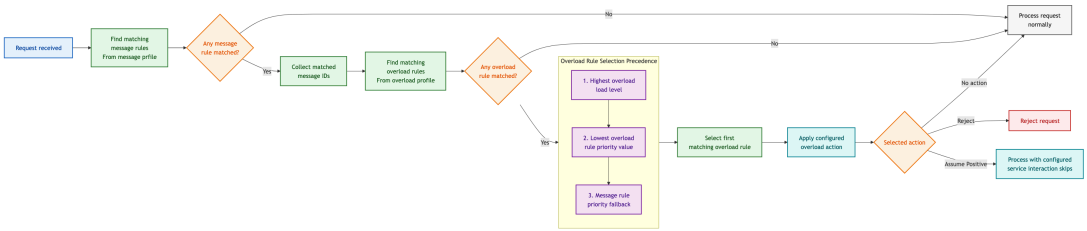


Table 4-156 Sample Message Profile Rule Mapping

Sample Message Profile Rule (used only for illustration purpose)	Incoming Message Pattern	MessageId
MP1	N7 Create for Internet DNN	sm_create_internet
MP2	N7 Create with any DNN	sm_create_any
MP3	N7 Update for Internet DNN	sm_update_internet
MP4	N7 Delete for any DNN	sm_delete_any

> **Note**
>
> Message profile Rule values (MP1, MP2, etc.) are for illustration only.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-157 Sample Expanded Decision Table (Illustrative Overload Rules)

Sample Rule Names (Used only for illustrative purpose)	Overload Level	Rule Priority	Message Id	Message Priority	Reject Percentage	Service Profile	Service Profile Apply Percentage	Validity Check (illustrative)
R1	L6	20	sm_create_internet	>= 7	40	SI_UDR_PRE	20	Valid (60)
R2	L6	10	sm_create_any	>= 5	25	SI_UDR_PRE	30	Valid (55)
R3	L6	15	sm_create_any	>= 6	10	SI_CHF_PRE	50	Valid (60)
R4	L6	30	sm_update_internet	>= 6	30	SI_PRE	40	Valid (70)
R5	L5	5	sm_create_any	>= 4	15	SI_ALL_SKIP	20	Valid (35)
R6	L6	40	sm_delete_any	>= 5	60	SI_NO_SKIP	50	**Invalid** (110 > 100)

> **Note**
>
> Rule Name values (R1, R2, etc.) are for illustration only. In the Overload Configuration GUI, rules are identified by configured fields.

Worked Example 1

Table 4-158 Rule Overlap Resolution

Input	Value
System Load Level	L6
Incoming Message	N7 Create (Internet)
Derived messageId (from Message Profile)	sm_create_internet, sm_create_any
Incoming Message Priority	8

Matching rules at L6: R1, R2, R3

Table 4-159 Rule priority comparison: R2 (10) wins over R3 (15) and R1 (20)

Selected Rule	R2
Reject Evaluation	Priority 8 >= 5, apply 25% reject
Assume Positive Evaluation	Apply SI_UDR_PRE with 30%
Constraint Check	25 + 30 = 55 (valid)

Worked Example 2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-160 Combined Percentages in One Rule

Rule	Value
Reject %	40
Service Interaction	SI_UDR_PRE
Service Interaction %	20

Table 4-161 Validation Results

Validation	Result
40 + 20 = 60	Valid (<= 100)

Behavior: 40% traffic handled by Reject action, 20% by Assume Positive (SI_UDR_PRE), remaining traffic follows normal handling as per product behavior.

Worked Example 3

Table 4-162 Invalid Configuration

Rule	Value
Reject %	60
Service Interaction %	50

Table 4-163 Validation Results

Validation	Result
60 + 50 = 110	**Invalid** (> 100)

Expected behavior: Rule must be rejected at configuration time (or not activated).

Worked Example 4

Table 4-164 Load-Level Fallback

Input	Value
System Load Level	L7
Rules at L7	**None**
Next Level Checked	L6
Incoming Message	N7 Create
Derived messageId (from Message Profile)	sm_create_internet, sm_create_any
Incoming Message Priority	6

At L6, matching candidates: R1, R2, R3; highest precedence is R2.

Table 4-165 Validation Results

Rule	Result
Selected Rule	R2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-165 (Cont.) Validation Results

Rule	Result
Reject Path	Eligible (6 >= 5), apply 25%
Assume Positive Path	Apply SI_UDR_PRE with 30%
Constraint Check	25 + 30 = 55 (valid)

Table 4-166 When multiple priority-based rules overlap, a request may match more than one rule

Scenario	Rule A: Condition	Rule A: Rule Priority	Rule B: Condition	Rule B: Rule Priority	Incoming Request Priority	Matched Rules	Selected Rule	Reason
Case 1: Normal precedence	priority >= 7	10	priority >= 15	20	17	Rule A and Rule B	**Rule A**	Both rules match; 10 < 20, so Rule A has higher precedence.
Case 2: Swapped precedence	priority >= 7	20	priority >= 15	10	17	Rule A and Rule B	**Rule B**	Both rules match; 10 < 20, so Rule B has higher precedence.

Table 4-167 Validation

Validation	Case 1	Case 2
Does request priority 17 satisfy Rule A (>= 7)?	Yes	Yes
Does request priority 17 satisfy Rule B (>= 15)?	Yes	Yes
Overlap detected?	Yes	Yes
Tie-break mechanism	Rule Priority	Rule Priority
Final applied rule	Rule A	Rule B

Rule Priority range: 1 to 65535 (1 is highest precedence).

If multiple rules match, the rule with the **lowest Rule Priority value** is applied.

4.94 Load Shedding through Admission Control in PCRF-Core

If you are using Policy 22.4.5 or any other later versions, Load Shedding through Admission Control in PCRF-Core is enabled by default.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The Admission Control enhancement in PCRF-Core performs message load shedding during congestion. Load Shedding through the Admission Control feature is enabled by default in the PCRF-Core. This enhancement enables PCRF-Core to monitor the message backlog. When the number of outstanding messages to be processed exceeds a certain threshold for a certain duration, Admission Control starts rejecting a subset of the messages that it receives.

The default behavior when a node is too busy is to:

- reject Gx CCR-I requests at L1 level of busyness.
- reject Gx CCR-I and Rx AAR-I requests at L2 level of busyness.
- reject all the requests at level L3.

This prevents corresponding sessions to be established, as such if the load is due to these applications, the node matches the backlog and switches to the “busy” state.

Load Shedding through Admission Control in PCRF-Core allows for the definition of up to three levels of busyness based on the amount of backlog: level 1, level 2, and level 3. Level 1 is the least busy level and level 3 is the busiest level.

> **Note**
>
> The node is busy whenever it is at any of the busy levels.

Another way to look at the different busy levels is by the amount of processing time the node needs to catch up with the backlog. The “catch-up” processing time will translate into increased response latencies. So, as the busy level increases, more drastic measures may need to be taken to attempt to clear the backlog and go back to normal response times.

The entrance criteria for a busy level are:

- The backlog of outstanding messages in a node crossed a pre-defined threshold for the level.
- The backlog has been above the busyness level’s threshold for a minimum amount of time.

The time portion is added as hysteresis to avoid too frequent level transitions. When the thresholds for multiple levels are crossed, the level of busyness is determined by the highest crossed threshold, as long as the time criteria is satisfied.

> **Note**
>
> A node could bypass levels of busyness if it crosses multiple thresholds. As an example, a node could go from not being busy to being at busy level 2.

The exit criteria from a busyness level are:

- The backlog of outstanding messages has been smaller than a pre-defined threshold for the level.
- The backlog has been below the busyness level’s threshold for a minimum amount of time.

At each level, allow for the following actions per Diameter application, message type and AVPs content:

- Reject with a specific result code (default is DIAMETER_TOO_BUSY)
- Drop

Copyright © 2019, 2026, Oracle and/or its affiliates.

For example, reject Gx CCR-I for APN X at level 1, reject Rx AAR-I message at level 2, and drop Gx CCR-U for APN Y at level 3.

The table below summarizes the default load shedding configuration values with which pcrf-core microservice is shipped with:

Table 4-168 Default Load Shedding Configuration

Busy Level	Entrance Threshold	Entrance Time Criterion (ms)	Exit Threshold	Exit Time Criterion (ms)	Actions
Level 1	300	300	150	500	• Reject Gx CCR-I with DIAMETER_TOO_BUSY • Accept CCR-I with DRMP=0 (Gx/CCR/CC-Request-Type=1 && DRMP=0)
Level 2	1000	300	600	500	• Reject Gx CCR-I with DIAMETER_TOO_BUSY • Reject Rx AAR-I with DIAMETER_TOO_BUSY • Accept CCR-I with DRMP=0 (Gx/CCR/CC-Request-Type=1 && DRMP=0)
Level 3	2000	300	1500	500	• DROP

For details on advanced configuration keys and values that are used for load shedding through admission control, see *PCRF-Core Configurations* section in *Cloud Native Core Policy Installation and Upgrade Guide*.

The following metric has been added in Diameter Gateway service for this feature:

- diameter_outstanding_msg_count

For more information, see Diameter Gateway Metrics.

> **Note**
>
> This metric can be used to create alerts as per the requirement.

4.95 Rate Limiting

With the support for rate limiting feature at Ingress Gateway, Ingress Gateway is expected to screen all configured routes and their respective rate limit configurations. Within the sampling period (configurable using REST APIs), Ingress Gateway calculates the rate for the required route along with the HTTP method. Then, it notifies the route level rate limiter rate about the

Copyright © 2019, 2026, Oracle and/or its affiliates.

calculated rate at the end of the sampling period. If the feature is enabled, any request with the sbi-priority header value greater than the configured value is discarded and Ingress Gateway returns the error response with configured errorCode.

> **Note**
>
> Ingress Gateway determines the number of messages to be silently dropped or rejected in the current sampling period on the basis of extra messages received in previous sampling period that are not rejected.

Managing Rate Limiting

Enable

Perform the following configurations to enable the rate limiting feature at Ingress Gateway:

- **CNC Console**: By default, this feature is disabled. To enable the rate limiting feature using CNC Console, set the **Enable Rate Limiting** parameter to `true` on the Rate Limiting Policy page.
- **REST API:** By default, this feature is disabled. To enable the rate limiting feature using REST API, set the `enabled` parameter to `true` in the following resource URI:

  Define rate limit: {apiRoot}/PCF/nf-common-component/v1/igw/routelevelratelimiting

  Define rate limit at route level: {apiRoot}/PCF/nf-common-component/v1/igw/routesconfiguration

  For more information, see the section Rate Limiting at Ingress Gateway in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

To configure the rate limiting policy, route level mapping, and error code profiles for rate limiting, you may use CNC Console as well as REST API.

- **Configure using CNC Console:** Perform the feature configurations on the Rate Limiting Policy, Route Level Mapping, and Error Code Profiles pages. For more information about the configurations, see Overload and Congestion Control Configurations.
- **Configure using REST API:** PCF provides the following REST API for configuring overload control feature on SBI interface:
  Define error code profiles: {apiRoot}/PCF/nf-common-component/v1/igw/errorcodeprofiles

  Define rate limit: {apiRoot}/PCF/nf-common-component/v1/igw/routelevelratelimiting

  Define rate limit at route level: {apiRoot}/PCF/nf-common-component/v1/igw/routesconfiguration

  You can perform the GET, PUT, or PATCH operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.96 Topology Hiding for Diameter Gateway

With the Topology Hiding feature, it is possible to do the following:

- Hide topology-related information in messages sent to external peers.
- Restore the topology-related information in messages from external peers.

Copyright © 2019, 2026, Oracle and/or its affiliates.

In Policy, the Diameter Gateway acts as a proxy for both incoming and outgoing diameter messages. Irrespective of the direction, request and response of diameter messages must include `Origin-Realm` and `Origin-Host` of diameter gateway on reaching external peers.

With Topology Hiding feature enabled, the Diameter Gateway verifies if the `Origin-Host` value in request or response from backend peers matches one of the managed backend peers, before sending to external peers. If yes, the value of `Origin-Host` is replaced with the Diameter Gateway identity in the message request and response. If the request or response is not for managed backend peers, no change is made to the `Origin-Host`.

Configure

To enable and configure this feature using CNC Console, the following parameters have been added under Diameter Configurations:

- **Topology Hiding**
- **Apps to Hide**

For more information about setting the parameter values, see Settings for Diameter Configurations.

Observe

Enabling the Topology Hiding feature replaces the Origin-Host dimension value with Diameter Gateway identity. It contains the value as per the message call-flow.

4.97 Two-phase Deployment of Policies

Policy allows you to configure and update the existing policies. However, updating or changing existing policies can impact existing traffic adversely. To overcome this challenge, Policy provides the two phase deployment model. This deployment model supports:

- Creation, modification, or deletion of policies, without impacting the existing policies.
- Testing of new policies with some percentage of live traffic before enabling it for 100% live traffic.

This feature allows you to create a policy project without deploying it. To implement this, Policy provides two possible states, **Prod** and **Dev** in the policy project.

By default, the **Dev** state is assigned to the policy project. Dev projects do not process any traffic in PRE (Policy Runtime Engine), where PRE is a pod. The Prod projects process traffic in PRE.

Managing Two-phase Deployment of Policies

Enable

The Two Phase deployment is a core functionality of Policy. You do not need to enable or disable this feature.

Configure

You can create new policy projects and update the existing projects using the CNC Console for Policy.

For more information about configuring Policy Projects, see Policy Projects.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.98 Binding Mechanism Support (Nbsf)

PCF Session Binding is used for AF to discover a PCF that contains the PDU session and communicates with that PCF for App session procedures.

The PCF interacts with BSF to maintain the PCF session binding information during the PDU session life cycle.

PCF implements service operations as a consumer defined in clause 4.2 of TS 29.521[11]:

- Nbsf_Management_Register Service Operation
- Nbsf_Management_Deregister Service Operation

PCF invokes Nbsf_Management_Register Service Operation to the BSF to create PCF session binding when creating SM Policy Association. PCF invokes Nbsf_Management_Deregister Service Operation and Nbsf_Management_Register Service Operation when modify SM Policy Association and the UE address information is changed.

The system considers BSF selection based on the IP range to invoke BSF operation.

The interaction with BSF is optional and can be configured in PCF SM Service configuration. For more information about these configurations, see PCF Session Management.

Managing Binding Mechanism Function

Enable

You can enable the Binding mechanism functionality using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** To enable the feature, set the **Binding Operation** parameter value to **TRUE** under the **Binding Configurations** group on the **PCF Session Management** page. For more information about enabling the feature through CNC Console, see PCF Session Management Service.
- **Enable using REST API:** Set the **bindingOperationEnabled** parameter value to **true** in the **Session Management Service** configuration API. For more information about enabling the feature through REST API, see "Session Management Service" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the Binding mechanism functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations under the **Binding Configurations** group on the **PCF Session Management** page. For more information about configuring the feature through CNC Console, see PCF Session Management Service.
- **Configure using REST API:** Policy provides the following REST API for Binding mechanism configuration:
  API: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm

  You can perform the PUT operation to configure the feature. For more information about REST API configuration, see Binding Configurations of the "Session Management Service" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observe

Copyright © 2019, 2026, Oracle and/or its affiliates.

Policy provides the Binding requests and response metrics in the Session Management services. For more information, see the Binding service metrics in SM Service Metrics.

4.99 LDAP Support

Policy establishes connections with data sources to retrieve information about subscribers from the database. It queries a data source using a key attribute that uniquely identifies a subscriber and stores the results in its cache. A data source uses this key attribute. For example, the phone or account number of the subscriber to index the information present in the database.

The Policy supports Lightweight Directory Access Protocol (LDAP) data source. It provides support for the following LDAP related functions:

- Configuring LDAP Server Information
- Providing support for LDAP server

Based on the conditions implemented in PCF system, Policy Data Source (PDS) retrieves all the relevant information from LDAP data source based on the rules configured in the system through LDAP gateway.

For information on configuring the LDAP server, see Data Source Configurations.

Managing LDAP

Enable

To enable the LDAP functionality, set value for the following parameter to true in the customer value file for Policy:

- **ldapGatewayEnable**

On setting the value for the aforementioned parameter to **true**, the Session Management (SM) or PCRF Core service routes the traffic to LDAP Gateway through PDS. For more information about setting the parameter values, see "Enabling/Disabling Services Configurations" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*

Configure

LDAP credentials are stored as kubernetes secret along with Authentication DN and LDAP name. You must create a Kubernetes secret to store LDAP credentials before setting a PDS as LDAP data source.

To create a kubernetes secret for storing LDAP credentials:

1. Create a yaml file with the following syntax:

```
apiVersion: v1
kind: Secret
metadata:
  name: ldapsecret
  labels:
    type: ocpm.secret.ldap
type: Opaque
stringData:
  name: ldap1
  password: camiant
  authDn: uid=PolicyServer,ou=customer1,c=hu,o=customer1
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

where, *name* is the configured LDAP server name.

password is the LDAP credential for that data source.

authDN is the authentication DN for that LDAP datasource.

> **Note**
>
> For LDAP data, more entries can be added in the above format with only the key of the entry specifying LDAP name in the Policy Graphical User Interface (GUI).

2. Create the kubernetes secret by executing the following command:

   ```
   kubectl apply -f yaml_file_name -n pcf-namespace
   ```

   where:

   yaml_file_name is a name of the yaml file that is created in Step 1.

   pcf-namespace is the deployment namespace used by the helm command.

Configure LDAP Server

If you are using LDAP for storing the user profiles, you must configure the LDAP server as the datasource. You can configure the LDAP server using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the configurations for LDAP on the **Data Sources** page. For information on configuring the LDAP server, see Data Sources.
- **Configure using REST API:** Policy provides the following REST API for LDAP Server configuration:
  API: {apiRoot}/oc-cnpolicy-configuration/v1/datasources/{datasourceName}

  You can perform the PUT operation to configure the feature. For more information about REST API configuration, see *Data Source* in *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide*.

After the configuration, you can use blockly action to retrieve resources from the LDAP datasource. For more information, see *PDS Category* in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Observe

Policy provides metrics and alerts specific to LDAP Service. For information related to LDAP Gateway metrics, see LDAP Gateway.

4.100 SOAP Support

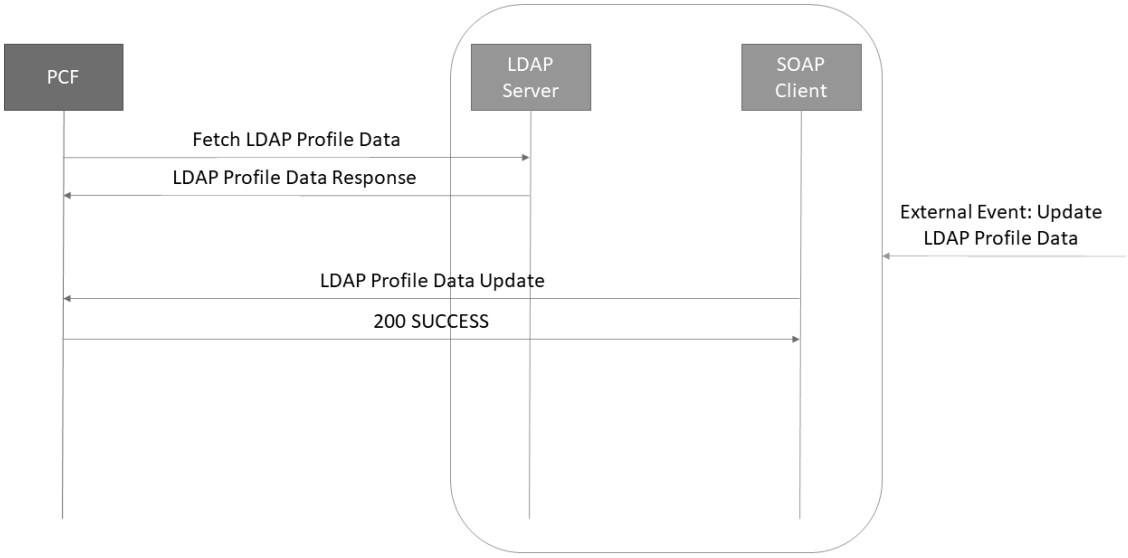
Policy establishes connections with data sources to retrieve information about subscribers from the database. It queries a data source using a key attribute that uniquely identifies a subscriber and stores the results in its cache. A data source uses this key attribute. For example, the phone or account number of the subscriber to index the information present in the database.

Policy uses the subscriber data to:

- evaluate policy
- define FUP objects
- billing reset mechanism

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-211 Fetching subscriber data



1. When Policy receives an SM Create request from SMF, it sends a request to the LDAP server to retrieve the subscriber profile.

   It uses IMSI, MSISDN, SUPI and GPSI to fetch the data.
2. Policy forwards the subscriber data received from LDAP server to PRE for evaluation.
3. Based on the outcome, Policy sends an SM Create response to SMF.

Further SM Create request, Policy processes the subscriber profile that is cached. If the subscriber profile data is not available, Policy triggers an LDAP read to update the cache. Based on the evaluation of policy, it sends an SM Create Response.

> **Note**
>
> SoapConnector service supports HTTP1.1 by default. SoapConnector service will respond with the error like "Invalid Frame or does not support HTTP2" if it receives force HTTP2 request without negotiation. To enable HTTP1.1, see the **Enabling HTTP1.1** section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

The Policy uses SOAP (1.2 version) data interface to access subscriber data from an external LDAP Source.

1. Policy receives a notification from a SOAP-XML feed when the profile is updated.

   The SOAP notification message contains the changed LDAP attributes only along with the Subscriber Identifier (IMSI/MSISDN) identifying the affected subscriber. The SOAP notification is expected when at least one subscriber session is active on Policy.
2. Policy processes the notification, uses the subscriber identifier available as part of the SOAP notification to trigger additional LDAP search request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. It updates the subscriber profile database, and triggers a policy re-evaluation. It uses IMSI, MSISDN, SUPI, or GPSI to process the notification.
4. It then acknowledges the notification with a 200 ok response and discards the inactive sessions.

Managing SOAP

To enable the SOAP support, set value of `global.soapConnectorEnable` parameter to `true` in the custom_values.yaml file.

For more information about setting the parameter values, see *Enabling/Disabling Services Configurations* in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

4.101 Support for Timer Configurations

Managing Timer Configurations

The timer profile sets request timeout values for UDR, CHF, BSF, and SMF messages in applications or interfaces. Policy applies the specific timeout profile while sending request to external NFs. The external NFs include UDR, CHF, BSF, and SMF. Policy updates the appropriate metrics in case of such request timeout.

In Policy, Ingress gateway applies operator configured interface specific timeout and use it as request timeout. It also propagate timeout value in `3gpp-Sbi-Max-Rsp-Time` header, so that it can be used by back-end services (if required).

Enable or Configure
When back-end service has to originate a message for producer or consumer NF, the following algorithm for applying request timeout value is used:

- When the corresponding timer profile is not associated for the originating service:
  - If incoming request contains `3gpp-Sbi-Max-Rsp-Time` header, then use the value specified in `3gpp-Sbi-Max-Rsp-Time` header as timeout. For more information about configuring this value, see SBI Timer Header.
  - If the incoming request does not contain the `3gpp-Sbi-Max-Rsp-Time` header, then configure the request timeout during deployment or configuration using CNC Console for Policy. For more information about configuring Timer Profile using CNC Console, see Timer Profiles.
- When the corresponding timer profile is associated for the originating service:
  - If incoming request contains `3gpp-Sbi-Max-Rsp-Time` header, then use the minimum of the values specified in `3gpp-Sbi-Max-Rsp-Time` header and service or default timeout from the profile. For more information about configuring this value, see SBI Timer Header.
- If incoming request does not contain the `3gpp-Sbi-Max-Rsp-Time` header,
  - Use service specific timeout, if configured in timeout profile
  - Otherwise use default timeout from the timeout profile

After the above operations, the originating service also set the timeout value in the `3gpp-Sbi-Max-Rsp-Time` header to propagate it for any further producer services. Egress Gateway applies the request timeout from the `3gpp-Sbi-Max-Rsp-Time` header and finally uses its blocklisted feature to remove this header from egress message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

SBI Timer Header

SBI Timer Headers are implemented at Ingress Gateway. These are taken into consideration while calculating request timeout for a route along with route level (if configured) and global level request timeout.

Enable

To enable the SBI Timer Header, set the **ingress-gateway.isSbiTimerEnabled** parameter to **true**, under the **ingress-gateway** configurations in the custom-value.yaml file for Policy.

If the **ingress-gateway.isSbiTimerEnabled** parameter is set to **true**, then

- `3gpp-Sbi-Sender-Timestamp`, `3gpp-Sbi-Max-Rsp-Time`, and `3gpp-Sbi-Origination- Timestamp` parameters are used along with route level and global level request timeout to calculate the final request timeout.
- After calculating the final request timeout, original values of the `3gpp-Sbi-Sender-Timestamp`, `3gpp-Sbi-Max-Rsp-Time`, and `3gpp-Sbi-Origination- Timestamp` parameters are published in the `Orig-3gpp-Sbi-Sender-Timestamp`, `Orig-3gpp-Sbi- Max-Rsp-Time`, and `Orig-3gpp-Sbi-Origination-Timestamp` respective custom headers.

If the **ingress-gateway.isSbiTimerEnabled** parameter is set to **false**, then the SBI headers are not taken into consideration even if, they are present and the custom headers are not published.

4.102 Custom AVP to Support Third-Party Vendor Specific AVPs

An Attribute-Value Pair (AVP) is used to encapsulate protocol-specific information supported by CNC Policy. Diameter messages such as RAA, CCA, CCR, and RAR and so on, are supported by third-party AVP policy conditions. The supported outgoing Diameter messages set or remove third-party AVPs.

Policy allows you to create policy conditions to evaluate the presence of both standard (base) and third-party AVPs in Diameter messages or group AVPs during policy execution. A policy condition can check for the presence of both standard and third-party AVPs in incoming Diameter messages and evaluate their values. A policy action can use standard and third-party AVPs for routing, authentication, authorization, and accounting. Standard AVPs can be included in third-party AVP conditions and actions. To include a standard (base) AVP in a nonstandard application message, or to use a pre-standard AVP as a standard AVP, define it as a custom AVP.

Standard AVPs can be included in third-party AVP conditions and actions. To include a standard (base) AVP in a nonstandard application message, or to use a pre-standard AVP as a standard AVP, you must define it as a Custom AVP. When defined, custom AVPs are located at the end of a parent Diameter message or group AVP. If the parent AVP is null, the custom AVP is inserted at the root level of the message.

For example, a custom AVP definition appears at the end of this Charging-Rule-Install message:

```
 Charging-Rule-Install ::= < AVP Header: 1001 >
*[ Charging-Rule-Definition ]
*[ Charging-Rule-Name ]
*[ Charging-Rule-Base-Name ]
[ Bearer-Identifier ]
[ Rule-Activation-Time ]
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
[ Rule-Deactivation-Time ]
[ Resource-Allocation-Notification ]
[ Charging-Correlation-Indicator ]
*[ customAVP ]
```

A Set or Get SPR user attribute value can be set to the defined third-party AVP in Diameter messages. You can also set or remove the defined third-party AVPs during the execution point.

A third-party AVP is identified by a unique identifier in the following format:

name:*vendorId*

For example:

Condition
where the request *AVP NEW_AVP3:555* value is numerically *equal to 2012*

Parameters
The AVP name and vendor ID. In the example, the vendor ID is 555.

Description
A well-defined AVP custom name is referred to if the vendor ID is not specified.

When entering and sending a new third-party AVP definition to CNC Policy, the definition must include the AVP name, code, vendor ID, data type, and an optional AVP parameter.

Validation of the AVP code, Name, and vendor ID prohibits a user from overwriting the existing base AVPs.

These AVP actions include the ability to perform the following:

- Routing
- Authentication
- Authorization
- Accounting

For more information about custom AVP, see Custom AVP.

Managing Support for Custom AVP

Enable

This is a core functionality of Policy. This feature remains enabled by default.

Configure

You can add and configure the Custom AVPs using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the configurations on the **Custom AVP** page. For more information about configuring PRAs, see Custom AVP.
- **Configure using REST API:** Policy provides the following REST API to create Custom AVPs:
  API: {apiRoot}/oc-cnpolicy-configuration/v1/policydata/common/customattributes/avp

  You can perform the POST, PUT, or GET operations to configure the Custom AVP. For more information about REST API configuration, see Custom AVP section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

After the configuration, you can use blockly actions to set values of Custom Values. For more information, see "PCRF-Core Actions" in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

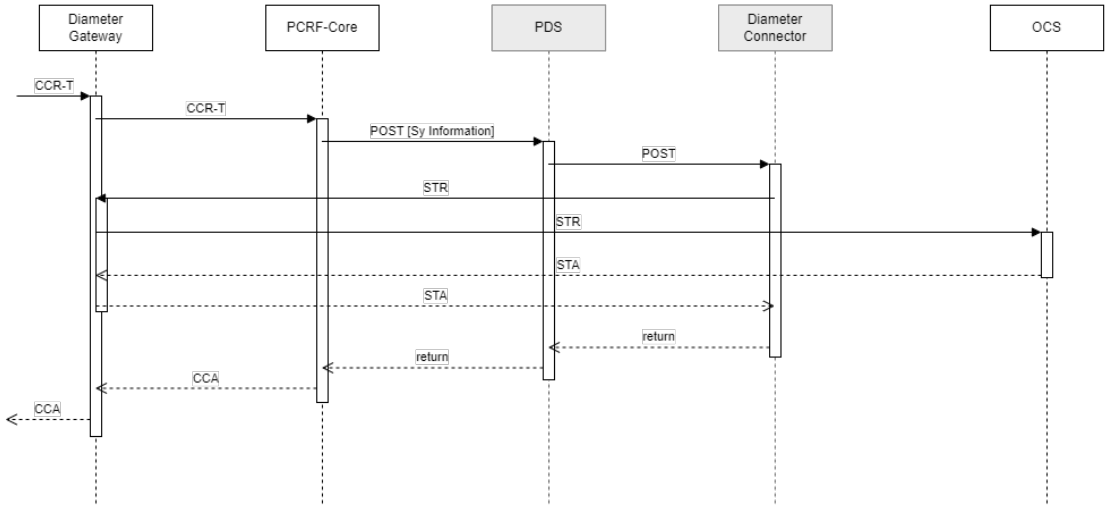
4.103 Adding Subscription-ID AVPs to STR messages

As part of the Final Spending Limit Report Request (SLR) procedure, PCRF sends a Session Termination Request (STR) to Online Charging System (OCS) through PDS and Diam-Connector to unsubscribe from all the Policy Counters belonging to the Diameter session and terminate the session.

OCS uses Subscription-ID AVPs to associate the STR with the SLR and close the session.

Without the Subscription-ID AVPs in STR, OCS returns a `DIAMETER_MISSING_AVP 5005` error to STRs.

Figure 4-212 Communicating STR messages



For this purpose, when PDS sends a GET request, the response header `oc-data-source-route-info` parameter from Diameter-Connector to PDS includes details such as `SubscriptionIdType` and `UserIds` used in SLR from Diameter-Connector.

This same header is used by the PDS in the subsequent OCS request including INTERMEDIATE and TERMINATE requests.

In case of a TERMINATE request, the Diameter-Connector receives the `oc-data-source-route-info` header from PDS. It extracts `SubscriptionIdType` and `UserIds` if `OCS_ENABLE_SUBS_ID_ON_STR` is set to `true`.

It then sends the Subscription-Id AVP in STR message.

Managing the Adding Subscription-ID AVPs to STR messages feature

Enable

You can enable addition of Subscription-Id information in Subscription-Id AVPs using `diam-connector.envSyEnableSubsIdOnSTR` Helm parameter during installation. For more information, see *Diameter Gateway and Diameter Connector Configuration* section in *Oracle*

Copyright © 2019, 2026, Oracle and/or its affiliates.

Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide.

Configure

You can configure addition of subscription-Ids using the `diam-connector.envSyEnableSubsIdOnSTR` Helm parameter during installation.

For more information, see *Diameter Gateway and Diameter Connector Configuration* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

4.104 Asynchronized Access to nCHF

The Policy solution supports asynchronized access of subscriber related information from data sources such as CHF.

Managing Asynchronized Access to nCHF

Enable

You can enable the Asynchronized Access to nCHF functionality using the CNC Console or REST API for Policy.

- Enable the **Enable Async CHF Query** parameter under the **User** group on the **PCF Session Management** page. For more information, see information about user configurations in PCF Session Management.
- **Enable using REST API:** Set the **enableChfQueryAll** parameter value to **true** in **User Configuration** of the **Session Management Service** API. For more information about enabling the feature through REST API, see "Session Management Service" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

After enabling this feature, you can perform the necessary configurations using the **Fetch Policy Counters from CHF** block for the SM service. Configure this block to fetch policy counters through asynchronous CHF lookup.

For more information about configuring the block, see "Public Category" in *Oracle Communications Cloud Native Core, Converged Policy Design Guide.*

4.105 Nudr to Support OperatorSpecificData

Policy supports custom JSON feature that allows you to configure flexible data schema as part of OperatorSpecificData for policy validation from Nudr interface and apply policies based on the data set. The advantages of this integration are:

- Uses new data type object for data not mapped to standardized fields
- Object contains IDs and map of Operator specific policy set objects (blobs)
  Blobs can be used to store Boolean, number, object, array, null, string <*JSON, XML, Base64 encoded binary data*>, and so on.
- Aligns with 3GPP

Managing Nudr Support for OperatorSpecificData

Enable

Copyright © 2019, 2026, Oracle and/or its affiliates.

You can enable the Nudr Support for OperatorSpecificData functionality using the CNC Console for Policy.

Enable the **Enable Operator Specific Data Query** parameter under the **User** group on the **PCF Session Management** page. For more information about enabling the feature through CNC Console, see PCF Session Management.

Configure
You can use the OperatorSpecificData as an input in different Policy Projects. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

4.106 Support for Spending Limit Pending Counter

The Policy solution enables you to use activation time in the pending policy counter as input to the Condition Data for either activation time or deactivation time. This functionality is available for condition data used by PCC rules and session rules.

> **Note**
>
> This functionality is only supported by Session Management (SM) Associations.

Example:

The following is a sample of Spending Limit Pending Counter:

```
{
 "supi": "imsi-450081100100001",
 "gpsi": "msisdn-9192503899",
 "PolicyCounterIds": [
 {
 "policyCounterId": "silver",
 "currentStatus": "valid",
 "penPolCounterStatuses": [
 {
 "policyCounterStatus": "start",
 "activationTime": "2020-05-16T16:25:00.659Z"
 }
 ]
 },
 {
 "policyCounterId": "gold",
 "currentStatus": "valid",
 "penPolCounterStatuses": [
 {
 "policyCounterStatus": "start",
 "activationTime": "2020-01-01T00:00:00.000Z"
 },
 {
 "policyCounterStatus": "end",
 "activationTime": "2020-12-31T23:59:59.000Z"
 }
 ]
 }
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
 ]
}
```

In the above sample, PCF selects one of the policy counters by `policyCounterId` and `policyCounterStatus`. After this, PCF uses the `activationTime` as the activation time or deactivation time for the condition data of PCC Rule or Session Rule, and finally sends the related PCC Rule or Session Rule to SMF.

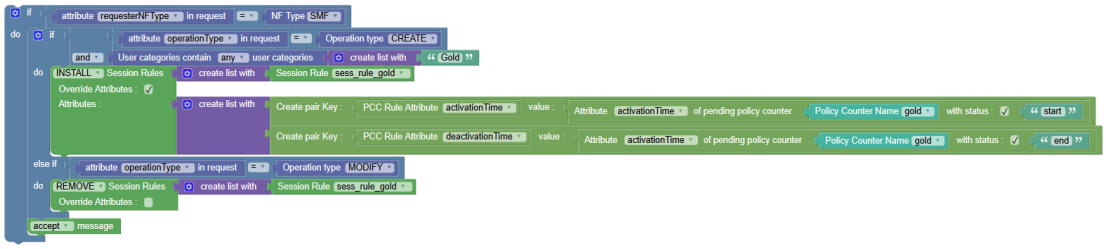
The existing policies support the spending limit pending counter functionality. You can perform the following configurations:

- Select the activationTime of pending counter by policyCounterId and policyCounterStatus.
- Install PCC Rule or Apply PCC Rule Profile using the activationTime as activationTime or/and deactivationTime of Condition Data of the PCC Rule or PCC Rule Profile.
- Install/Modify Session Rule using the activationTime as activationTime or/and deactivationTime of Condition Data of the Session Rule

For more information on Activation/Deactivation Time of PCC Rules/Session Rules blockly design for policy design, see **PCF-SM Category** section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

A Policy Sample, this sample is used to install session rule using policy pending counter from the above sample.

Installing Session Rule Using Policy Pending Counter



Managing Spending Limit Pending Counter Support

Enable
This feature remains enabled by default.

Configure
You can configure the Spending Limit Pending Counter functionality by configuring the following SM service functions:

- **Policy Counter ID**: Perform the Policy Counter Id configurations on the **Policy Counter ID** page. For more information, see Policy Counter Id,
- **Condition Data**: Perform the Condition Data configurations on the **Condition Data** page. For more information, see Condition Data.
- **PCC Rule**: Perform the PCC Rule configurations on the **PCC Rule** page. For more information, see PCC Rule.
- **Session Rule**: Perform the Session Rule configurations on the **Session Rule** page. For more information, see Session Rule.

Copyright © 2019, 2026, Oracle and/or its affiliates.

After the above configurations, you can use blockly action to install session rule/PCC rule using policy pending counter . For more information, see "PCF-SM Category" in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

4.107 XFCC Header Validation

Overview

With XFCC Header Validation feature, Policy (PCF) as a producer, checks if the SCP that is sending the HTTP request is the same SCP that is configured in the PCF. Policy performs this check by comparing the FQDN of the SCP present in the “x-forwarded-client-cert” (XFCC) of http2 header with the list of FQDN of the SCPs configured in the PCF. This configured list contains all the host FQDNs resolved successfully via DNS-SRV as well as static SCPs. The header validation can be enabled at global as well as at the route level.

> **Note**
>
> This feature is applicable only when SCP is deployed in the network topology.

XFCC header validation applies to all the interfaces of Policy (PCF), which support indirect communication through SCP. The list of the interfaces is as follows:

- AMF, SMF, and AF SBI service requests and responses
- UDR, CHF, and NRF notification messages

Configuring SCPs at Policy

To configure SCP, you need to customize `custom-values.yaml` at the time of deploying Policy.

In the earlier releases, users could only configure SCPs statically as shown in the following snippet:

```
xfccHeaderValidation:
    validation:

      enabled: false
      nfList:
        - scp.com
        - smf.com
        - amf.com
```

Starting Policy release 22.1.0, you can configure single or multiple virtual FQDNs for the SCP along with the static configuration as shown in the following snippet:

```
global:
    xfccHeaderValidation:
      validation:
        enabled: false
        peerList:
          - name: scp.com
          - name: smf.com
          - name: amf.com
          - name: scp1.com
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    enabled: true
  - name: scp2.com
  - name: scp3.com
    enabled: false
  - name: xyz.test.com
    enabled: true
    scheme: http
    type: virtual
  - name: abc.test.com
    enabled: true
    scheme: https
    type: virtual
  - name: xfcc.test.com
    enabled: false
    scheme: http
    type: virtual
```

Static SCP: To define an SCP instance statically, add the name and set enabled parameter to true in the peerList. If the enabled parameter is set to false for an instance, then it is not included in the list of configured FQDNs. If you do not specify enabled parameter then by default it is considered as true.

Virtual SCP: To define an SCP with virtual FQDN, add the name, scheme as http or https, type as virtual, and set enabled parameter to true. If the enabled parameter is set to false for an instance, then it is not included in the list of configured FQDNs.

Resolving FQDNs to find Authorized SCPs for Policy

During the bootup of Ingress Gateway, it tries to resolve the configured virtual FQDN via Alternate Route service using the following helm configuration:

```
dnsSrv:
    port: *svcAlternateRouteServiceHttp #Alternate-route port for scheme
'http'. Change is required if the scheme below changes.
    scheme: http
```

If Alternate Route service is unable to resolve the configured virtual host, Ingress Gateway stores it in the list of failed FQDNs and reattempts the request at 300 s (default value configured for **dnsResolutionInterval**).

The following metric is used when the request to resolve configured virtual FQDNs is unsuccessful:

- `oc_ingressgateway_dns_resolution`: This metric is pegged when DNS resolution for a given FQDN fails.
- `oc_ingressgateway_dns_resolution_failure`: This is a gauge metric that is triggered when DNS resolution for a given FQDN fails.

Handling Traffic Flow

The specification for the XFCC header validation of an incoming request with the FQDN's of SCP configured at the IGW are as follows:

1. When a request is received at IGW, it gets forwarded to the back-end micro-service based on the configured rules.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. The **ingress-gateway.xfccHeaderValidation.validation.matchField** parameter configured in IGW remains available in the client certificate field of XFCC header. You must validate this parameter with the configured FQDNs of SCP.
3. If multiple XFCC headers are present in the incoming request to IGW, then the IGW validates the **ingress-gateway.xfccHeaderValidation.validation.matchField** parameter present in each XFCC header against the configured FQDNs of SCP, until a match is found.

There are following scenarios to handle the XFCC header present in the incoming request to IGW:

- Validation of single XFCC header present in the incoming request to IGW
- Validation of multiple XFCC headers present in the incoming request to IGW

Validating single XFCC Header
The following figure describes the call flow for validation of single XFCC header:

Figure 4-213 Call Flow Validating single XFCC Header

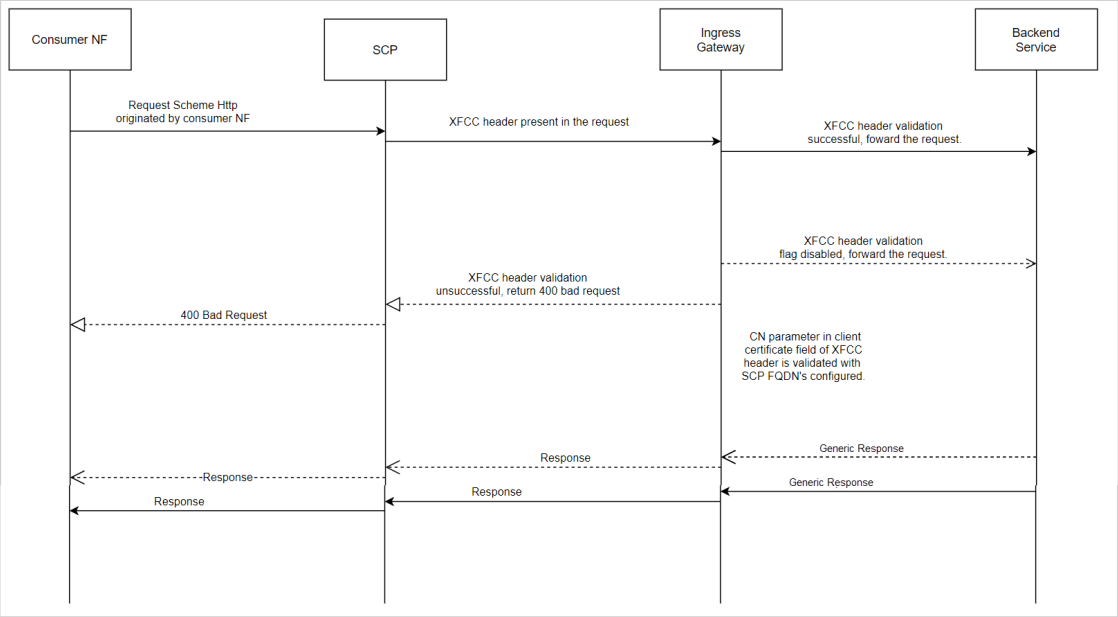


Table 4-169 Single XFCC Header Configuration

Prerequisite	Condition	Steps
Given XFCC Header validation parameter is enabled for the corresponding route match and matchCerts count correctly configured.	If the matchField parameter of client certificate field in XFCC header matches with one of the FQDNs of SCP configured.	Forward the request to back-end microservice and receive a corresponding response.
Given XFCC header validation parameter is enabled for the corresponding route match and matchCerts count correctly configured.	If matchField parameter of client certificate field in XFCC header does not match with the FQDNs of SCP configured.	Return 400 Bad Request response from Ingress Gateway.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-169 (Cont.) Single XFCC Header Configuration

Prerequisite	Condition	Steps
Given XFCC header validation parameter is not enabled for the corresponding route match.	The matchfield parameter is not considered.	Forward the request to the back-end microservice and receive a corresponding response.

Example of XFCC Header:

```
x-forwarded-client-cert: By=http://
router1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8de68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=Test Client"; URI=http://
testenv1.blr.com;DNS=blr.com; DNS=www.blr.com
```

Validating multiple XFCC Headers

The following figure describes the call flow for validation of multiple XFCC header:

Figure 4-214 Call Flow Validating Multiple XFCC Headers

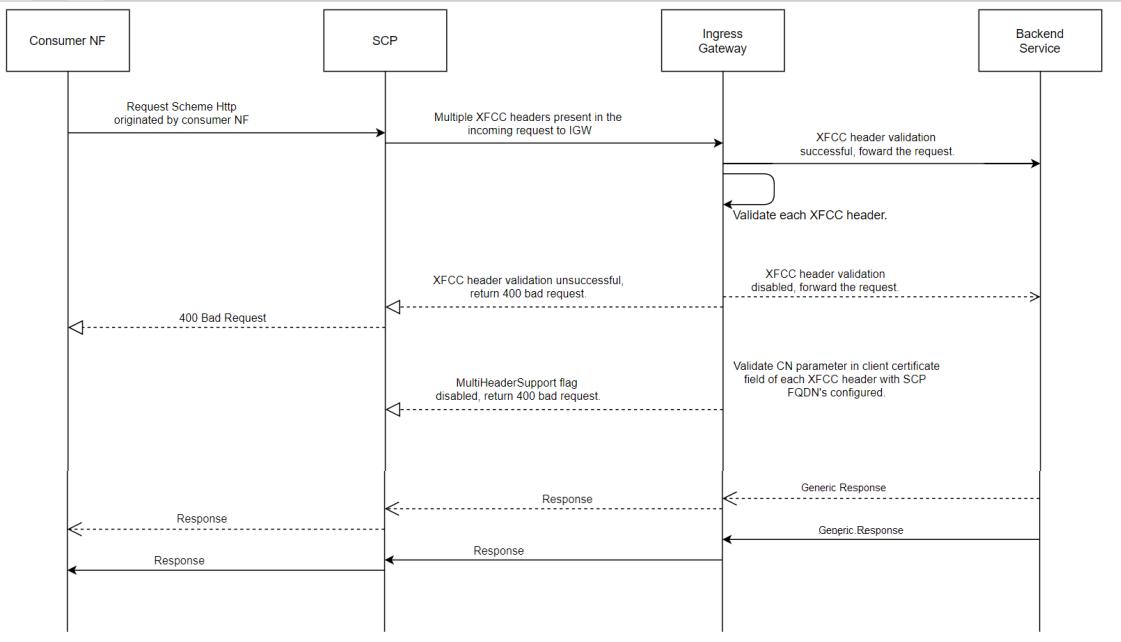


Table 4-170 Multiple XFCC Headers Configuration

Prerequisite	Condition	Steps
Given XFCC header validation parameter is enabled and matchCerts count correctly configured to validate across XFCC header certificates from the right most entry.	If matchField parameter of the corresponding client certificate field being validated against currently in the corresponding XFCC header matches with the FQDNs of SCP configured at Ingress Gateway.	Consider the request as a valid request and forward the request to the back-end micro-service and receive a corresponding response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-170 (Cont.) Multiple XFCC Headers Configuration

Prerequisite	Condition	Steps
Given XFCC header validation parameter is enabled and matchCerts count correctly configured to validate across XFCC header certificates from the right most entry.	If matchField parameter of client certificate field in corresponding XFCC headers do not match with the FQDNs of SCP configured at Ingress Gateway for the corresponding matchCerts count.	Consider the request as an invalid request and return a 400 Bad Request response from IGW. For more information about error codes, see SBI Ingress Error Code Profiles Collection.
Given XFCC header validation parameter is enabled and matchCerts count -1.	The virtual fqdns should get resolved with the help of ARS.	Consider the request as valid request and match against the corresponding match field in all XFCC headers, if validation successful then forward the request else return 400 BAD Request.
Given XFCC header validation parameter is not enabled.	Behaves normally.	Forward the request to back-end microservice and receive a corresponding response.

Example of XFCC Header:

```
x-forwarded-client-cert:By=http://
router1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8d
e68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=nf1.com"; URI=http://
testenv1.blr.com; DNS=nf8.com; DNS=nf1.com; DNS=nf6.com, By=http://
router1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8d
e68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=nf10.com"; URI=http://
testenv1.blr.com; DNS=nf10.com; DNS=nf8.com; DNS=nf9.com, By=http://
routexr1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8
de68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=nf4.com"; URI=http://
testenv1.blr.com; DNS=nf9.com; DNS=nf4.com;DNS=nf1.com
```

Managing XFCC Header Validation

Enable

- **Global Level**: To enable or disable the XFCC header validation feature, set the value of the `ingress-gateway.global.xfccHeaderValidation.validation.enabled` to true or false respectively.
- **Route Level**: To enable or disable the XFCC header validation feature at route level, set the value of the `xfccHeaderValidation.validationEnabled` under routesConfig to true or false respectively.

> **Note**
>
> If the `xfccHeaderValidation.validationEnabled` parameter is defined at route level, then the configuration takes precedence over global configuration.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For instance, if you want to enable XFCC header validation for selected routes, then set the global parameter as false and make route specific configuration to true.

```
global:
    xfccHeaderValidation:
      validation:
        enabled: false


routesConfig:
    - id: sm_create_session_route
      uri: http://{{ .Release.Name }}-occnp-pcf-sm:
{{ .Values.global.servicePorts.pcfSmServiceHttp }}
      path: /npcf-smpolicycontrol/*/sm-policies
      order: 1
      method: POST
      readBodyForLog: true
      filters:
        subLog: true,CREATE,SM
      metadata:
        xfccHeaderValidation:
          validationEnabled: true
```

For more information about setting the parameter values, see "XFCC Header Validation Configuration" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

Configure

You can configure the various parameters related to XFCC Header Validation feature in the `custom-values.yaml`. For more information, see "XFCC Header Validation Configuration" section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

Observe

The XFCC Header Validation feature can be observed using the metrics specific to Ingress Gateway. For information related to Ingress Gateway metrics, see Ingress Gateway Metrics.

Configuring Error Codes

When the XFCC header validation feature is enabled and SCP FQDN in the incoming header does not match the configured FQDN in PCF, XFCC header is not present, or XFCC header is invalid, then PCF may return error in the response. Users have the ability to customize the error code returned in the response using the following helm configuration:

```
errorTrigger:
          - exceptionType: XFCC_HEADER_INVALID
            errorCode: '401'
            errorCause: xfcc header is invalid
            errorTitle: 'Invalid XFCC Header'
            errorDescription: 'Invalid XFCC Header'
          - exceptionType: XFCC_MATCHCERTCOUNT_GREATER_THAN_CERTS_IN_HEADER
            errorCode: '402'
            errorCause: matchCerts count is greater than the certs in the
request
            errorTitle: ''
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    errorDescription: ''
  - exceptionType: XFCC_HEADER_NOT_PRESENT_OR_EMPTY
    errorCode: '403'
    errorCause: xfcc header is not present or empty in the request
    errorTitle: ''
    errorDescription: ''
```

If the configured error code in the errorCodeOnValidationFailure field lies in 3xx error series only then the values for retryAfter and redirectUrl if configured under XFCC Header Validation Configuration at Ingress Gateway are used to populate Retry-After and LOCATION headers correspondingly while sending error response from Ingress Gateway.

4.108 Policy Event Records

The Policy Event Records feature enables you to view transaction related information that includes input data set, policies that were evaluated, and resulting policy actions from any transactions. Policy event records provides an insight on the policy flow, conditions that are executed, and policy actions enforced by the Policy solution. Single record is generated including the following information:

- Transaction and input Data input set
- Executed policies
- Flow of the executed policies
- Executed instructions or rules
- Policy results and actions

The format of this data is in accordance with the JSON format.

Following are the attributes of the JSON schema:

- policyStartTime
- policyRequest
- policyExecution
- policyEndTime
- policyResponse

Sample Schema:

```
{
    "policyStartTime": "2021-09-14T09:00:37.261Z",
    "policyRequest": {
      "request": {
        "requestType": "SMF",
        "operationType": "CREATE"
      }
    },
    "policyExecution": "[\" Start evaluating policy
main\",\"utils.getAttributeVal(['request.request.operationType'], request) ==
'CREATE' evaluates to be true\",\" INSTALL  Session Rules
     ['sessionRule2']\",\" End evaluating policy main\"]",
    "policyEndTime": "2021-09-14T09:00:37.262Z",
    "policyResponse": {
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    "actions": [],
    "customAttributeActions": [],
    "variables": {},
    "ruleActions": [
      {
        "actionType": "INSTALL",
        "ruleType": "SESSION_RULE",
        "sessionRule": [
          {
            "sessRuleId": "sessionRule2"
          }
        ]
      }
    ]
  }
}
```

For more information on configuration parameters related to policy event records, see General Settings section.

4.109 URSP Policy Support

With this enhancement, you should be able to define URSP policy in PCF and deliver the policy to UE. UE Route Selection Policy (URSP) is used by the UE to determine how to route outgoing traffic. Traffic can be routed to an established PDU Session, can be offloaded to non-3GPP access outside a PDU Session, or can trigger the establishment of a new PDU Session.

- UE policy service should be able to establish UE Policy Association requested by the NF service consumer
- UE policy service should be able to define and deliver URSP message to UE via AMF using N1N2 message

For more information about configuring URSP, see URSP Rule.

Managing URSP

Enable

This is a core functionality of Policy. It remains enabled by default.

Configure

You can configure the URSP Rules using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations on the **URSP Rule** page. For more information on configuring the feature through CNC Console, see URSP Rule.
- **Configure using REST API:** Policy provides the following REST API for URSP configuration:
  API: {apiRoot}/oc-cnpolicy-configuration/v1/policydata/pcfue/ursps

  You can perform the POST and PUT operation to configure the feature. For more information on REST API configuration, see "URSP" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observe

Copyright © 2019, 2026, Oracle and/or its affiliates.

Policy provides the UE service metrics for observing all the features related to the service. For more information, see the UE Service metrics in UE Service Metrics.

4.110 AF Integration over Rx

Rx interface handling supports the following:

- Diameter session management (creation, modification and deletion)
- Session association and trigger policies on N7 interface with PCC rules
- Compliant with 29.214 V15.1.0
- Integration with BSF for session binding management
- Integration with UDR for updating policyInfo and SM policy association

4.111 IMS Emergency Session Support

This feature allows a caller to contact local CNC Policy Emergency services, such as Police, Fire department, or ambulance for assistance. To ensure uninterrupted services, separate Data Network Names (DNNs) are defined to support the emergency services sessions. The subscription related information is not relevant for such sessions.

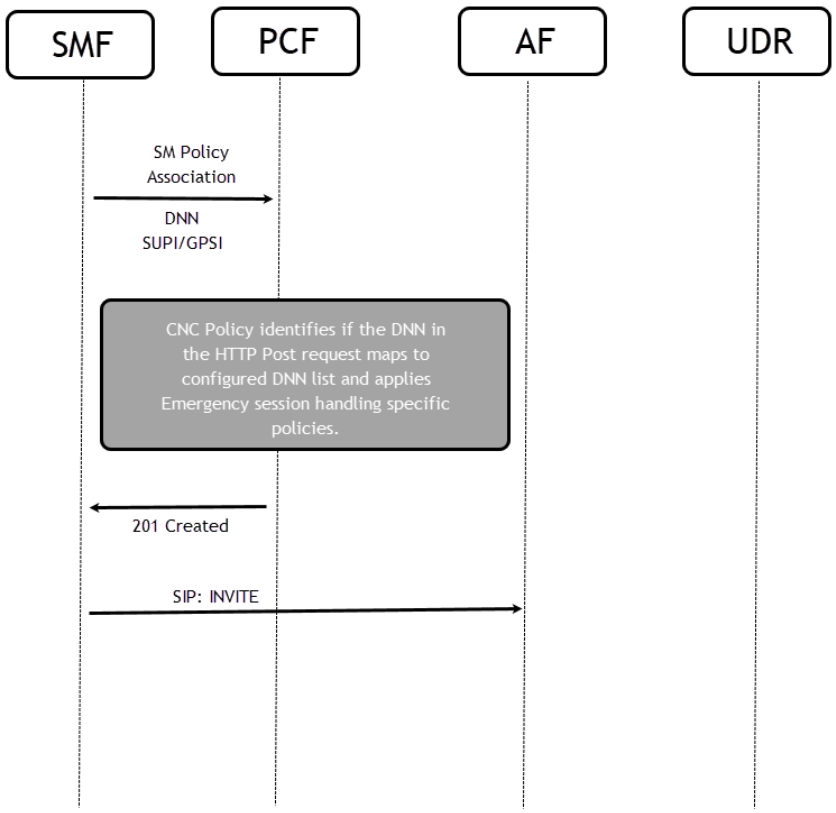
The IMS Emergency Support provides the following capabilities:

- All the devices, with or without SIM can trigger an emergency session and provided access to the emergency services
- The local operator policies are applied for QoS determination

The following figure describes the call flow for the Emergency Session handling in Policy:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-215 Call Flow - IMS Emergency



- SMF sends an HTTP POST message for establishing SM Policy Association and the "dnn" attribute including the Emergency DNN. The SMF includes the SUPI within the "supi" attribute and the GPSI if available within the "gpsi" attribute.
- The PCF detects that the PDU session is restricted to IMS Emergency services when the HTTP POST message is received and the "dnn" attribute includes a data network identifier that matches one of the Emergency DNs from the configurable list.
- Then, suitable PCC Rules are applied restricting the access to Emergency Services in a response message.

> **Note**
>
> Policy does not support the IMS restoration for emergency sessions.

Managing IMS Emergency

Enable

This feature remains enabled by default.

Configure

Copyright © 2019, 2026, Oracle and/or its affiliates.

You can configure the IMS Emergency functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:**
  - To configure emergency DNN which allows for N7 request to be successful without MSISDN or IMSI, perform the feature configurations under the **IMS Emergency Session** group on the **PCF Session Management** page. For more information, see PCF Session Management Service.
  - To configure emergency DNN for Rx calls, perform the feature configurations under the **IMS Emergency Session** group on the **PCF Policy Authorization** page. For more information, see PCF Policy Authorization.
- **Configure using REST API:** Policy provides the following REST API for Binding mechanism configuration:
  - To configure emergency DNN which allows for N7 request to be successful without MSISDN or IMSI:
    API: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfsm

    You can perform the PUT operation to configure the feature. For more information on REST API configuration, see **IMS Emergency Session Configuration** of the "Session Management Service" in *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide*.
  - To configure emergency DNN for Rx calls:
    API: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfpa

    You can perform the PUT operation to configure the feature. For more information on REST API configuration, see **IMS Emergency Session Configuration** of the "Policy Authorization Service" in *Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide*.

After the configuration, you can use the blockly actions for IMS Emergency related action. For more information, see "IMS Emergency Session Support" in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Observe

Policy provides metrics and alerts specific to SM service and Policy Authorization service.

For information related to SM service metrics, see SM Service Metrics.

For information related to Policy Authorization service metrics, see PA Service Metrics.

4.112 IMS Restoration

Policy supports restoring an IMS network as defined in 3GPP TS 29.212V15.4.0.

Also, it supports enhancements to the restoration procedure as defined in 3GPP TS 29.214V15.4.0.

> **Note**
>
> This feature is applicable only for PCRF flows in Converged mode of deployment.

The automatic restoration procedure involves:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. If AF provisions information about the AF signaling flows between the UE and the AF, PCRF installs the corresponding dynamic PCC rules by triggering a RAR message.
2. The PCRF provides the Charging-Rule-Install AVP including the Charging-Rule-Definition AVP(s).

   The Charging-Rule-Definition AVPs include:

   - the flow-Information AVP, the signaling flows between UE and the AF.
   - AF-SignallingProtocol AVP set to the value corresponding to the signaling protocol used between the UE and the AF.
3. PCRF shares the AF address with PCEF.
4. PCEF:
   a. Responds to PCEF with a RAA message.
   b. Initiates the corresponding bearer procedure if required.
   c. Extracts the AF address from the PCC rules.
   d. Checks if the monitoring procedure must be started for the corresponding AF.
   e. Starts the monitoring procedure as defined for the different access types.

In case AF de-provisions the information about the AF signaling flows between the UE and the AF, as defined in 3GPP TS 29.214 [10] Section 4.4.5a:

1. PCRF removes the corresponding dynamic PCC rules by triggering a RAR message.
2. PCRF sends the Charging-Rule-Remove AVP including the corresponding Charging-RuleName AVP(s) to PCEF.
3. PCEF uses the AF address associated with the removed rule to check if it can stop monitoring the corresponding AF.
4. PCEF acknowledges by sending a RAA command to the PCRF.

In case of P-CSCF restoration enhancement,

1. PCRF receives a request for P-CSCF restoration from the P-CSCF.
2. PCRF sends a Gx RAR command including the PCSCF-Restoration-Indication AVP set to value 0 (PCSCF_RESTORATION) to the PCEF for the corresponding Gx session.
3. PCEF acknowledges the RAR command by sending an RAA command to the PCRF and initiates the corresponding bearer procedure for the IMS PDN connection as defined in 3GPP TS 23.380 [33].

4.113 Automated Test Suite Support

Policy provides Automated Test Suite (ATS) for validating different functionalities. ATS allows you to execute Policy test cases using an automated testing tool, and then compares the actual results with the expected or predicted results. In this process, there is no intervention from the user is required. For more information, see *Oracle Communications Cloud Native Core, ATS User Guide*.

4.114 Notification Handling from PDS for PCRF-Core

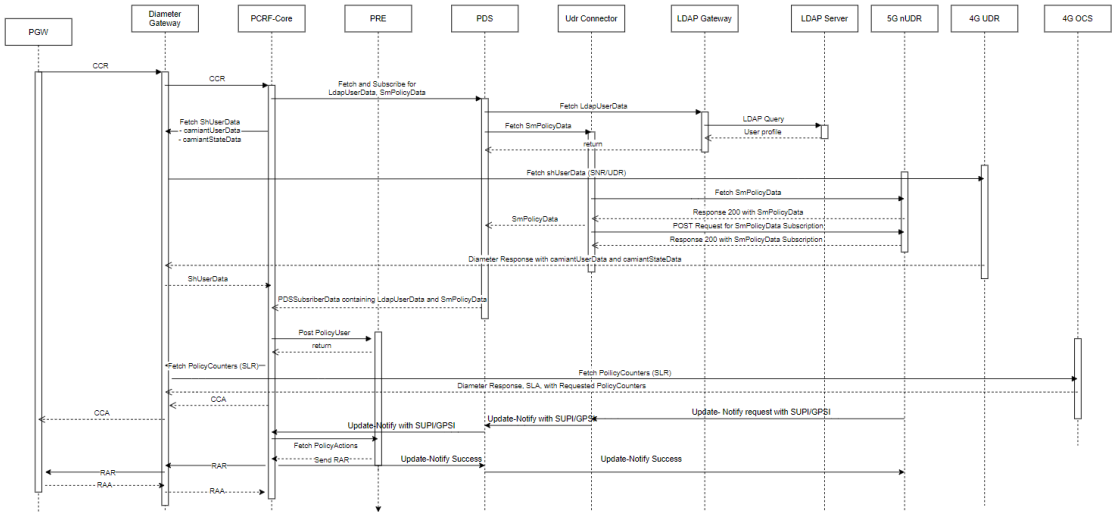
In earlier releases, PCRF-Core could communicate with 4G UDR and OCS (Sy interface) through Diameter Gateway. PCRF-Core could communicate with LDAP through PDS. With the

Copyright © 2019, 2026, Oracle and/or its affiliates.

latest enhancements, PCRF-Core can now communicate with 5G nUDR through PDS to fetch SmPolicyData.

As illustrated in the following call flow diagram, when PCRF-Core receives notify request with SUPI or GPSI from PDS for smPolicyData, that is, from nUDR - PCRF-Core initiates reauthorization request, and populates PolicyUser structure. Then, it sends the evaluation request to PRE. PRE further evaluates policy based on the new structure received. If installed rules or any of its related fields are different from the PRE Evaluation result, then PCRF-Core triggers a RAR request towards PGW.

Figure 4-216 Call flow for notification handling from PDS for PCRF-Core



Enable

To enable this feature, set the values for the following fields to **true**, on Settings page:

- **SmPolicyData** (Enable)
- **Subscribe to Notify** (SmPolicyData Attributes)

4.115 Service mesh for intra-NF Communication

Policy leverages the Istio or Envoy service mesh (Aspen Service Mesh) for all internal and external communication. The service mesh integration provides inter-NF communication and allows API gateway co-working with service mesh. The service mesh integration supports the services by deploying a special sidecar proxy in the environment to intercept all network communication between microservices.

The Aspen Service Mesh (ASM) configurations are classified into:

- **Control Plane**: It involves adding labels or annotations to inject sidecar.
- **Data Plane**: It helps in traffic management like handling NF call flows by adding Service Entries (SE), Destination Rules (DR), Envoy Filters (EF) and other resource changes like apiVersion change between versions. This is done manually depending on each NF requirement and ASM deployment.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing Service mesh for intra-NF Communication

Enable

To enable Aspen Service Mesh, configure the following parameters under **nrf-client-nfdiscovery**, **ingress-gateway**, **egress-gateway**, and **alternate-route** sections in the custom values file for Policy:

- serviceMeshCheck
- istioSidecarQuitUrl
- istioSidecarReadyUrl

For more information on enabling the parameter value, see "Aspen Service Mesh Configurations" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*

Configure
The Aspen Service Mesh (ASM) configurations are classified into:

- **Control Plane**: For information on configuring the parameter values, see "Aspen Service Mesh Configurations" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*
- **Data Plane**: For information about Data plane configurations, see "Aspen Service Mesh Data Plane Configurations" in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*

4.116 Turning off AccessToken signature Validation

OAuth access tokens are used to grant an NF service consumer access to the services of an NF producer of a particular NFType for a specific period of time. With this feature, Policy has the capability to turn off AccessToken signature validation at the application layer. For instance, when service mesh, for example Aspen service mesh, is integrated with Policy, the service mesh may perform the AccessToken validation. In such cases, operator may want Policy to skip validating AccessToken signature. It checks audience and scope fields only, and send 403 - Forbidden response when any of the values do not match. In addition, when Policy receives a request without AccessToken, it sends a 401 - Unauthorized response code.

Configure

To turn of AccessToken signature validation at PCF application, the user must perform configurations that are described in the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*.

4.117 Pending Transactions on N7 and N15 Interface

Policy Charging and Control (PCC) services, such as Npcf_SMPolicyControl, Npcf_AMPolicyControl service, etc. allow the NF producer to update a given policy association in the following two ways:

1. **Unsolicited** – In the unsolicited method, NF producer provides updates to the NF consumer using UpdateNotify service operation. For instance, if PCF is a NF producer that needs to notify SMF (NF consumer) about a policy association in an unsolicited manner, then PCF initiates UpdateNotify service operation for Npcf_SMPolicyControl service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. **Solicited** – In the solicited method, NF producer sends a response on receiving a request from the NF consumer. For instance, PCF installs policy decisions on receiving Npcf_SMPolicyControl_Update service request from SMF.

As the request can be initiated by either consumer or producer network function, a situation may arise when requests to modify the same policy are initiated concurrently. Additionally, if an HTTP proxy say Service Communication Proxy (SCP) is deployed for communication between network functions, the messages may get delivered out of order thereby resulting in wrong information maintained for a policy association by NF producer and NF consumer.

Feature Negotiation

Once the feature has been enabled, feature negotiation needs to happen between SMF and PCF during Npcf_SMPolicyControl_Create service operation. As defined by the 3GPP feature negotiation mechanism, the following conditions must be met for SMF and PCF to agree upon the Pending transactions feature:

- NF consumer or SMF advertises "PendingTransaction" feature within the attribute supportedFeatures (suppFeat) when sending a request to create SM policy association.
- In turn, PCF advertises the same value for the supportedFeatures (suppFeat) while sending the response for the policy association create request.

Enable

By default, this feature is not configured on the Policy deployment. You can opt to configure the Pending Transactions on N7 and N15 interface using the CNC Console or REST API.

On PCF Session Management and PCF Access and Mobility page, under Service Configurations, select `PendingTransaction` from the drop-down menu of **Override Supported Features** parameter. For more information about the configurations, see PCF Session Management.

Using the REST APIs for Session Management Service, you can enable the feature by updating the value as `PendingTransaction` for the following parameter under the `system` group:

```
overrideSupportedFeatures": [
      "PendingTransaction"
    ],
```

Configure

Perform the configurations for the pending transactions on N7 and N15 features using the CNC Console or REST API:

Perform the feature configurations on the PCF Session Management page. For more information about the configurations, see PCF Session Management.

Using the REST APIs for Session Management Service, you can configure the feature by updating the values of parameters under the `pendingTransaction` group:

```
pendingTransaction": {
    "updateNotifyRetryBackoff": 1000,
    "updateNotifyRetryCount": 2
  },
```

No helm configurations are required for this feature.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observe

The existing Ingress and Egress Gateway metrics have been enhanced for this feature.

- ocpm_ingress_request_total
- ocpm_ingress_response_total
- ocpm_egress_request_total
- ocpm_egress_response_total

The following metrics have been added for this feature.

- occnp_http_in_conn_response_total
- occnp_http_in_conn_request_total
- http_bulwark_lock_request_total
- http_bulwark_unlock_request_total
- http_bulwark_lock_response_total
- http_bulwark_lock_request_retry_total
- http_bulwark_unlock_request_retry_total
- occnp_http_ue_request_total
- occnp_http_ue_response_total

No new alerts are introduced for this feature.

Maintain

Logs are generated when the system returns with a 400 error message for a pending transaction. The following is a sample log for SM update-notify request in case of Pending Transaction:


```
{
  "instant": {
    "epochSecond": 1633660911,
    "nanoOfSecond": 292427900
  },
  "thread": "boundedElastic-4",
  "level": "DEBUG",
  "loggerName": "ocpm.pcf.service.sm.domain.component.SmfManager",
  "message": "is400BadRequestWithPendingTransaction: true",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 166,
  "threadPriority": 5,
  "messageTimestamp": "2021-10-07T22:41:51.292-0400"
}
```


The following is a sample log when lock is acquired for SM update request:


```
{
  "instant": {
    "epochSecond": 1633660909,
    "nanoOfSecond": 626486627
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
  },
  "thread": "PartitionedCacheWorker:0x0000:15",
  "level": "DEBUG",
  "loggerName": "ocpm.common.bulwark.repository.processor.LockProcessor",
  "message": "Lock is acquired for a key: bf87d498-0849-42f3-86ff-
d015a97b5721 with value: {\"lockID\":\"bb666052-270a-4e0a-
b4a5-017852c86fe3\",\"ttl\":3000,\"serviceInfo\":
{\"serviceName\":\"serviceId\",\"serviceID\":\"serviceName\"}}",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 41,
  "threadPriority": 5,
  "messageTimestamp": "2021-10-08T02:41:49.626+0000"
}
```


4.118 Pending Transactions on Gx Interface

Pending transaction functionality handles race condition and retry logic for Gx messages (CCR-U and RAR).

Feature Negotiation

Once the feature has been enabled, feature negotiation needs to happen between PGW and PCRF during CCR-I operation. As defined by the 3GPP feature negotiation mechanism, the following conditions must be met for PGW and PCRF to agree upon the Pending transactions feature:

- NF consumer or PGW advertises "PendingTransaction" feature within supportedFeatures (AVP) when sending a request to create PCRF.
- In turn, PCRF advertises the same value for the supportedFeatures (AVP) while sending the response for the PGW as a CCA-I message.

Enable and Configure

By default, this feature is not configured on the Policy deployment. You can enable and configure the Pending Transactions on Gx interface using the CNC Console and REST API.

You can configure the pending transaction configurations under **Pending Transaction** section in **Settings** page for **PCRF Core** on Oracle Communications Cloud Native Core, Cloud Native Configuration Console (CNC Console). For more details, see Settings.

Using the REST APIs for Session Management Service, you can configure the feature by updating the values of parameters under the pendingTransaction group:

```
{
    "pendingTransaction": {
        "enabled": true,
        "rarRetryBackoff": "800",
        "rarRetryCount": "2",
        "userNotifyReauthErrorHandling": 1,
        "afReauthErrorHandling": 1,
        "reauthErrorHandling": 1,
        "waitGxUpdateBeforeRejectDuration": 0,
        "skipPolicyEvaluationOnReauthRetry": true
    }
}
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see "PCRF Core Service" section in Oracle Communications Cloud Native Core, Converged Policy REST API Specification Guide.

> **Note**
>
> In Rx interface sync mode, the diameter configuration response timeout must be configured till the retry exhausts. The response timeout is calculated as *Retry Backoff* multiplied by *Retry Count*. The *response timeout* must be updated in the CNC Console.
>
> When the pending transactions on Gx interface feature is disabled and there is an error in the Gx RAA triggered by Rx interface in sync mode, then the AAA is not accepted as the message could not re-authenticate the primary session.

Observe

The following metrics have been added or enhanced for this feature:

- occnp_app_request_local_process_total
- occnp_app_response_local_process_total
- occnp_diam_response_local_total

For more information, see PCRF Core Metrics.

4.119 NRF Client Retry and Health Check

With the alternate route retry feature, Policy can attempt service requests to an alternate secondary Network Repository Function (NRF) when the primary NRF throws errors. In addition, the health status check feature actively monitors the health of the NRFs and provides the list of the healthy NRFs for session requests only. The NRF client also provides the health information of NRFs to other services if requested, and notifies any change in the health status.

For a given service request, the NRF client initiates a request towards a healthy and the highest priority NRF. If the NRF client receives a failure response for the request or the request timed-out, it attempts to send the request to the same NRF for `NrfRetryConfig.primaryNrfRetryCount` number of times. If a success response is received before the retry count gets exhausted, NRF client accepts the response and does not send any further service requests. However, if NRF client fails to receive a success response, it attempts to send the service request to an alternate NRF. The alternate NRF is selected based on the assigned priority and health status.

If the NRF Client receives a `retryAfterTime` value in the response header from the NRF, the NRF Client halts any further attempts to the NRF and flags the NRF as unhealthy for the specified time period. The NRF client retries the service request to alternate NRFs until any one of the following conditions are met:

- NRF-client receives a success response.
- NrfRetryConfig.alternateNRFRetryCount is exhausted.
- All attempts to available healthy NRFs are exhausted.

Once any of the listed conditions are met, NRF-client accepts the response and proceeds.

NRF Client marks NRF as unhealthy under the following conditions:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- If the NRF Client receives a *retryAfterTime* value in the response header from the NRF, then NRF will be unhealthy for a time period as defined in *retryAfterTime*.
- If the status code received is available in the default values for *errorCodeReasonsForFailure*, then NRF will be unhealthy for a period of time as defined in `ConfigMap.data: profile.retryAfterTime`.
- If the status code received is available in the default values for *errorCodeReasonsForFailure* and all the retry attempts are exhausted.
- If NRF Client receives an error from Gateway service and the error is configured in the *gatewayErrorCodes* with all the exhausted retry attempts.

Note

- If NRF Client receives an error from Gateway service and the error is not configured in the *gatewayErrorCodes*, then NRF remains marked as healthy.
- *HealthCheckConfig* and *NRFRetryConfig* must be configured for the NRF Client functionality to work as expected.
- NRF Client considers a response as failure only when it is configured in the `errorReasonsForFailure` parameter in the custom-values.yaml file. The primary and non-primary NRFs must be geo-redundant for the NRF Retry mechanism to work.
- For autonomous procedures such as NfRegistration, NfHeartbeat, NfStatusSubscribe (BSF, CHF, and UDR), and NfDiscovery, NRF-client continues to retry sending service requests till a success response is received.
  For details on NRF Client configuration parameters, see *NRF Client Configuration* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide.*

4.120 Support for PCF Status on NRF on CNC Console

Policy provides a consolidated status of the PCT registered with NRF.

The **NRF Status** is available under **Discovered NF Instances** section in **Status and Query** page on CNC Console.

Under **Discovered NF Instances** page, you can also view the health status of primary and secondary NRFs, or alternate NRF.

This feature is available for Converged and PCF only deployment modes.

To view the status using CNC Console, see NF Data.

4.121 Support for Stale Binding Detection in BSF

To support BSF to query PCF for suspected stale binding records, the Binding service has been made mandatory in the PCF mode of deployment. In BSF, whenever a binding record is detected as stale on the expiry of its binding age, BSF may send a query to PCF to confirm its status. To support this query to PCF, PCF is first required to send the **Vendor-Specific-Attribute** containing PCF Notification URL in the Binding Register request. When PCF sends the **Vendor-Specific-Attribute** in the register request, it is also required to provide the vendorID.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure this support, the following two new parameters are added to the Binding Service configurations page:

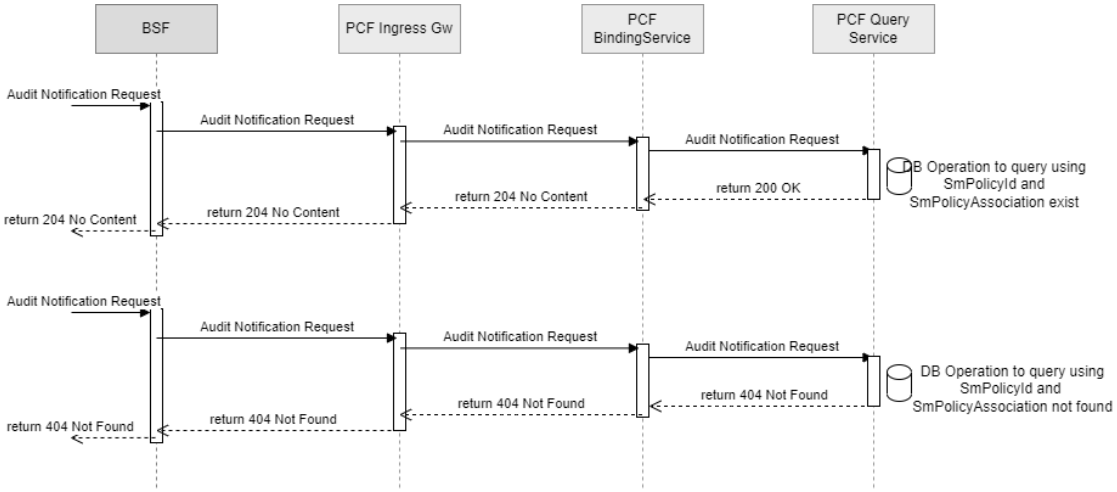
- Enable Vendor-Specific-Attribute In Register Request
- VendorId

Considering that the support for stale binding detection in BSF is enabled, the following diagram describes the call flow between BSF ad PCF. BSF on receiving an Audit notification request, sends the Audit Notification request to PCF Binding Service via Ingress Gateway. Then, Binding Service sends a request to the PCF Query Service to check if the ContextId (SmPolicyAssociation) exists. If it exists, PCF Binding service responds with 200 OK.

If the ContextId (SmPolicyAssociation) does not exist, Query service sends 404 Not Found to Binding Service. Then, Binding service returns the same response to BSF.

In case Policy is unable to process the Audit Notification request due to any failures, then it returns the 500 Internal Server error response to BSF.

Figure 4-217 BSF and PCF Interaction for Stale Binding Detection



Based on the system configurations, Policy supports receiving `3gpp-Sbi-Binding` header in the Audit Notification requests from BSF. Then, it updates the record in its database and send the updated `3gpp-Sbi-Binding` header in the response for Audit Notification request.

Metrics

The following metrics are implemented for this feature:

- occnp_binding_query_request_count
- occnp_binding_query_response_count

Logs

Policy generates logs for request and response messages from BSF including the VSA attribute. In addition, it generates logs for audit notifications requests and responses sent for it.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.122 Pod Protection at Ingress Gateway Using Rate Limiting

This section describes how to protect the Ingress Gateway(IGW) pods when they are overloaded with numerous incoming requests.

The Ingress Gateway pods are not protected against any incoming traffic congestion. As a result, the pods are overloaded and congested. This impacts system latency and performance. It also leads to stability issues due to uneven distribution of connections and traffic on Ingress Gateway pods. As a front end microservice for HTTP traffic, it is important for Ingress Gateway to have pod protection implemented.

Policy supports configuring Rate Limiting for Ingress Gateway service in order to provide pod protection by throttling inbound requests, if they are above configured rate. From release 25.2.200, Policy supports congestion control and message priority capabilities also for Ingress Gateway in order to provide pod protection.

Policy 25.2.200 integrates below functionalities for IGW:
Request Limiting and Precedence:

IGW must be able to limit (allow or deny) signaling requests to prevent exceeding its default capacity, with decision-making based on HTTP Method or Path, and assigned priority.

Non-Rejection Under Capacity:

IGW should not reject requests—regardless of HTTP Method, Path, or Priority—if capacity is not exceeded.

Priority Determination:

IGW must determine request Priority using specified information elements through configuration.

Control Over Denied Requests:

IGW needs the ability to control actions for denied requests (reject, drop, or process) based on Priority and its own congestion status.

Congestion Status Assessment:

IGW must determine congestion status using CPU utilization, with support for hysteresis to avoid rapid status changes.

Observability:

IGW must generate observability data to track and analyze request rate limiting for pod protection.

> **Note**
>
> Only HELM configuration mode is supported for this feature.

Managing Pod Protection at Ingress Gateway

Enable

Pod protection using rate limiting can be enabled by configuring the value of `podProtectionByRateLimiting.enable` Helm parameter to `true`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information, see *Basic Configurations in Ingress Gateway* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*

Configure

Pod protection at Ingress Gateway is configured using Helm parameters at the time of installation.

Pod protection by rate limiting can be configured using `podProtectionByRateLimiting` Helm parameter.

For more information, see *Basic Configurations in Ingress Gateway* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Here is a sample configuration for SM traffic. This configuration is to be added in **ingress-gateway** section of *custom-values.yaml* file.

```
# Mode of operation for routeConfigMode. Possible values are HELM, REST
  routeConfigMode: HELM

  # If set to true then existing routes configured in helm will be converted
to json and inserted in database. Default value is false.
  convertHelmRoutesToREST: false

  #ingress-gateway pod protection by rate limiting
  podProtectionByRLConfigMode: HELM
  podProtectionByRateLimiting:
    enabled: false
    fillRate: 3000                                # indicates tokens to be
added in 1000 ms
    bucketAllocation: 150                         # defines the bucket size
as percentage of fillRate
    routes: []
#      - id: 1
#        routeId: "sm_create_session_route"          # Reference to
routesConfig.id
#        percentage: 15                             # fillRate for this
route in % of the aggregateFillRate
#      - id: 2
#        routeId: "sm_delete_session_route"          # Reference to
routesConfig.id
#        percentage: 15
    errorCodeProfile: ERR_429                     # Reference to
errorCodeProfiles[].name

    priorityHeaderName: 3gpp-Sbi-Message-Priority # name of the header to use
for priority.
    defaultPriority: 24                           # Default message priority
to be used in absence of priority header.

    # Actions to be performed for denied requests based on SBI Message
Priority and Pod Local Congestion Level
    deniedRequestActions:
      - id: 1
        congestionLevel: 0
        action: CONTINUE
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
        - id: 2
          congestionLevel: 1
          action: CONTINUE
        - id: 3
          congestionLevel: 2
          priority: 0-18
          action: CONTINUE
        - id: 4
          congestionLevel: 3
          priority: 0-16
          action: CONTINUE
        - id: 5
          congestionLevel: 4
          priority: 0-10
          action: CONTINUE
        - id: 6
          congestionLevel: 4
          priority: 11-31
          action: REJECT
          errorCodeProfile: ERR_503

    congestionConfigMode: HELM
    congestionConfig:
      refreshInterval: 500
      levels:
        - value: 1                                  # default is 0 that is not
configurable, 1 -10 allowed
          name: DANGER_OF_CONGESTION
          resources:
            - name: CPU                             # only CPU supported by apigw
for the release
              onset: 60
              abatement: 55
        - value: 2
          name: CONGESTION_L1
          resources:
            - name: CPU
              onset: 70
              abatement: 65
        - value: 3
          name: CONGESTION_L2
          resources:
            - name: CPU
              onset: 80
              abatement: 75
        - value: 4
          name: CONGESTED
          resources:
            - name: CPU
              onset: 90
              abatement: 85
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> If the above congestion level is not configured, then the defaults would be considered and all the requests (accepted and denied ones) would be rejected (REJECT in action).

Here is a sample configuration for AM/UE traffic. This configuration is to be added in **ingress-gateway** section of *custom-values.yaml* file.

```
# Mode of operation for routeConfigMode. Possible values are HELM, REST
  routeConfigMode: HELM

  # If set to true then existing routes configured in helm will be converted
to json and inserted in database. Default value is false.
  convertHelmRoutesToREST: false

  #ingress-gateway pod protection by rate limiting
  podProtectionByRLConfigMode: HELM
  podProtectionByRateLimiting:
    enabled: false
    fillRate: 3000                                  # indicates tokens to
be added in 1000 ms
    bucketAllocation: 150                           # defines the bucket
size as percentage of fillRate
    routes: []
#      - id: 1
#        routeId: "am_create_session_route"         # Reference to
routesConfig.id
#        percentage: 20                             # fillRate for this
route in % of the aggregateFillRate
#      - id: 2
#        routeId: "am_delete_session_route"         # Reference to
routesConfig.id
#        percentage: 20
#      - id: 3
#        routeId: "ue_create_session_route"         # Reference to
routesConfig.id
#        percentage: 20
#      - id: 4
#        routeId: "ue_delete_session_route"         # Reference to
routesConfig.id
#        percentage: 20
#      - id: 5
#        routeId: "n1_message_notify"               # Reference to
routesConfig.id
#        percentage: 5
    errorCodeProfile: ERR_429                       # Reference to
errorCodeProfiles[].name

    priorityHeaderName: 3gpp-Sbi-Message-Priority   # name of the header
to use for priority.
    defaultPriority: 24                             # Default message
priority to be used in absence of priority header.
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
    # Actions to be performed for denied requests based on SBI Message
Priority and Pod Local Congestion Level

    deniedRequestActions:
      - id: 1
        congestionLevel: 0
        action: CONTINUE
      - id: 2
        congestionLevel: 1
        action: CONTINUE
      - id: 3
        congestionLevel: 2
        priority: 0-18
        action: CONTINUE
      - id: 4
        congestionLevel: 3
        priority: 0-16
        action: CONTINUE
      - id: 5
        congestionLevel: 4
        priority: 0-10
        action: CONTINUE
      - id: 6
        congestionLevel: 4
        priority: 11-31
        action: REJECT
        errorCodeProfile: ERR_503

  congestionConfigMode: HELM
  congestionConfig:
    refreshInterval: 500
    levels:
      - value: 1                                          # default is 0 that is
not configurable, 1 -10 allowed
        name: DANGER_OF_CONGESTION
        resources:
          - name: CPU                                     # only CPU supported
by apigw for the release
            onset: 60
            abatement: 55
      - value: 2
        name: CONGESTION_L1
        resources:
          - name: CPU
            onset: 70
            abatement: 65
      - value: 3
        name: CONGESTION_L2
        resources:
          - name: CPU
            onset: 80
            abatement: 75
      - value: 4
        name: CONGESTED
        resources:
          - name: CPU
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
onset: 90
abatement: 85
```

Observability

Alerts

The following alerts are added for this feature:

- `POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST` For more information, see POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST.
- `IGW_POD_PROTECTION_DOC_STATE` For more information, see IGW_POD_PROTECTION_DOC_STATE.
- `IGW_POD_PROTECTION_CONGESTED_STATE` For more information, see IGW_POD_PROTECTION_CONGESTED_STATE.

4.123 Support for Concurrency Handling using Bulwark Service in Policy

Policy supports the Bulwark service to handle the concurrent requests coming from other Policy services. Bulwark Service provides lock and unlock mechanism over a SUPI or GPSI key and allows only one notification at a time to proceed.

The Policy Services sends the following parameters to request a lock:

- **Key:** The key is the identifier value with which the lock is identified. You can select either SUPI or GPSI value to be the key parameter for which the lock acquisition request must be made. By default, SUPI values are used for lock requests.
- **Lease Duration:** This value defines the duration for which lock is kept once the acquisition is successful. After this duration, the lock will be released automatically.

> **Note**
>
> If the Lease Duration is shorter than the request processing time, then there could be chance of conflict and concurrency handling may not work.

> **Note**
>
> The maximum and minimum configured value of Lease Duration has been fixed by Engineering as 15000 ms and 10 ms respectively. If the given Lease Duration value is higher than the maximum configured value, then it is overwritten to 15000 ms. If the given Lease Duration is lower than the minimum configured value, then it is overwritten to 10 ms.

- **Lock Wait Timeout:** This defines the duration by which the Policy services wait for the response to get a lock. The same duration is used by Bulwark to poll for the lock in case the lock is not available. The Lock Wait timeout is also considered as the polling interval which sends the request towards Bulwark service periodically to acquire the lock for another create or delete request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Retry Count:** This defines the count of retry attempts that are made by the Policy services if a lock request fails. In case all the retry attempts fail, the create or delete request is rejected. By default, 3 retry attempts are enabled.

4.123.1 Support for Concurrency Handling using Bulwark Service in SM

The Bulwark Service integrates with the SM service to handle the concurrent requests for the SM Create, SM Update, SM Delete, SM Update-Notify, and SM Clean procedures. The SM service integration with Bulwark service handles the concurrent requests for the same subscriber in a concurrent and efficient manner.

In case of multiple create, update, delete, or clean requests for the same subscriber, the SM service requests a lock for the SUPI or GPSI value from the Bulwark service. Once the lock is acquired, the SM create, SM Update, SM delete, SM Update-Notify, or SM Clean request is executed for the SUPI or GPSI value with which the lock is requested. After the successful completion of the requests, the SM service sends a request to release the lock to Bulwark.

As the notification is locked, pending transaction comes into picture.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and SM Update:

Table 4-171 Pending Transaction and Concurrency in SM Update

Pending Transaction	Concurrency in SM Update	Use-Case
Enabled	Disabled	Single Key - Session level lock will be acquired. Pending-transaction call flow would work.
Disabled	Enabled	Single Key - Subscriber level lock will be acquired. Update-Notify call flow with concurrency would work.
Enabled	Enabled	Multi-Key - Session Level & Subscriber Level locks will be acquired.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and update-notify:

Table 4-172 Pending Transaction and Concurrency in SM Update-Notify

Pending Transaction	Concurrency in Update-Notify	Use-Case
Enabled	Disabled	Single Key - Session level lock will be acquired. Pending-transaction call flow would work.
Disabled	Enabled	Single Key - Subscriber level lock will be acquired. SM-Update call flow would work.
Enabled	Enabled	Multi-Key - Session Level & Subscriber Level locks will be acquired.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and SM Update and SM update-notify:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-173 Pending Transaction and Concurrency in SM Update as well as SM Update-Notify

Pending Transaction	Concurrency in SM Update	Concurrency in SM Update-Notify	Use-Case
Enabled	Disabled	Disabled	Session Level Lock Acquired - during collision, lock acquisition fails at SessionID
Disabled	Enabled	Disabled	Subscriber Level lock acquired - during collision, lock acquisition fails at subscriberID
Disabled	Enabled	Enabled	Subscriber Level lock acquired - during collision, lock acquisition fails at subscriberID
Enabled	Enabled	Disabled	Session Level & Subscriber Level locks will be acquired - during collision, lock acquisition will fail at SessionID

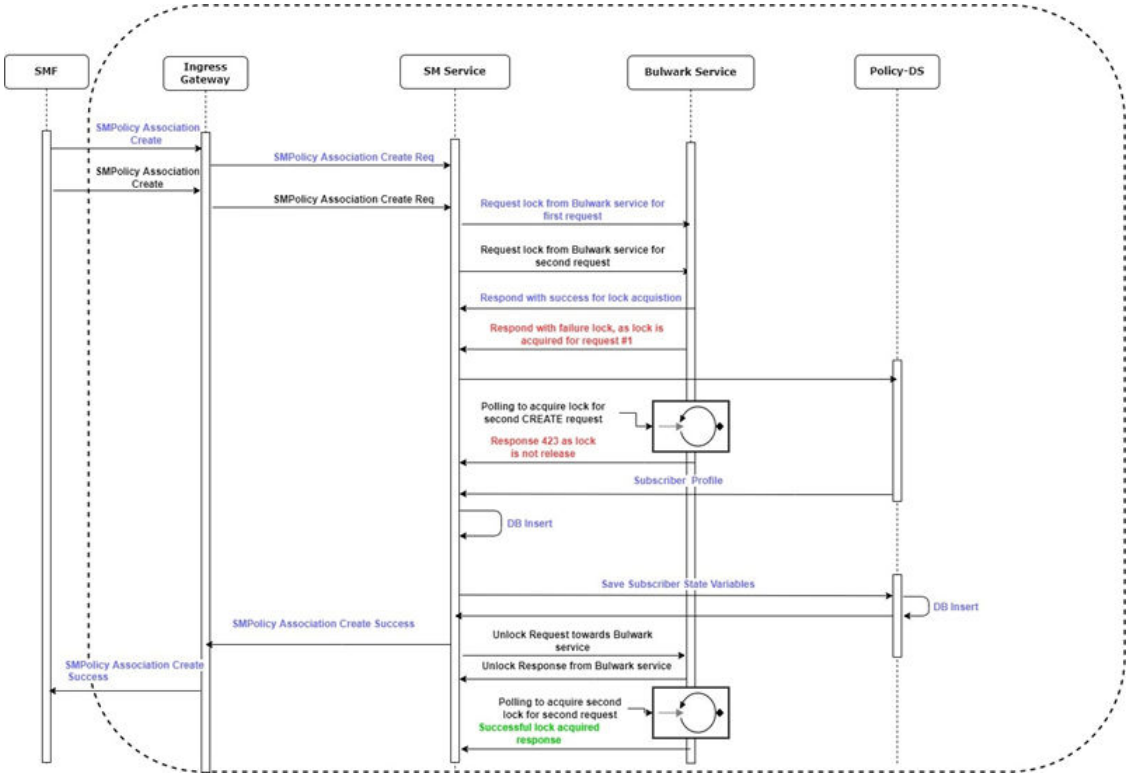
Call Flow for handling concurrent requests for SM Service

Call Flow for SM Create Request

The following diagram shows a scenario for SM create call flow where no service responds with error:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-218 Call Flow - Bulwark Lock Request SM Create Procedure

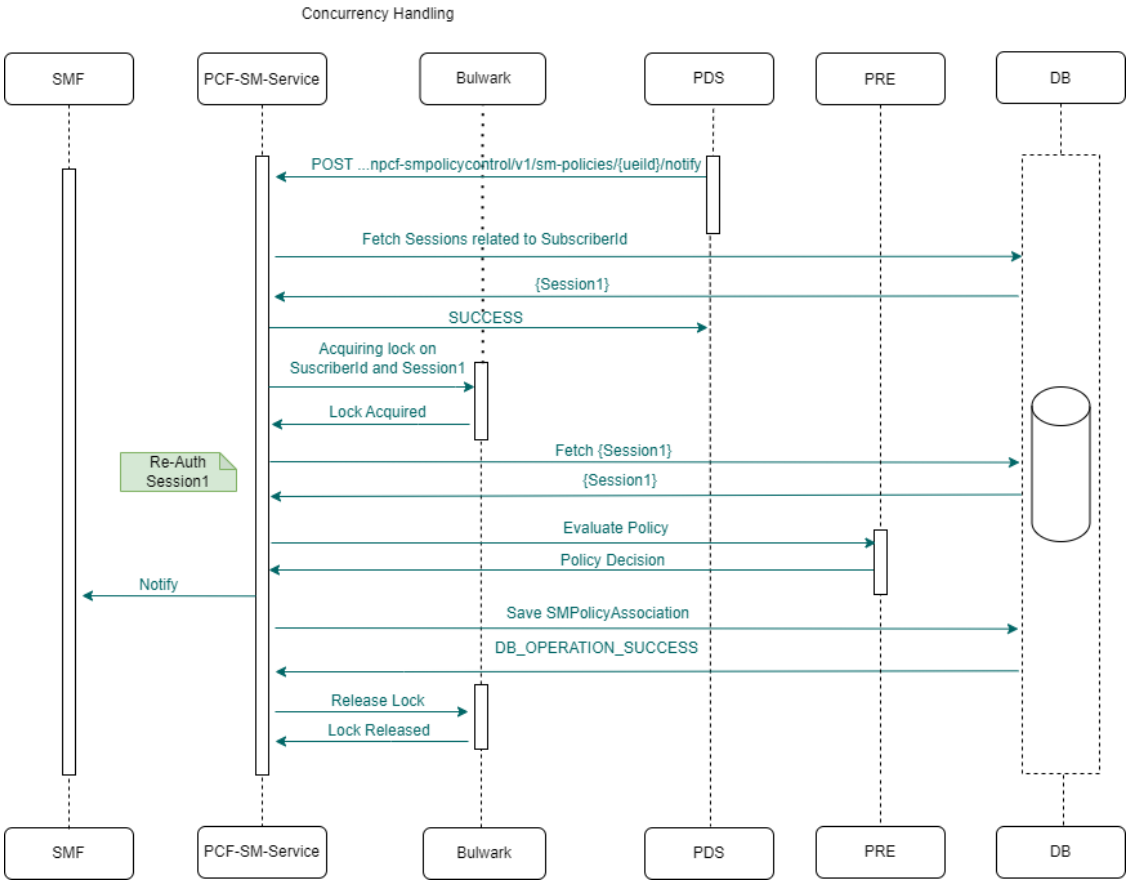


Call Flow for SM Update-Notify Request

The following diagram shows a scenario for SM Update-Notify call flow for one notification and one session:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-219 Call Flow for SM Update-Notify Request (One Notification and One Session)

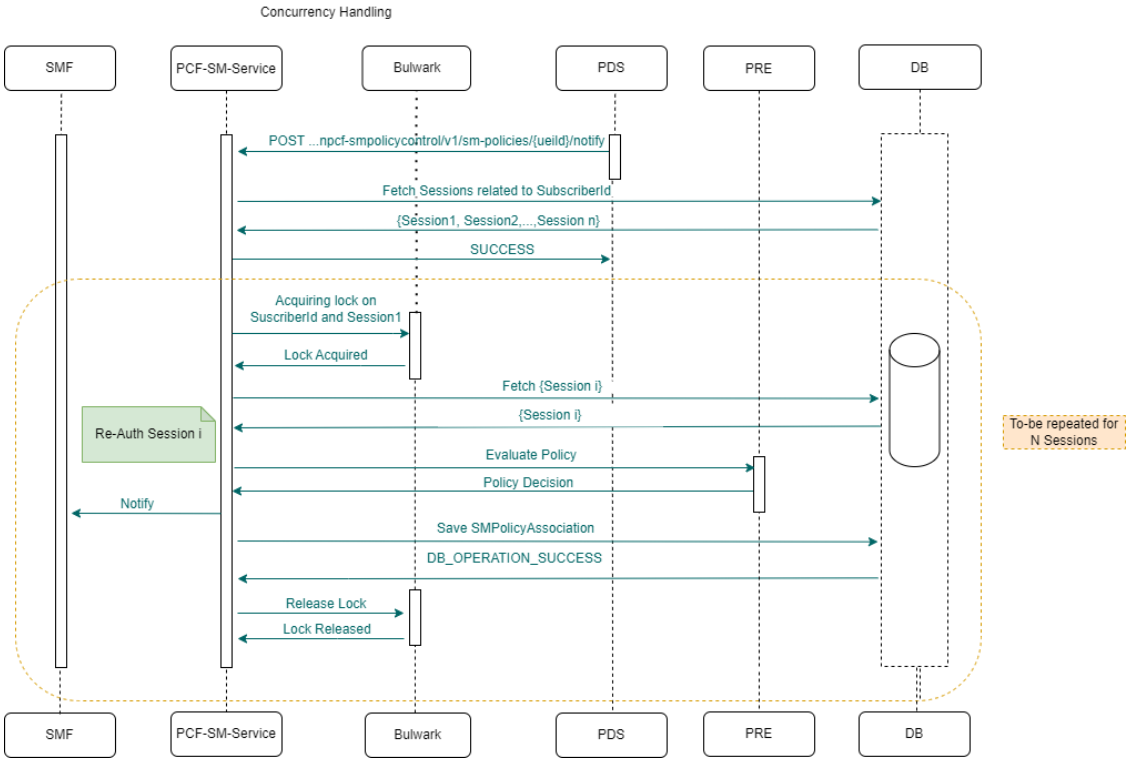


1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. A notify request tries to acquire the lock from bulwark service and gets the lock.
4. The notify request starts processing by fetching the session.
5. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. SM policy association is saved in DB.
7. On successful save, a notify response is sent to SMF and the lock is released.

The following diagram shows a scenario for SM Update-Notify call flow for one notification and n sessions:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-220 Call Flow for SM Update-Notify Request (One Notification and n Sessions)

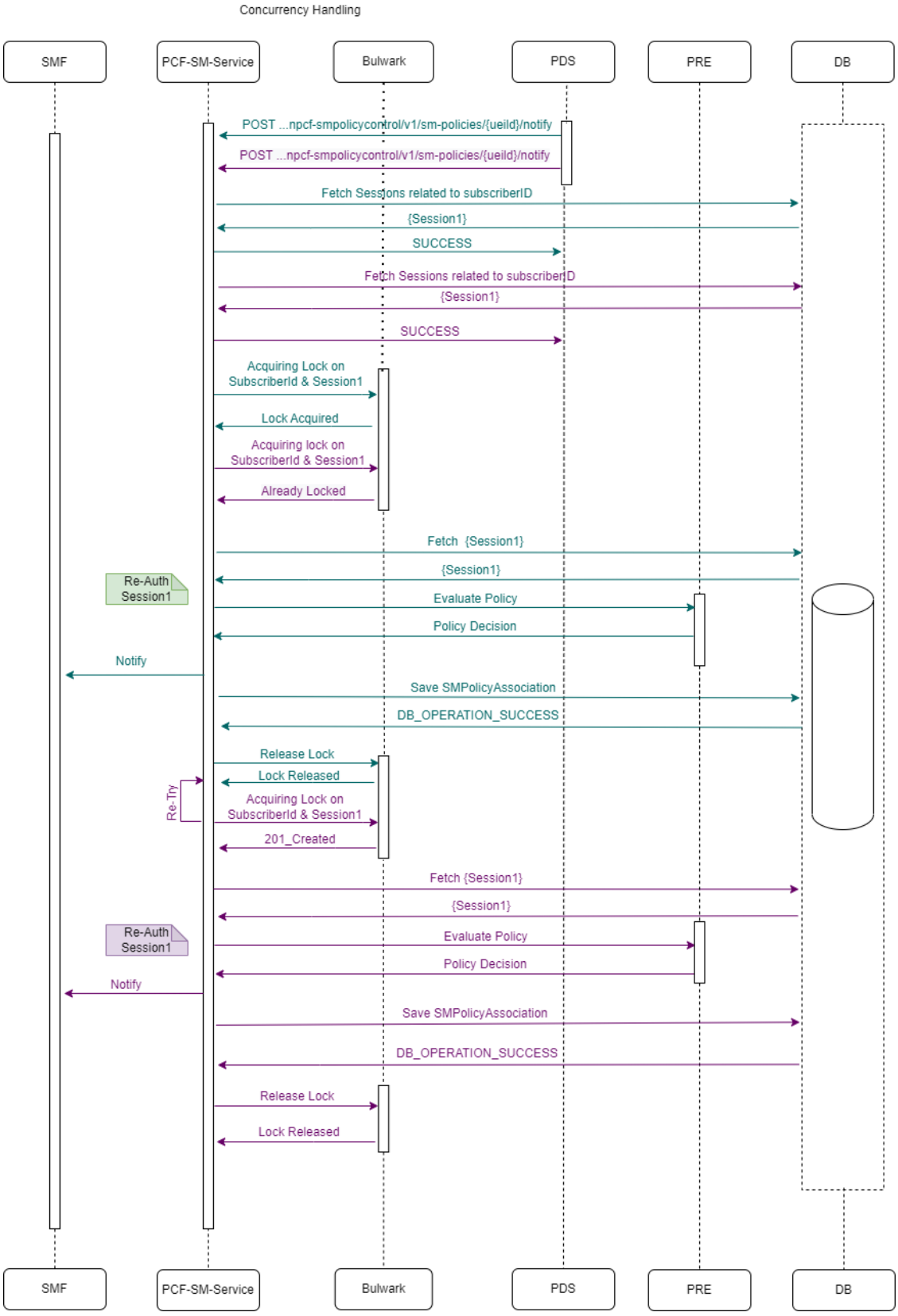


1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. A notify request tries to acquire the lock from bulwark service and gets the lock.
4. The notify request starts processing by fetching each sessions one by one.
5. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. SM policy association is saved in DB.
7. On successful save, a notify response is sent to SMF and the lock is released.
8. This process gets repeated for n sessions of the Notify request.

The following diagram shows a scenario for SM Update-Notify call flow for two notifications and one session:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-221 Call Flow for SM Update-Notify Request (Two Notifications and 1 Session)



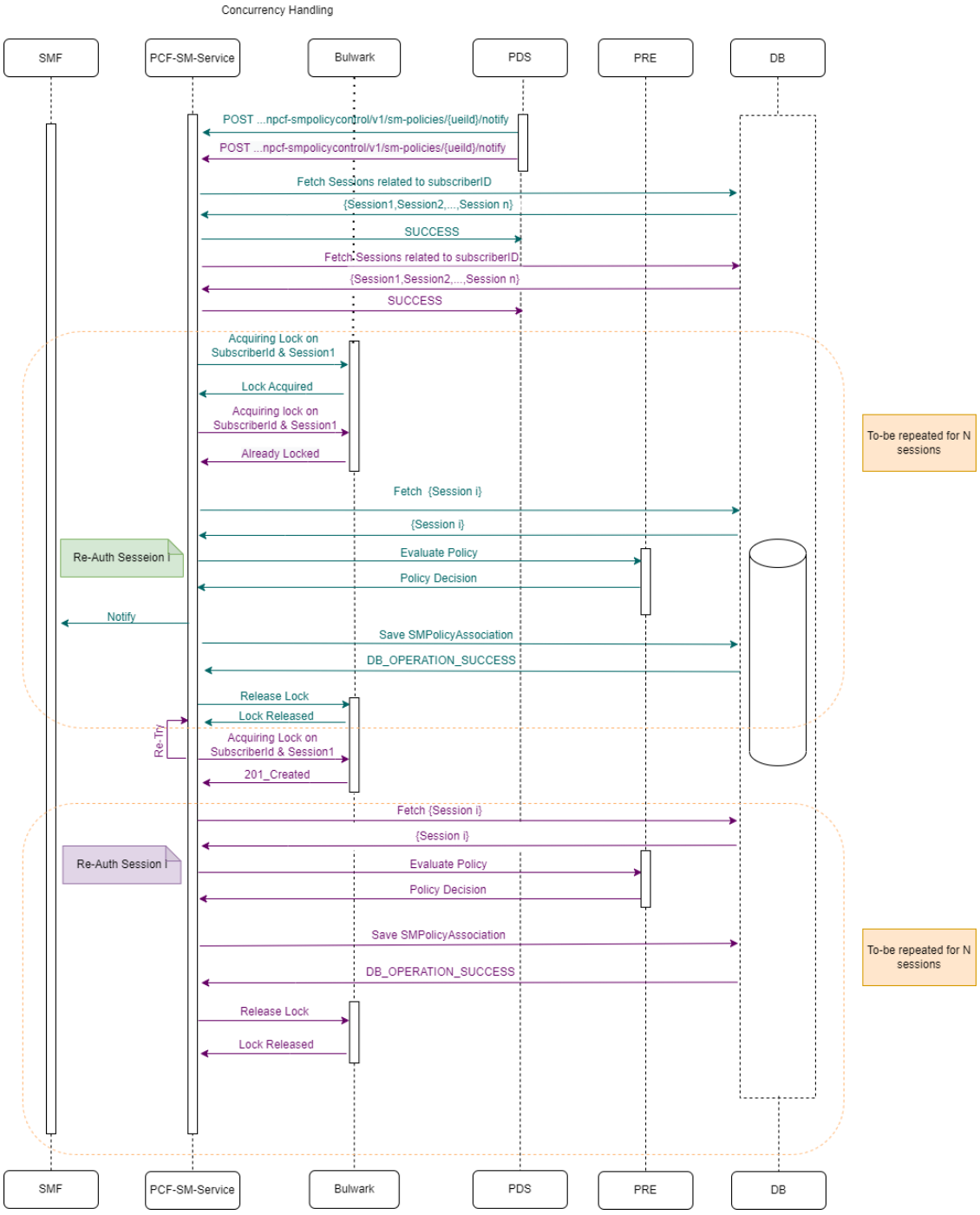
Copyright © 2019, 2026, Oracle and/or its affiliates.

1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. First notify request tries to acquire the lock from bulwark service and gets the lock.
4. Meanwhile, if second notify request tries to acquire lock, it will get an already locked response from Bulwark.
5. First notify request starts processing by fetching each sessions one by one.
6. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
7. SM policy association is saved in DB.
8. On successful save, a notify response is sent to SMF and the lock is released.
9. Then the second notify request will retry to acquire the lock. On lock acquisition, the same process is followed for second request as well.

The following diagram shows a scenario for SM Update-Notify call flow for two notifications from same subscriber and n sessions each:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-222 Call Flow for SM Update-Notify Request (Two Notifications from Same Subscriber and n Sessions Each)



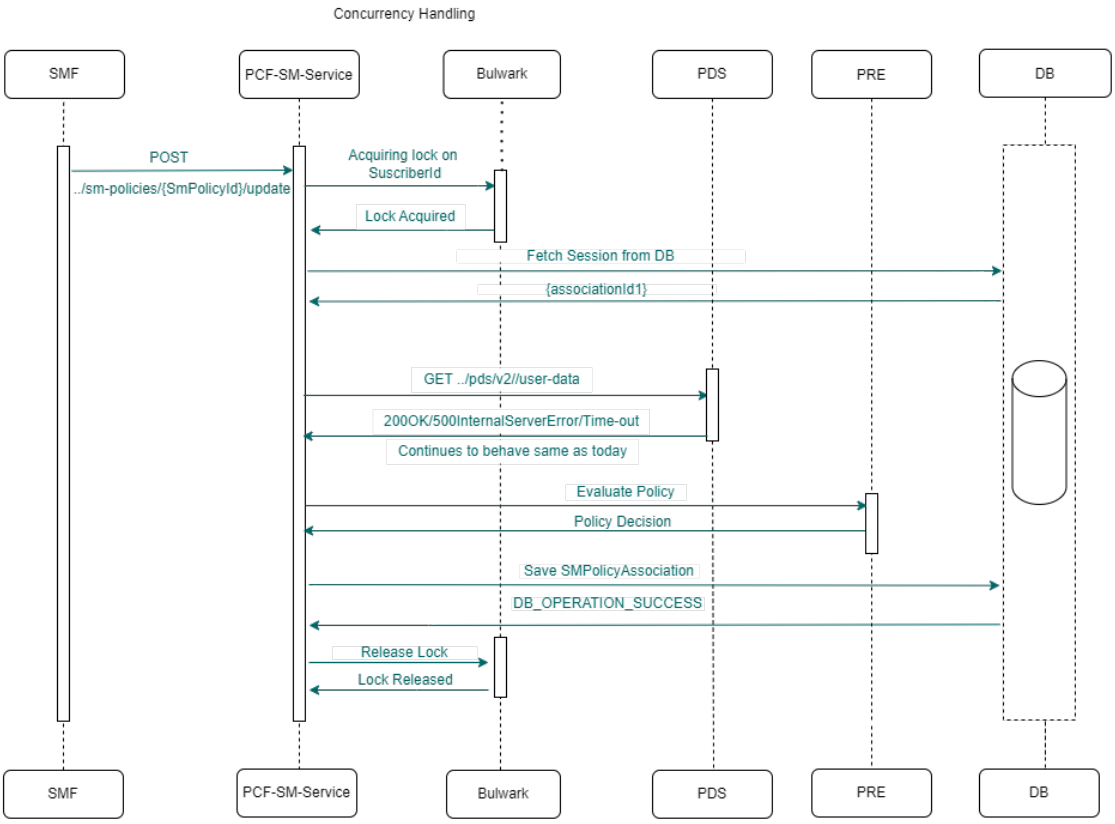
1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. First notify request tries to acquire the lock from bulwark service and gets the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. Meanwhile, if second notify request tries to acquire lock, it will get an already locked response from Bulwark.
5. First notify request starts processing by fetching each sessions one by one.
6. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
7. SM policy association is saved in DB.
8. On successful save, a notify response is sent to SMF and the lock is released.
9. This process gets repeated for n sessions of first Notify request.
10. Then the second notify request will retry to acquire the lock. On lock acquisition, the same process is followed for second request as well.

Call Flow for SM Update Request

Figure 4-223 Concurrency enabled for SM Update for a single session



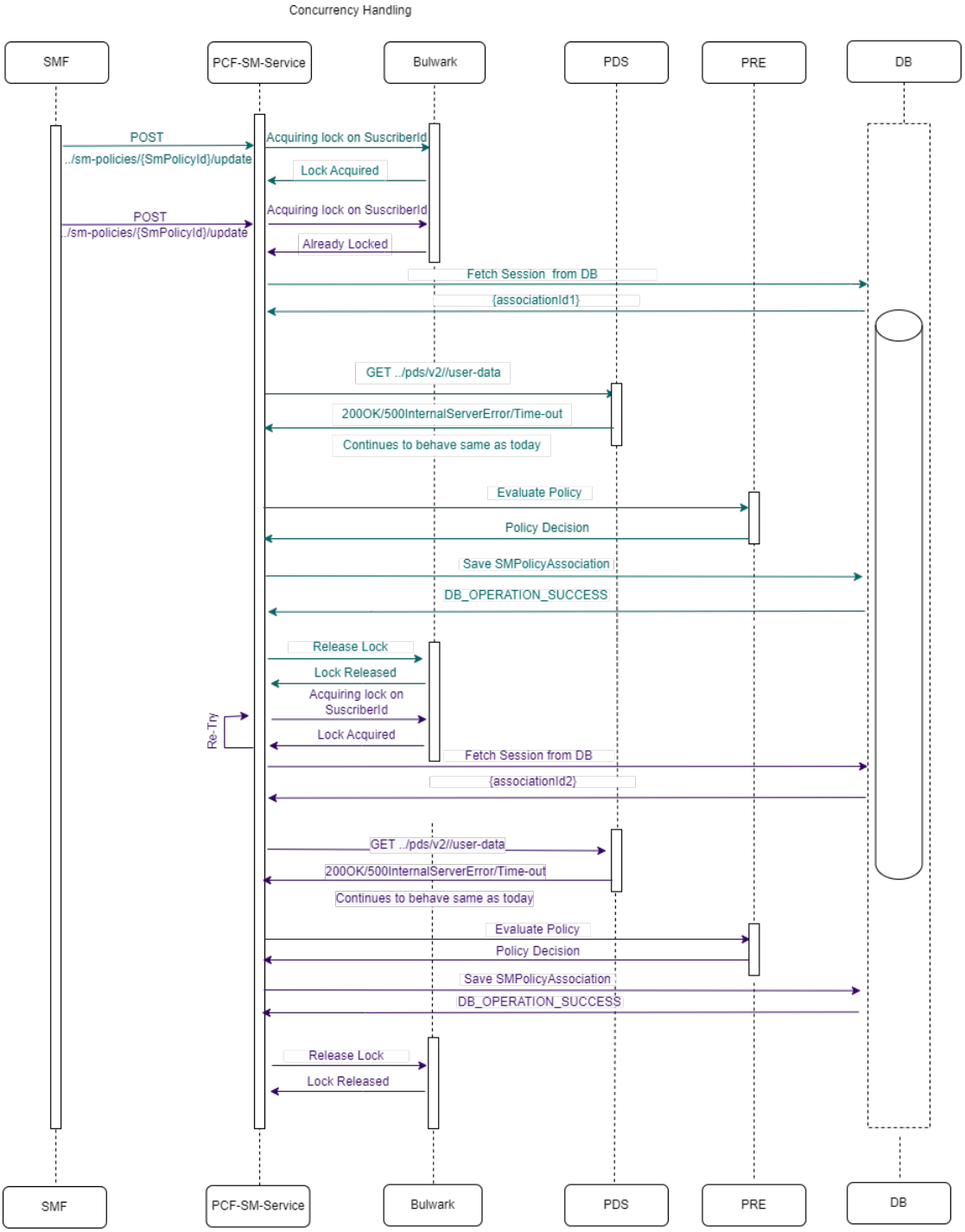
In this case, only concurrency is enabled for SM update and pending transaction is disabled. SM Service acquires a single key lock using subscriber ID of the request.

1. SM Service receives an SM Update request from SMF.
2. SM Service sends a lock request to Bulwark Service based on Subscriber ID.
3. SM Service acquires a lock from Bulwark Service.
4. SM Service fetches the session details from the database and sends the update request to PDS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. SM policy association is saved in the database.
7. After the successful completion of the updates, SM Service sends a lock release request to Bulwark Service to release the lock.

Figure 4-224 Concurrency Enabled for SM-Update and multiple updates for the same subscriber

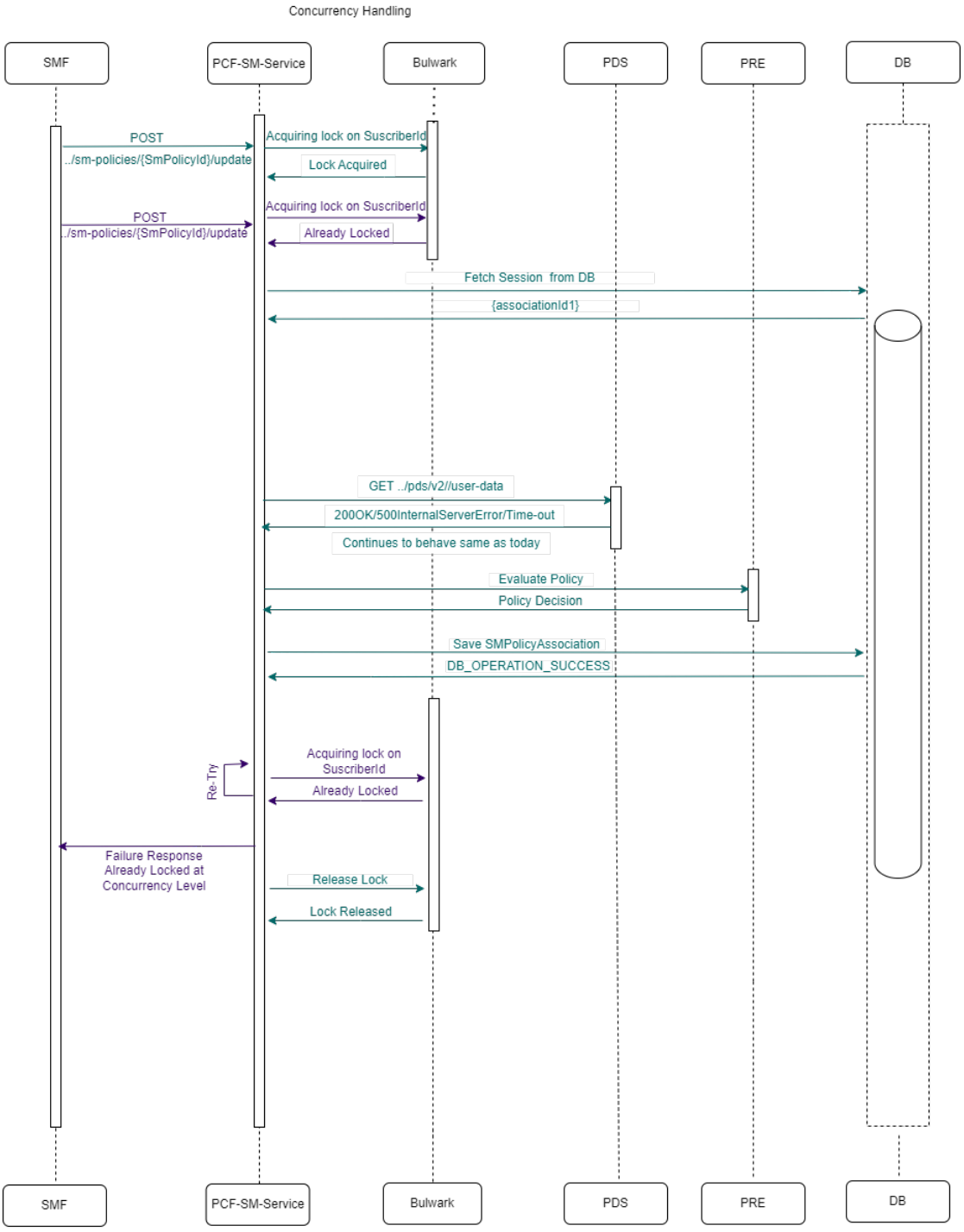


Copyright © 2019, 2026, Oracle and/or its affiliates.

1. SM Service receives the first SM Update request from SMF.
2. SM Service sends a lock request to Bulwark Service based on Subscriber ID.
3. SM Service acquires a lock for first request from Bulwark Service.
4. SM Service receives second SM Update request from SMF for the same subscriber.
5. SM Service sends a lock request to Bulwark Service for the second SM Update request.
6. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
7. SM Service fetches the session details from the database for the first update request and sends the update request to PDS.
8. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
9. SM policy association is saved in the database.
10. After the successful completion of the updates, SM Service sends a lock release request to Bulwark Service to release the lock for the first update request.
11. SM Service retries to acquire the lock for the second update request from Bulwark Service.
12. SM Service acquires a lock for the second update request, processes the update request.
13. After completing the updates for the second request, SM Service sends an unlock request to Bulwark Service to release the lock for the second request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-225 Retrial failure when there are multiple updates for same subscriber in different sessions



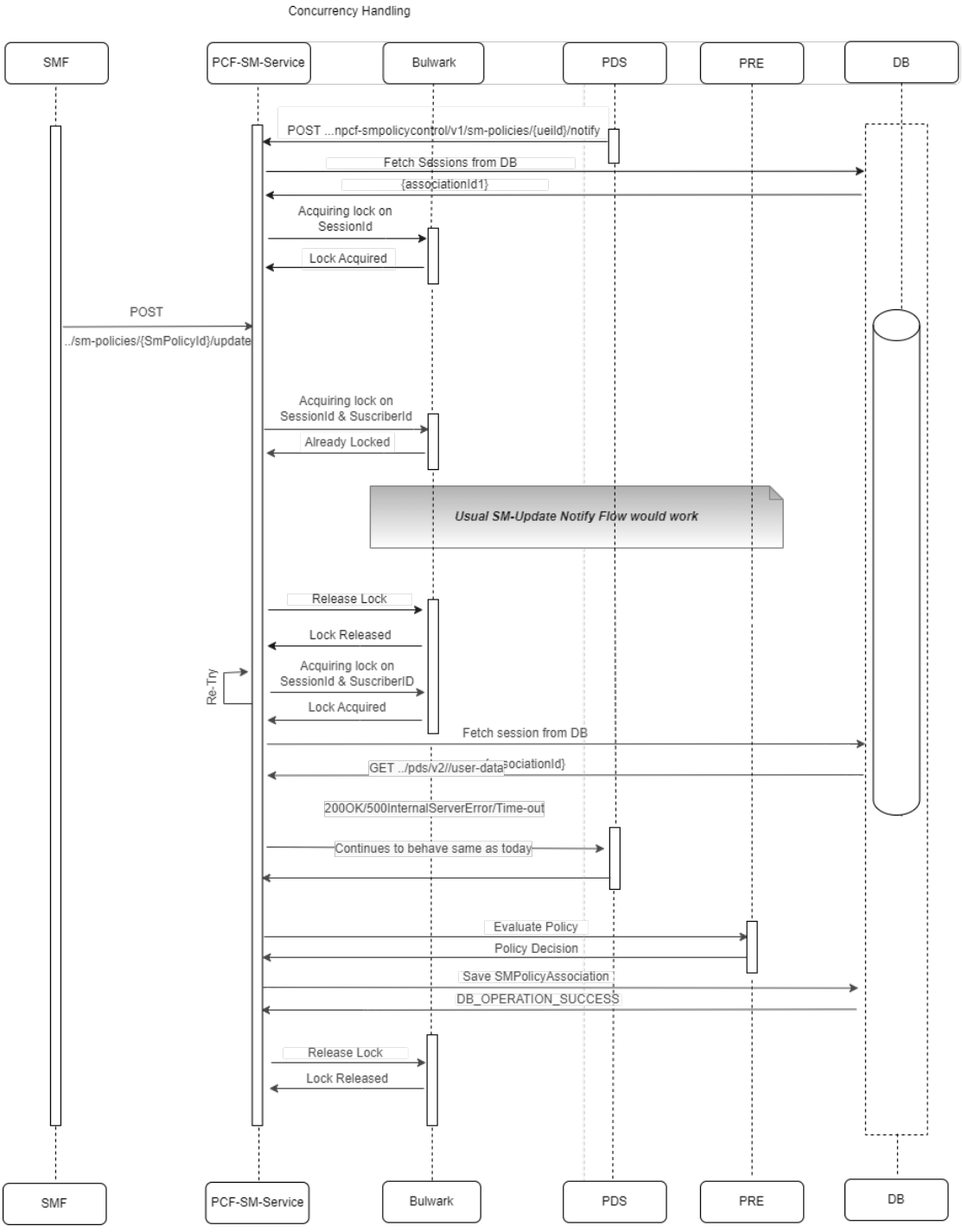
1. SM Service receives the first SM Update request from SMF.
2. SM Service sends a lock request to Bulwark Service based on Subscriber ID.
3. SM Service acquires a lock for first request from Bulwark Service.
4. SM Service receives second SM Update request from SMF for the same subscriber.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. SM Service sends a lock request to Bulwark Service for the second SM Update request.
6. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
7. SM Service fetches the session details from the database for the first update request and sends the update request to PDS.
8. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
9. SM policy association is saved in the database.
10. SM Service retries to acquire the lock for the second update request from Bulwark Service.
11. SM Service receives a 423 already acquired lock for the second lock request from Bulwark Service.
12. After the successful completion of the updates for the first request, SM Service sends a lock release request to Bulwark Service to release the lock for the first update request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-226 Pending transaction and Concurrent SM-Update for same session - Success scenario



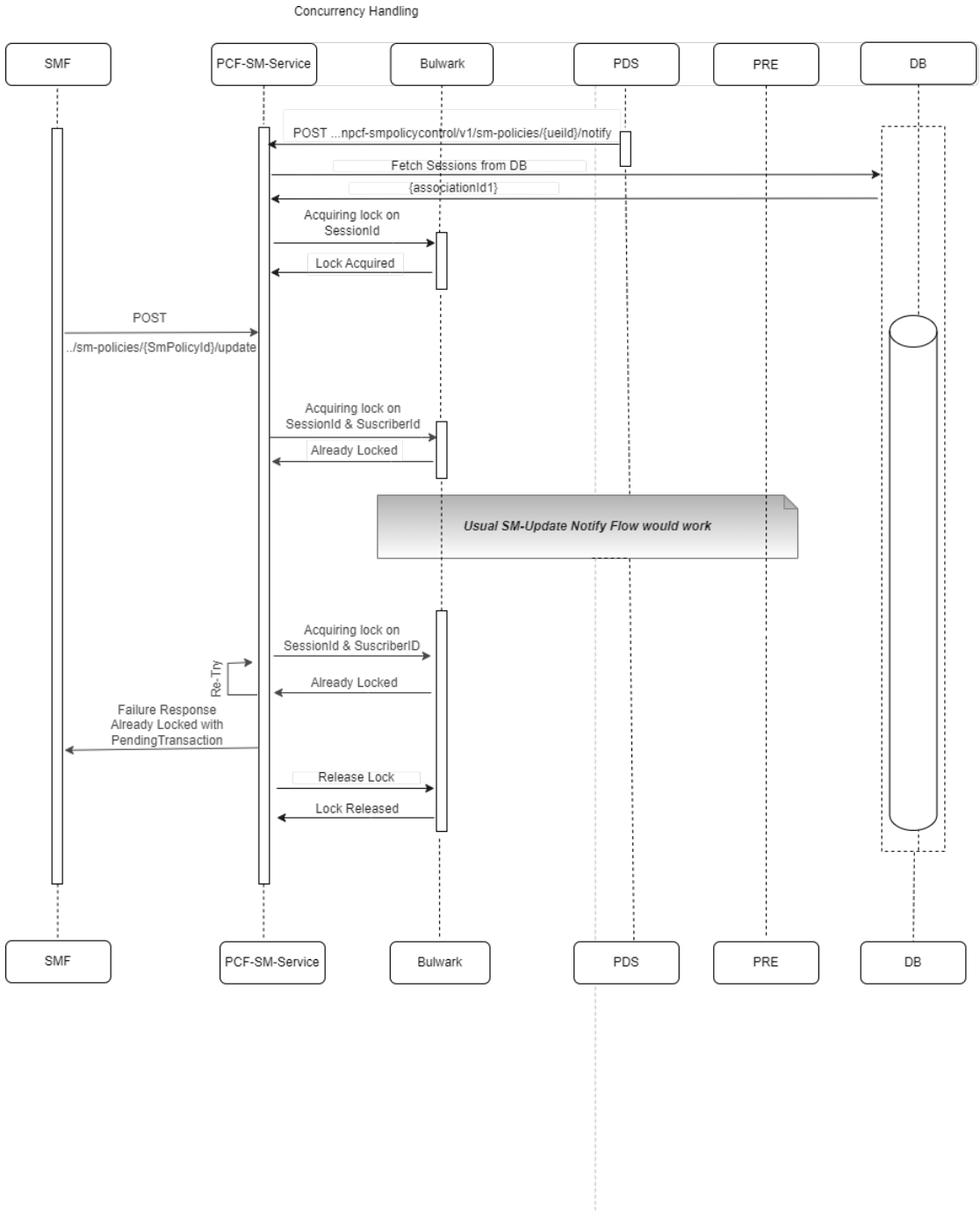
1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. SM Service tries to acquire a lock from Bulwark Service using SessionID and gets the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. SM Service receives an SM Update request from SMF.
5. SM Service sends a lock request to Bulwark Service using the Session ID as well as Subscriber ID.
6. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
7. After the successful completion of the first SM Update-notify request, SM Service sends an unlock request to Bulwark Service and Bulwark Service releases the lock for the first SM Update-Notify request.
8. SM Service retries to acquire the lock for the SM-Update request from SMF using the same Session ID as well as Subscriber ID.
9. SM Service acquires a lock with the retry.
10. SM Service fetches the session details from the database for the first update request and sends the update request to PDS.
11. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
12. SM policy association is saved in the database.
13. After the successful completion of the updates for the SM Update request, SM Service sends a lock release request to Bulwark Service to release the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-227 Pending transaction and Concurrent SM-Update for same session - Retry failure scenario



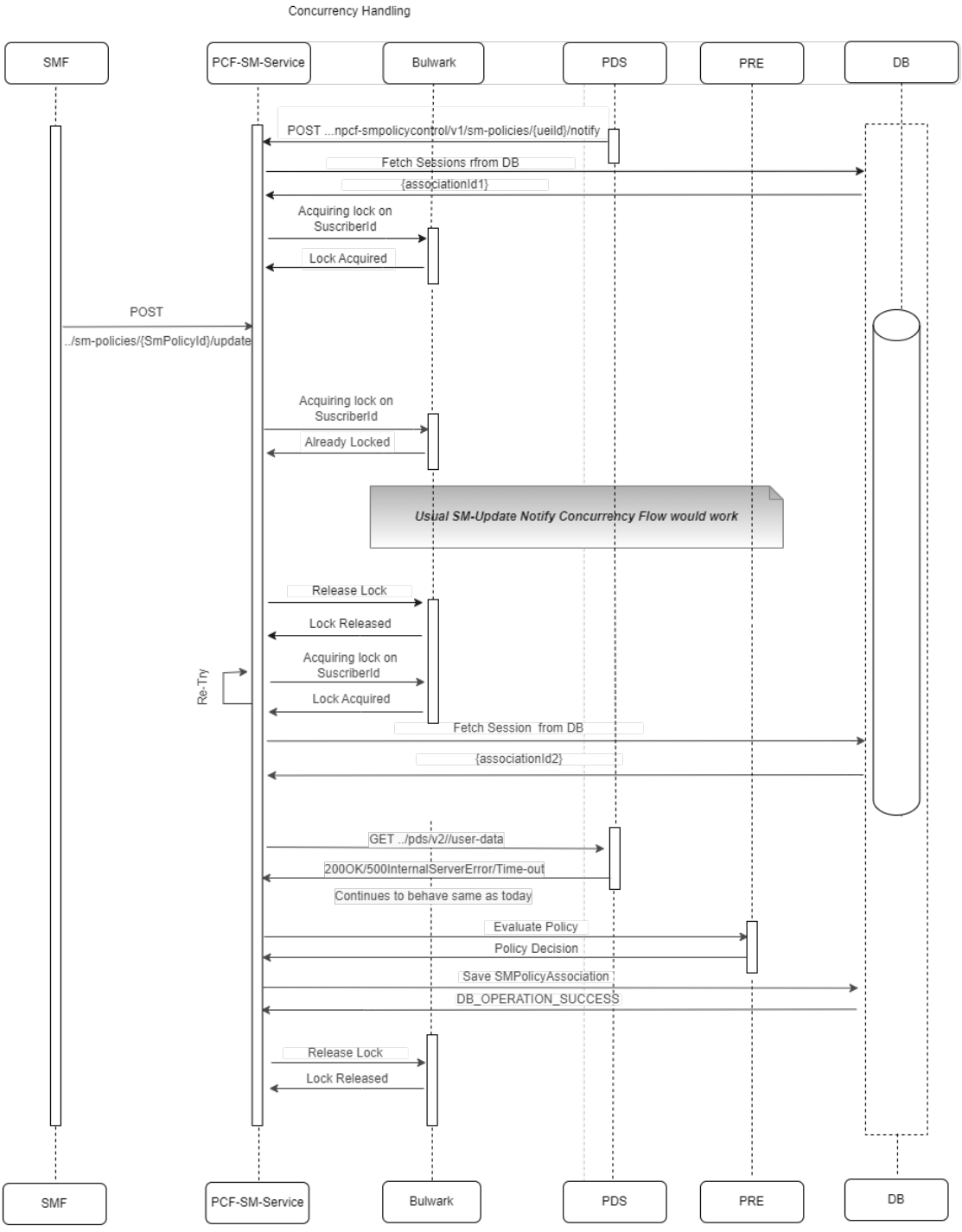
1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. SM Service tries to acquire a lock from Bulwark Service using SessionID and gets the lock.
4. SM Service receives an SM Update request from SMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. SM Service sends a lock request to Bulwark Service using the Session ID as well as Subscriber ID.
6. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
7. SM Service processes the SM Update-notify request.
8. SM Service retries to acquire the lock for the SM-Update request from SMF using the same Session ID as well as Subscriber ID.
9. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
10. If the retry count exhausts, SM Service sends an already locked with pending transaction - failure response to SMF.
11. After the successful completion of the updates for the SM Update-Notify request, SM Service sends a lock release request to Bulwark Service to release the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-228 Concurrent SM-Update-Notify and Concurrent SM-Update - Success scenario



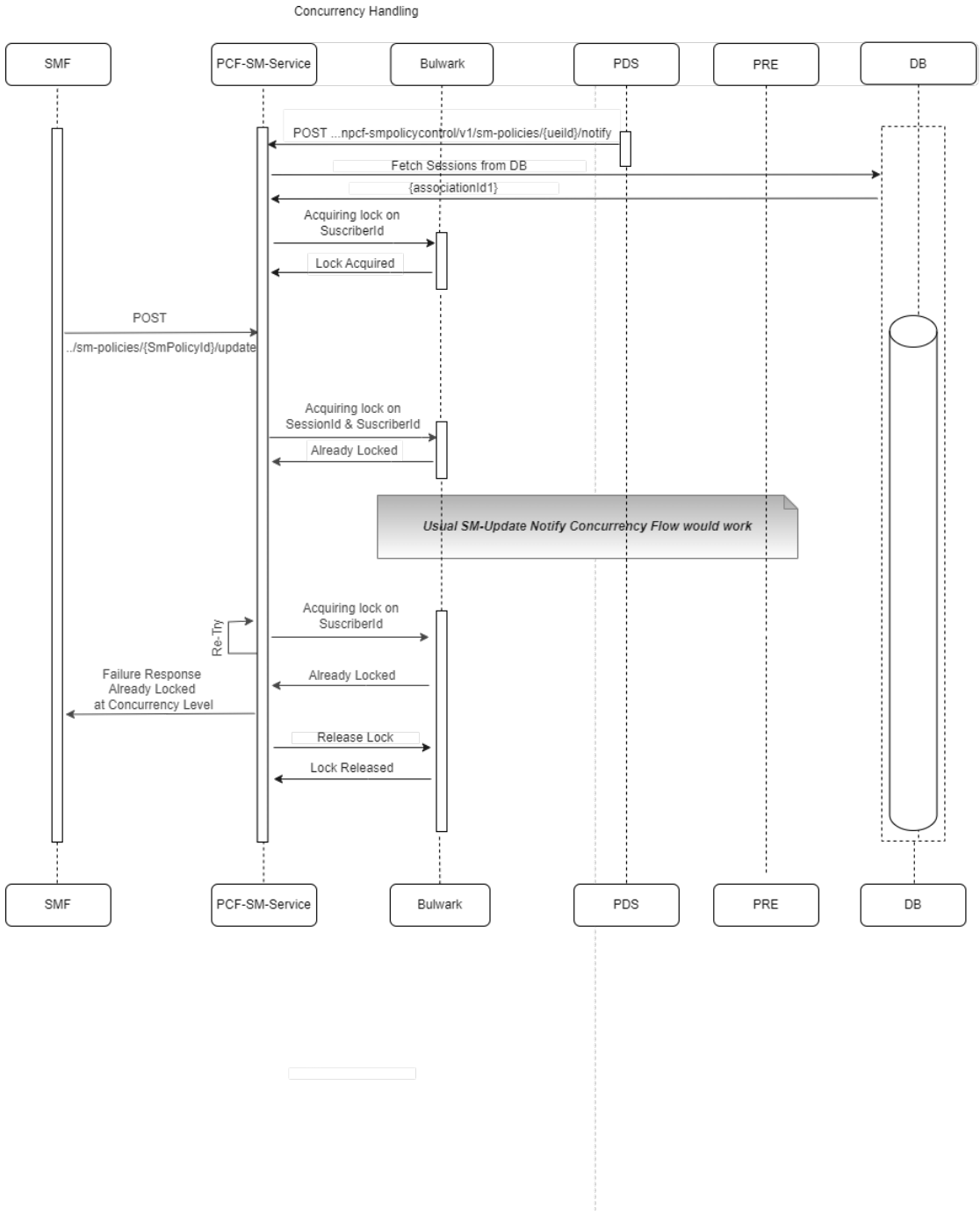
1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. SM Service tries to acquire a lock from Bulwark Service using SubscriberID and gets the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. SM Service receives an SM Update request from SMF.
5. SM Service sends a lock request to Bulwark Service for the same Subscriber ID.
6. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
7. SM Service processes the SM Update-notify request.
8. After the successful completion of the updates for the SM Update-Notify request, SM Service sends a lock release request to Bulwark Service to release the lock.
9. SM Service retries to acquire the lock for the SM-Update request from SMF using the same Subscriber ID and acquires the lock.
10. SM Service fetches the session details from the database for the second update request and sends the update request to PDS.
11. SM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
12. SM policy association is saved in the database.
13. After the successful completion of the updates for the second request, SM Service sends a lock release request to Bulwark Service to release the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-229 Concurrent SM-Update-Notify and Concurrent SM-Update - Failure scenario



1. PDS sends a notify request to SM service.
2. SM service fetches the corresponding sessions from database and sends a success response to PDS.
3. SM Service tries to acquire a lock from Bulwark Service using SubscriberID and gets the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

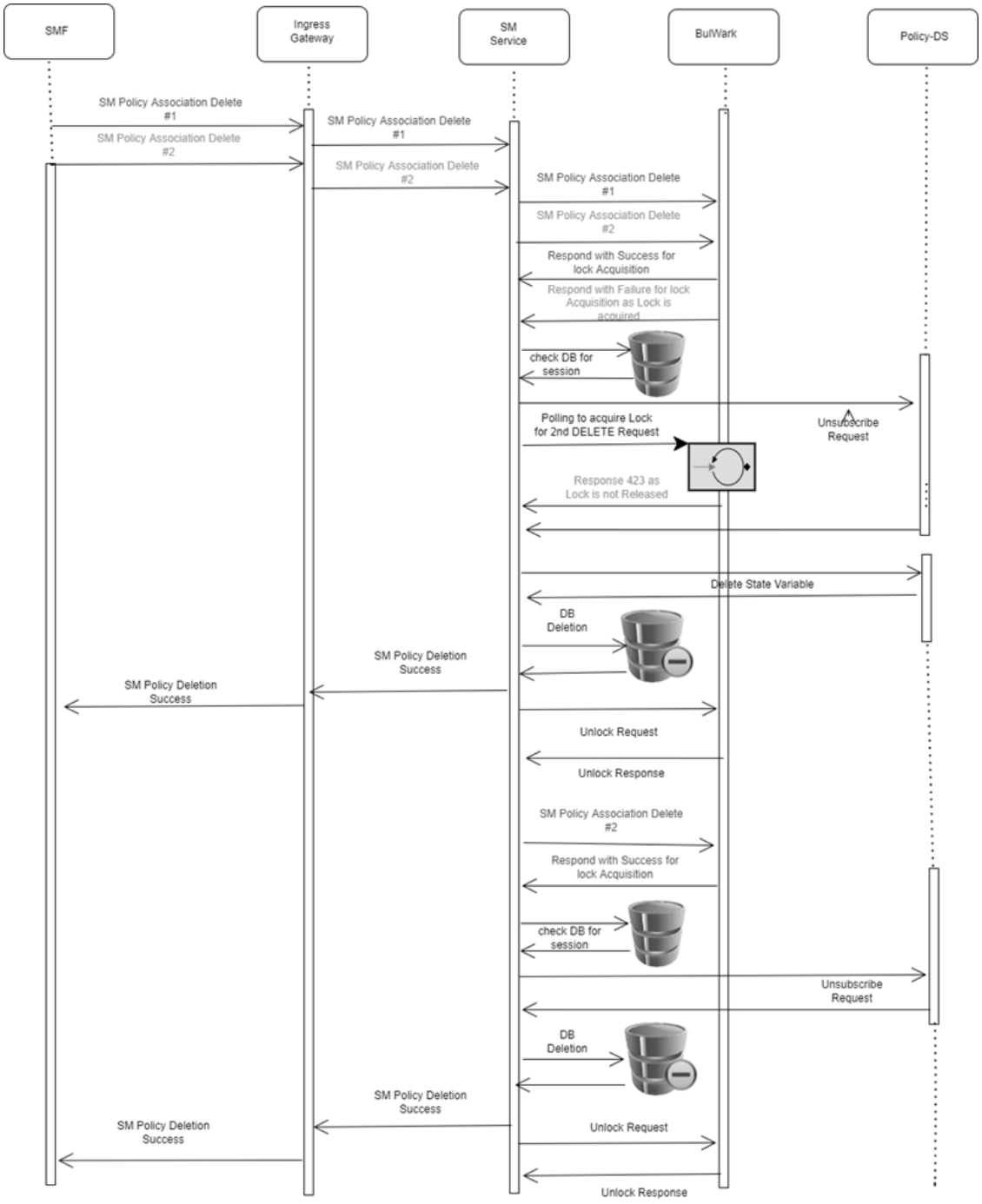
4. SM Service receives an SM Update request from SMF.
5. SM Service sends a lock request to Bulwark Service for the same Subscriber ID.
6. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
7. SM Service processes the SM Update-notify request.
8. SM Service retries to acquire the lock for the SM-Update request from SMF using the same Subscriber ID.
9. Bulwark Service responds to SM Service for the second request with a 423 already locked message.
10. After the successful completion of the updates for the SM Update-Notify request, SM Service sends a lock release request to Bulwark Service to release the lock.

Call Flow for SM Delete Request

The following diagram shows a scenario for SM delete call flow where no service responds with error:

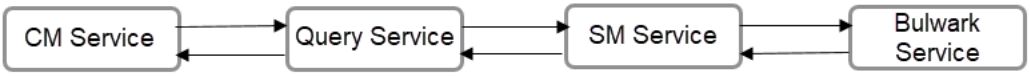
Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-230 Call Flow - Bulwark Lock Request SM Delete Procedure



Call Flow for SM Cleanup (Session Viewer Delete)

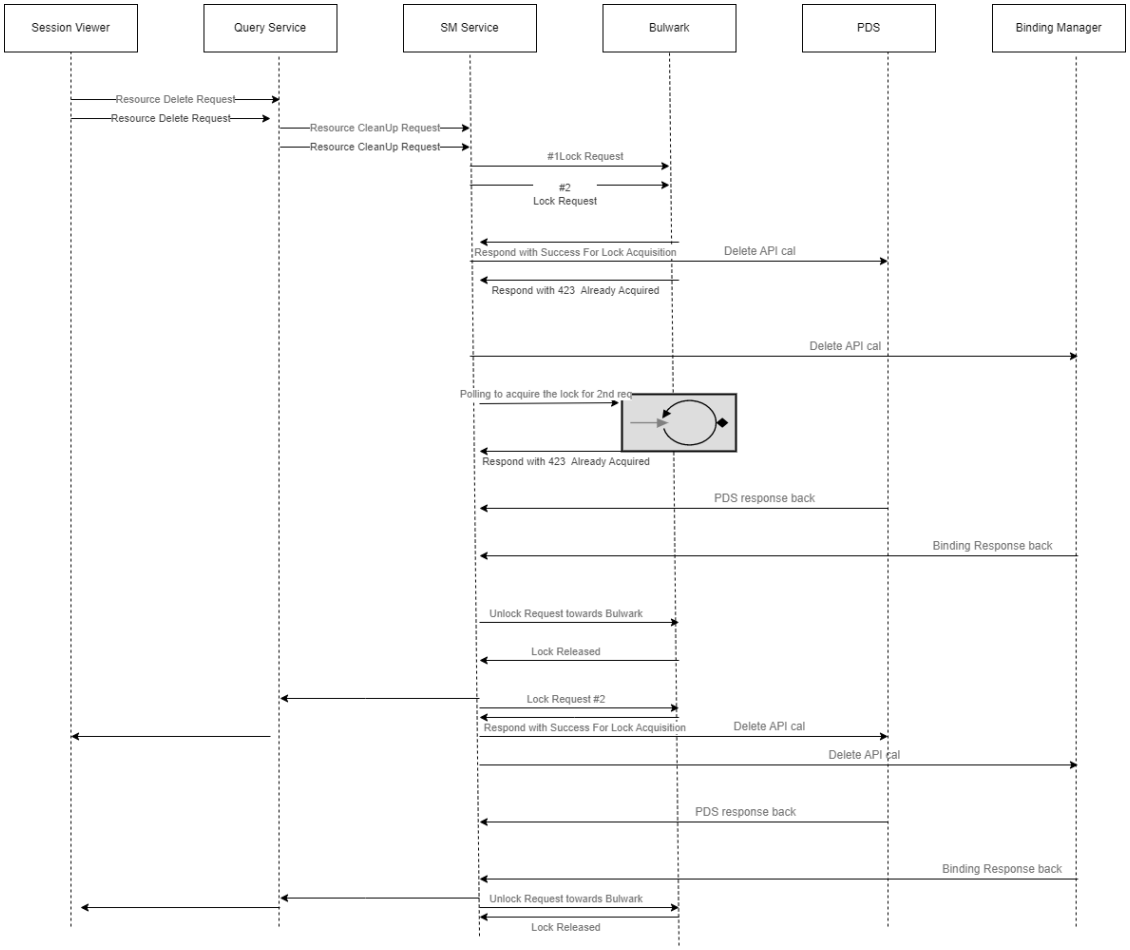
Figure 4-231 Requests for SM Clean



Copyright © 2019, 2026, Oracle and/or its affiliates.

The cleanup can be either a local delete or a remote delete. In either case, SM Cleanup API is called to delete the resource.

Figure 4-232 Local delete

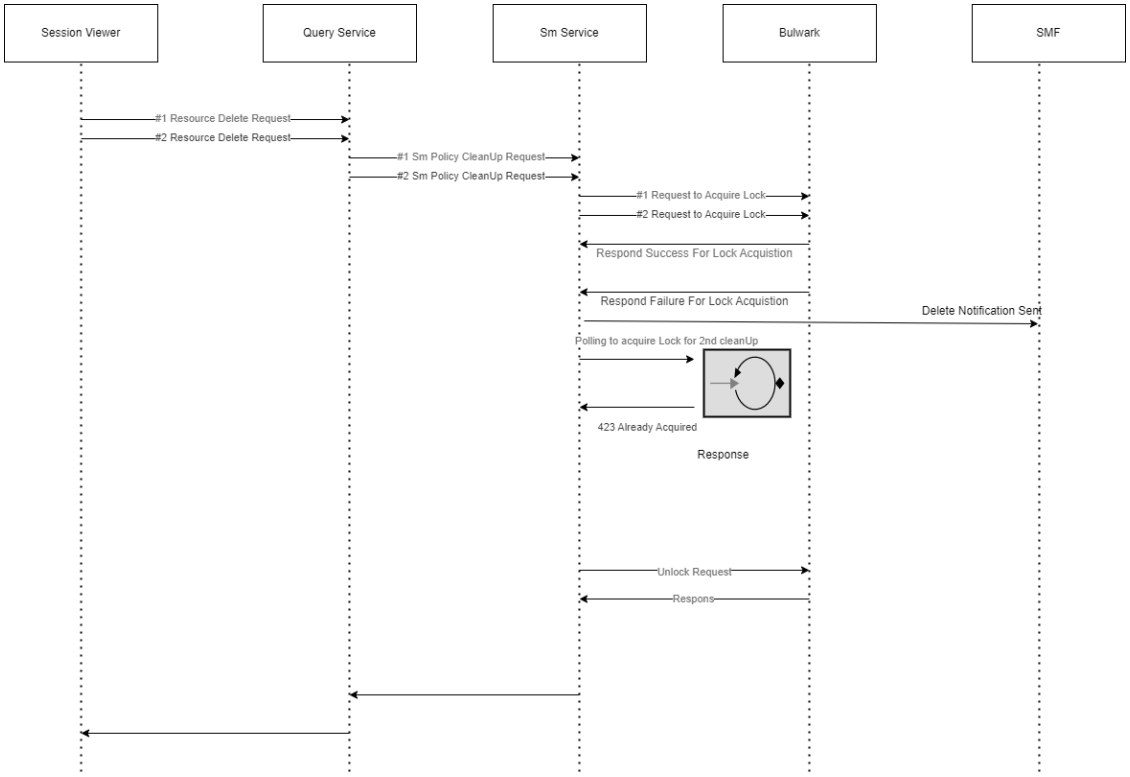


1. CM Service (**Session Viewer**) sends a Resource Delete Request based on policy association ID to Query Service, which in turn sends the Resource Cleanup request to SM Service.
2. If `CONCURRENCY.BULWARK_ENABLED_FOR_N7_CLEANUP` is enabled, SM Service sends a lock request to Bulwark Service to acquire the lock for the cleanup request.
   SM Service extracts the subscriber value using the policy association ID and uses the same as the key to gain the lock from Bulwark Service.
3. If the lock acquisition is successful:
   a. SM Service sends a delete request to PDS Resource Delete API to delete SM service's user data related to the individual SM policy association or the subscriber.
   b. After the data deletion, PDS responds to SM Service.
   c. SM service sends a delete request to Binding Service Resource Delete API to delete the binding data related to the individual SM policy association or the subscriber.
   d. After the data deletion, Binding Service responds to SM Service.
4. After receiving response from PDS and Binding Service, SM Service sends an unlock request to Bulwark Service to release the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. If SM Service receives another cleanup request at the same time, it tries to gain a lock for this second request from Bulwark Service.
6. If the lock request fails, SM Service receives a 423 already acquired response from Bulwark Service.
7. As per the configured number of retry counts, SM Service retries to gain the lock.
8. If it gains a lock, the SM Service sends a delete request to PDS and to Binding Service to delete the data.
9. If it fails to gain a lock and the number of retries reaches `CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_CLEANUP`, Bulwark Service sends a 500 internal error to SM Service.

Figure 4-233 Remote delete



SM Service cleans up the data remotely when you check **Remote** checkbox in **Session Viewer** page on the UI and then click **Delete**.

1. CM Service (**Session Viewer**) sends a Resource Delete Request based on policy association ID and `deleteScope=Remote` to Query Service, which in turn sends the Resource Cleanup request to SM Service.
2. If `CONCURRENCY.BULWARK_ENABLED_FOR_N7_CLEANUP` is enabled, SM Service sends a lock request to Bulwark Service to acquire the lock for the cleanup request.
   SM Service extracts the subscriber value using the policy association ID and uses the same as the key to gain the lock from Bulwark Service.
3. If the lock acquisition is successful:
   a. SM Service sends a Session Delete Notification to SMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

   b. If SM Service, receives a `404 not found` response, it emulates a Session Delete Request to delete the SM Policy Association.
   c. SM Service deletes the SM Policy Association as per the PA Session Delete Procedure.
4. After the deletion is successful, SM Service sends an unlock request to Bulwark Service to release the lock.
5. If SM Service receives another cleanup request at the same time, it tries to gain a lock for this second request from Bulwark Service.
6. If the lock request fails, SM Service receives a 423 already acquired response from Bulwark Service.
7. As per the configured number of retry counts, SM Service retries to gain the lock.
8. If it gains a lock, the SM Service sends a Session Delete Notification to SMF and deletes the SM Policy Association as per the PA Session Delete Procedure.
9. If it fails to gain a lock and the number of retries reaches `CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_CLEANUP`, Bulwark Service sends a 500 internal error to SM Service.

Managing Concurrency Handling for SM Service

Enable

You can enable the concurrency handling through Bulwark using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** Set value for the following parameters under the **Advanced Settings** section on the **PCF Session Management** page:
  - CONCURRENCY.BULWARK_ENABLED_FOR_N7_CREATE
  - CONCURRENCY.BULWARK_ENABLED_FOR_N7_DELETE
  - CONCURRENCY.LOCK_LEASE_DURATION_FOR_UPDATE_NOTIFY
  - CONCURRENCY.LOCK_WAIT_DURATION_FOR_UPDATE_NOTIFY
  - CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_UPDATE_NOTIFY
  - CONCURRENCY.BULWARK_ENABLED_FOR_N7_UPDATE_NOTIFY
  - CONCURRENCY.UPDATE_USERDATA_IN_ASSOCIATION_ON_LOCKFAILURE
  - CONCURRENCY.LOCK_LEASE_DURATION_FOR_UPDATE
  - CONCURRENCY.LOCK_WAIT_DURATION_FOR_UPDATE
  - CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_UPDATE
  - CONCURRENCY.BULWARK_ENABLED_FOR_N7_UPDATE
  - CONCURRENCY.LOCK_LEASE_DURATION_FOR_CLEANUP
  - CONCURRENCY.LOCK_WAIT_DURATION_FOR_CLEANUP
  - CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_CLEANUP
  - CONCURRENCY.BULWARK_ENABLED_FOR_N7_CLEANUP

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> If you do not make these parameters as configurable, the SM service uses the default values for these parameters.

For more information about enabling the feature through CNC Console, see PCF Session Management.

- **Enable using REST API:** Set the Keys and Values for **Advanced Settings** under PCF Session Management Service. For more information about enabling the feature through REST API, see "PCF Session Management" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the concurrency handling through Bulwark functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations under the **Advanced Settings** section on the **PCF Session Management** page. For more information about configuring audit service, see PCF Session Management.
- **Configure using REST API:**Set the Keys and Values for **Advanced Settings** under PCF Session Management Service. For more information about enabling the feature through REST API, see "PCF Session Management" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.123.2 Support for Concurrency Handling using Bulwark Service in AM

The Bulwark Service integrates with the AM service to handle the concurrent requests for the AM Create, AM Update, AM Delete, and AM Update-Notify procedures. The AM service integration with Bulwark service handles the concurrent requests for the same subscriber in a concurrent and efficient manner.

In case of multiple create, update, or delete requests for the same subscriber, the AM service requests a lock for the SUPI or GPSI value from the Bulwark service. Once the lock is acquired, the AM create, AM Update, AM delete, or AM Update-Notify request is executed for the SUPI or GPSI value with which the lock is requested. After the successful completion of the requests, the AM service sends a request to release the lock to Bulwark.

As the notification is locked, pending transaction comes into picture.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and AM Update:

Table 4-174 Pending Transaction and Concurrency in AM Update

Pending Transaction	Concurrency in AM Update	Use-Case
Enabled	Disabled	Single Key - Session level lock will be acquired. Pending-transaction call flow would work.
Disabled	Enabled	Single Key - Subscriber level lock will be acquired. Update-Notify call flow with concurrency would work.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-174 (Cont.) Pending Transaction and Concurrency in AM Update

Pending Transaction	Concurrency in AM Update	Use-Case
Enabled	Enabled	Multi-Key - Session Level & Subscriber Level locks will be acquired.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and update-notify:

Table 4-175 Pending Transaction and Concurrency in AM Update-Notify

Pending Transaction	Concurrency in Update-Notify	Use-Case
Enabled	Disabled	Single Key - Session level lock will be acquired. Pending-transaction call flow would work.
Disabled	Enabled	Single Key - Subscriber level lock will be acquired. AM-Update call flow would work.
Enabled	Enabled	Multi-Key - Session Level & Subscriber Level locks will be acquired.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and AM Update and AM update-notify:

Table 4-176 Pending Transaction and Concurrency in AM Update as well as AM Update-Notify

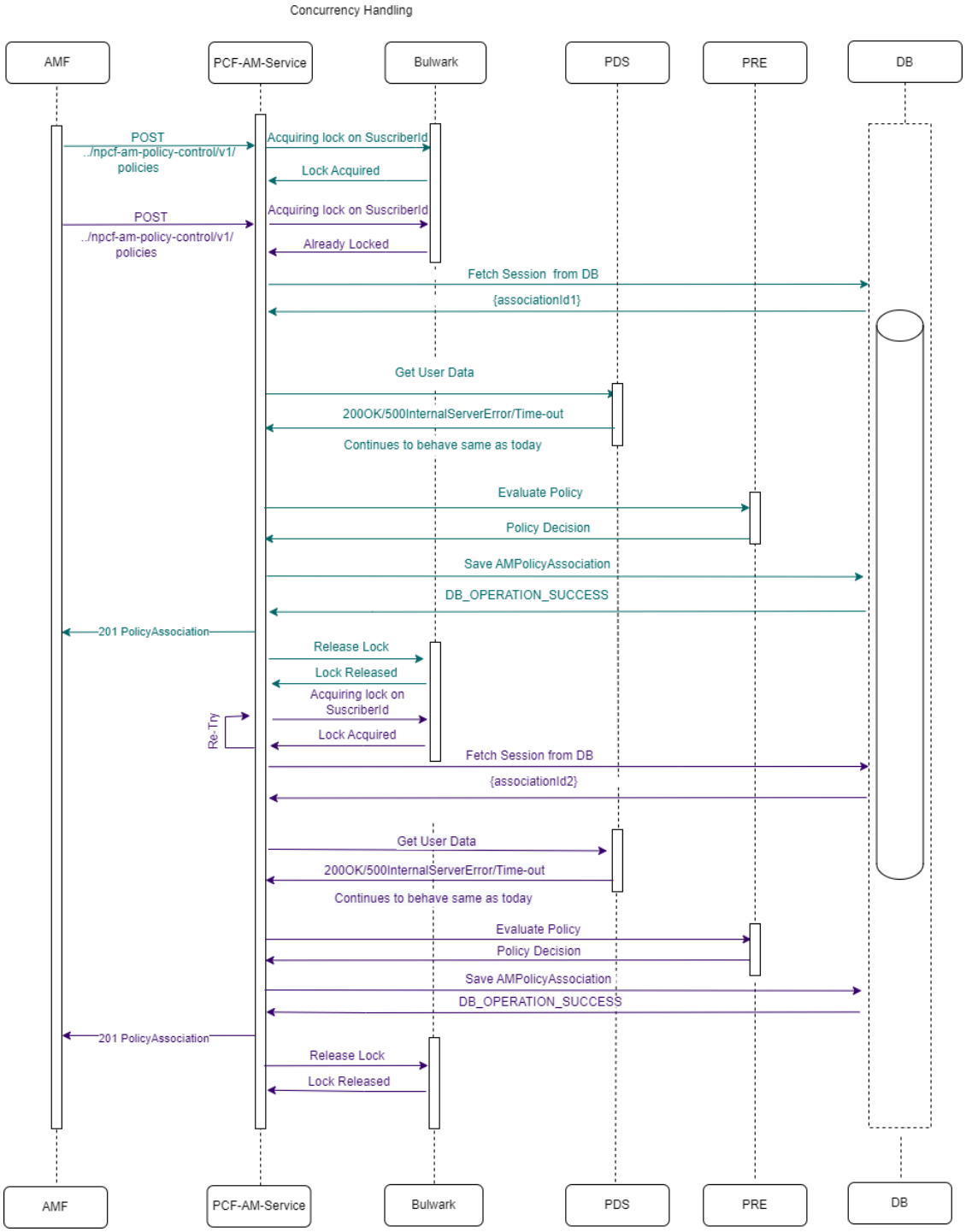
Pending Transaction	Concurrency in AM Update	Concurrency in AM Update-Notify	Use-Case
Enabled	Disabled	Disabled	Session Level Lock Acquired - during collision, lock acquisition fails at SessionID
Disabled	Enabled	Disabled	Subscriber Level lock acquired - during collision, lock acquisition fails at subscriberID
Disabled	Enabled	Enabled	Subscriber Level lock acquired - during collision, lock acquisition fails at subscriberID
Enabled	Enabled	Disabled	Session Level & Subscriber Level locks will be acquired - during collision, lock acquisition will fail at SessionID

Call Flow for handling concurrent requests for AM Service

Call flow for two AM-Create requests for same subscriber and retry success

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-234 Call flow for two AM-Create requests for same subscriber and retry success



In this case, only concurrency is enabled for AM Create. AM Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. AM Service receives an AM Create request from AMF.

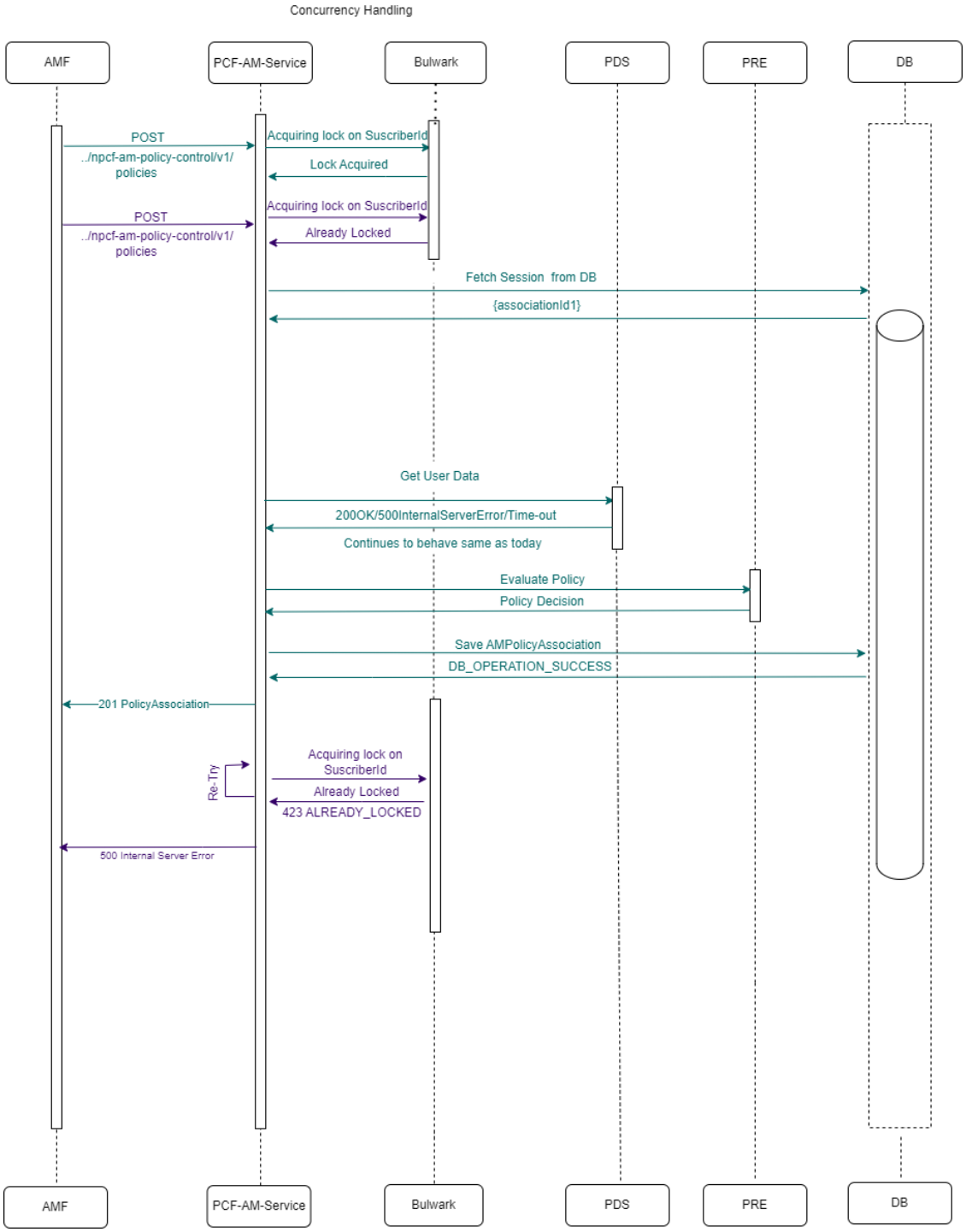
Copyright © 2019, 2026, Oracle and/or its affiliates.

2. AM Service sends a lock request to Bulwark Service based on the configuration of RESOURCEID.SUFFIXLIST.
3. AM Service acquires a lock from Bulwark Service.
4. AM Service fetches the session details from the database and sends the create request to PDS.
5. AM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. AM policy association is saved in the database.
7. After the successful completion of the create, AM Service sends a unlock release request to Bulwark Service to release the lock.

Two AM-Create requests for same Subscriber and retry failure (retry =1, CONCURRENCY.N15.CREATE.ALLOW_ON_SERVICE_FAILURE = false)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-235 Two AM-Create requests for same Subscriber and retry failure (retry =1, CONCURRENCY.N15.CREATE.ALLOW_ON_SERVICE_FAILURE = false)



Concurrency is enabled for AM Create. AM Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. AM Service receives the first AM Create request from AMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

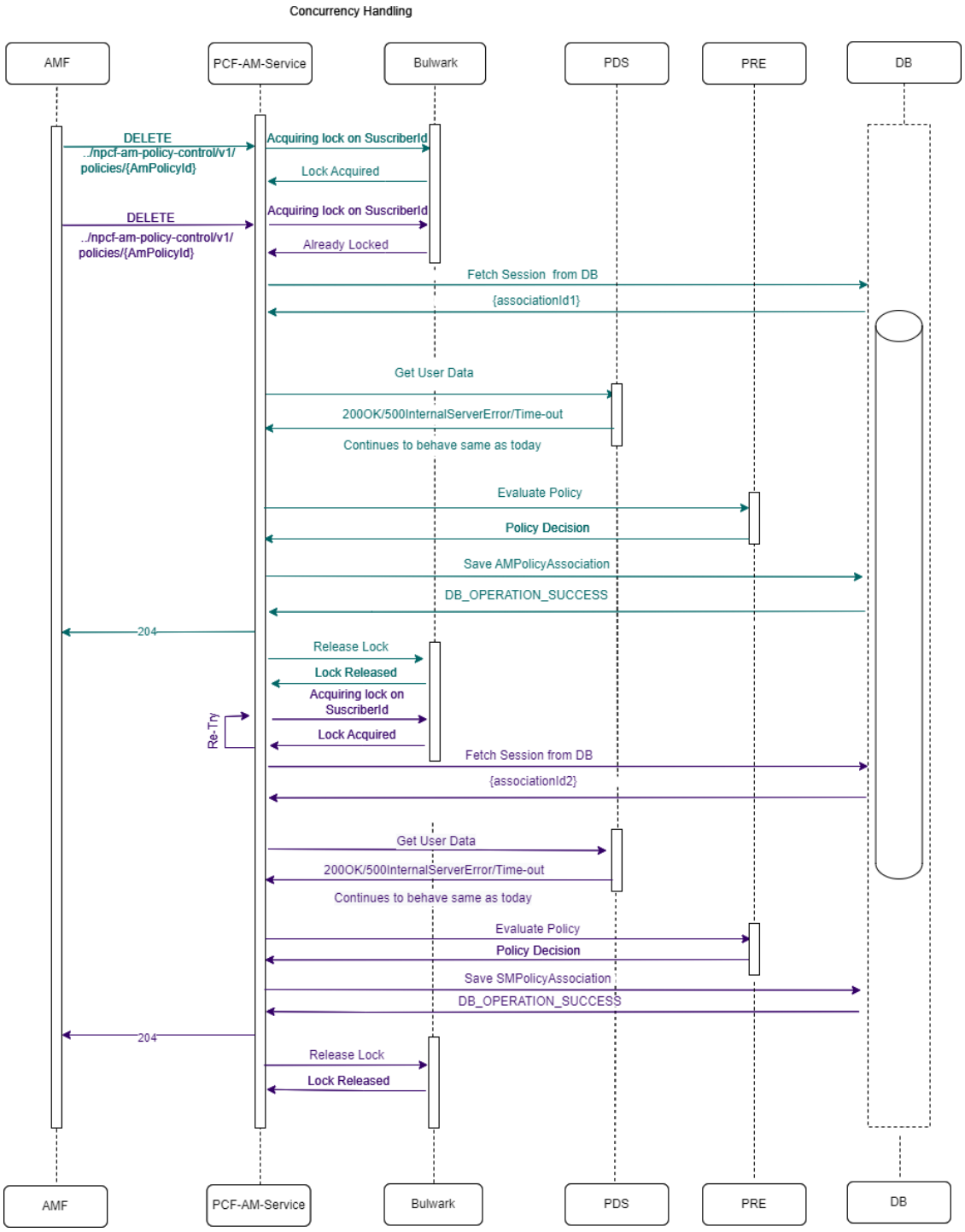
2. AM Service sends a lock request to Bulwark Service based on what is configured in RESOURCEID.SUFFIXLIST.
3. AM Service acquires a lock for first request from Bulwark Service.
4. AM Service receives second AM Create request from AMF for the same subscriber.
5. AM Service sends a lock request to Bulwark Service for the second AM Create request.
6. Bulwark Service responds to AM Service for the second request with a 423 already locked message.
7. AM Service fetches the session details from the database for the first create request and sends the create request to PDS.
8. AM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
9. AM policy association is saved in the database.
10. After the successful completion of the request, AM Service sends a lock release request to Bulwark Service to release the lock for the first create request.
11. AM Service retries to acquire the lock for the second create request from Bulwark Service.
12. AM Service acquires a lock for the second create request, processes the create request.
13. After completing the create for the second request, AM Service sends an unlock request to Bulwark Service to release the lock for the second request.

> **Note**
>
> If CONCURRENCY.N15.CREATE.ALLOW_ON_SERVICE_FAILURE is true and the request is allowed to be processed further even after exhausting the retries, the response could be 201 Success.

Two AM-Delete requests for same Subscriber and retry success

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-236 Two AM-Delete requests for same Subscriber and retry success



In this case, only concurrency is enabled for AM Delete. AM Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. AM Service receives an AM Delete request from AMF.
2. AM Service sends a lock request to Bulwark Service based on the configuration of RESOURCEID.SUFFIXLIST.

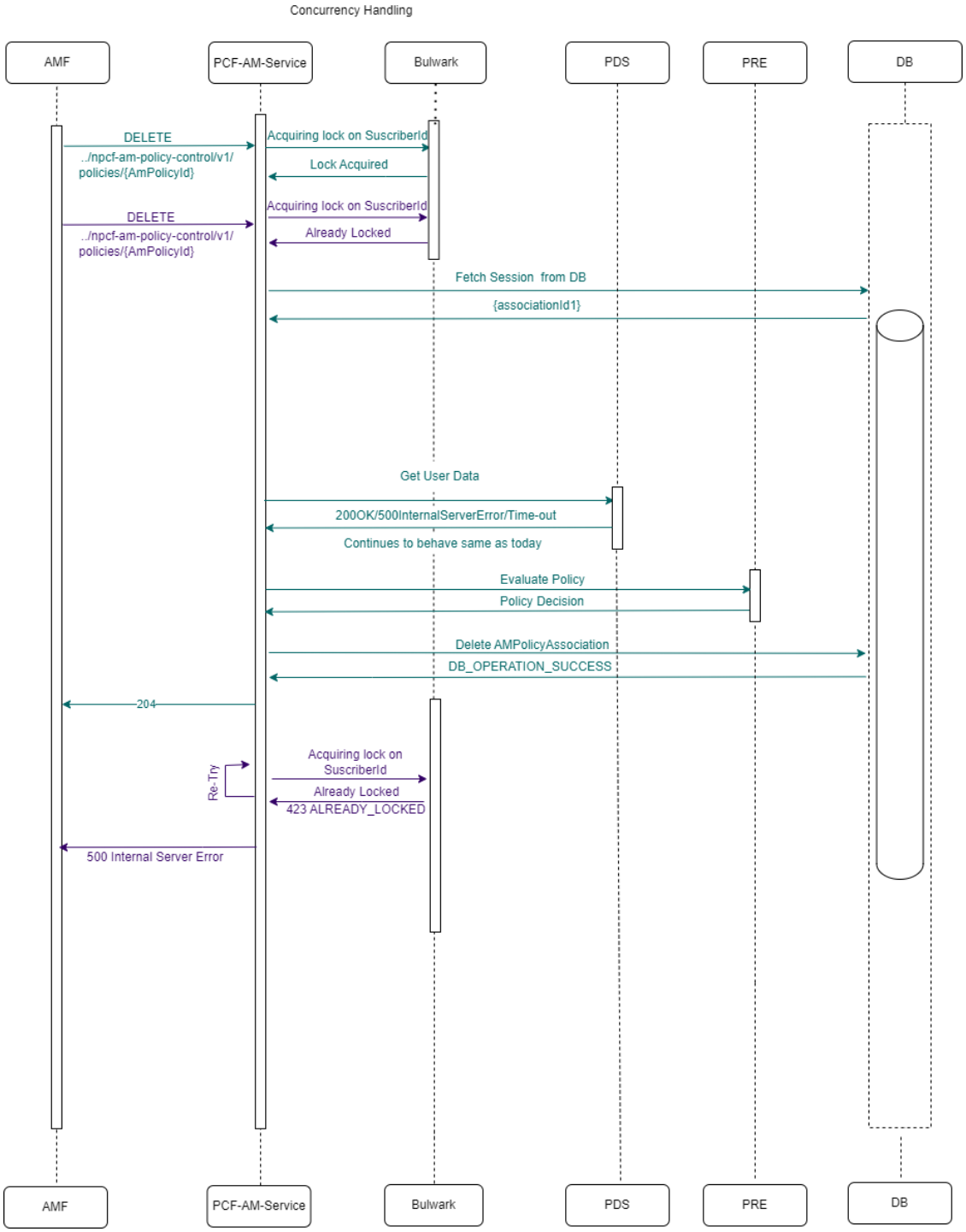
Copyright © 2019, 2026, Oracle and/or its affiliates.

3. AM Service acquires a lock from Bulwark Service.
4. AM Service fetches the session details from the database and sends the delete request to PDS.
5. AM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. AM policy association is deleted in the database.
7. After the successful completion of the delete, AM Service sends a unlock release request to Bulwark Service to release the lock.

Two AM-Delete requests for same Subscriber and retry failure (retry =1, CONCURRENCY.N15.TERMINATE.ALLOW_ON_SERVICE_FAILURE = false)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-237 Two AM-Delete requests for same Subscriber and retry failure (retry =1, CONCURRENCY.N15.TERMINATE.ALLOW_ON_SERVICE_FAILURE = false)



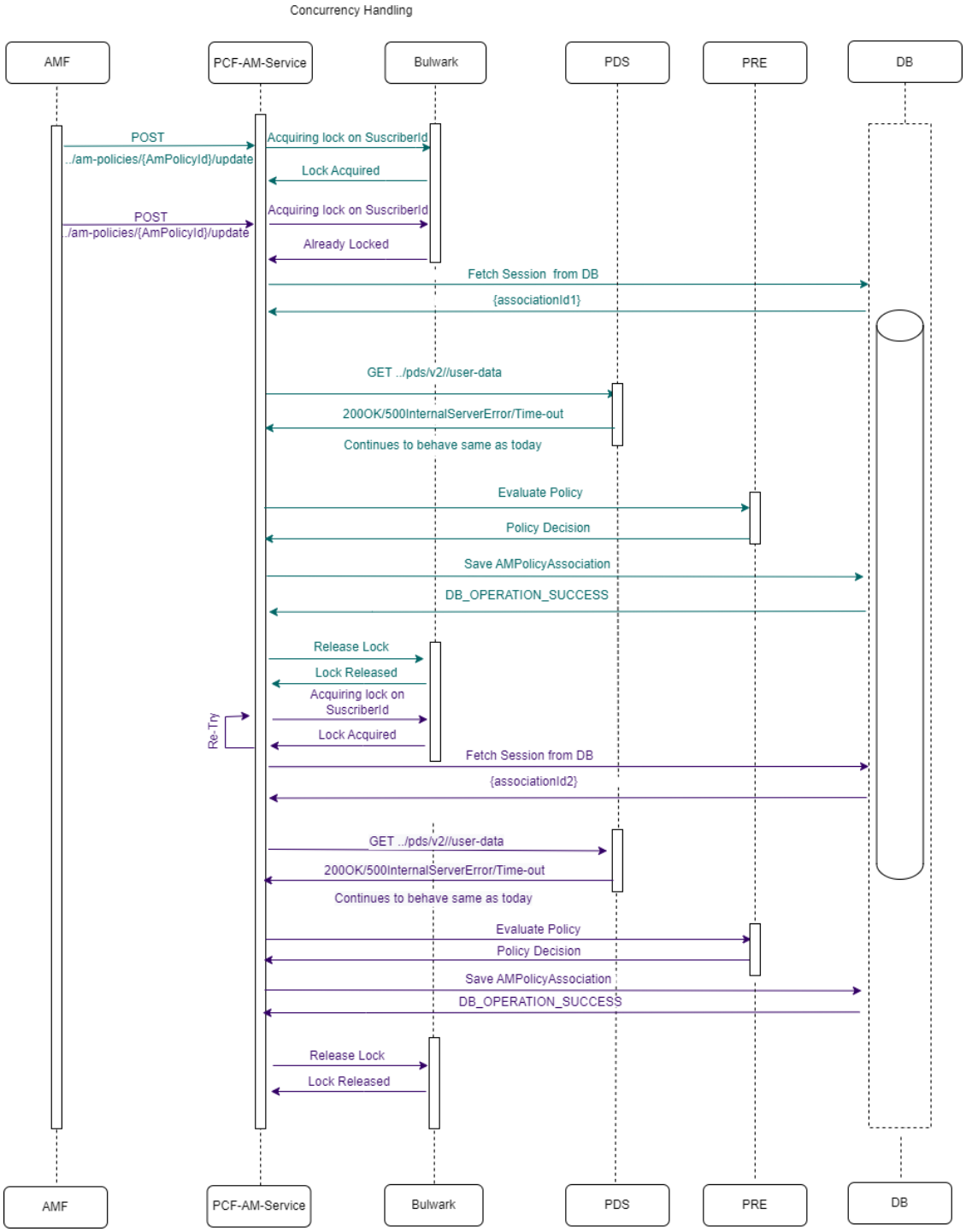
Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> If CONCURRENCY.N15.TERMINATE.ALLOW_ON_SERVICE_FAILURE is true and the request is allowed to be processed further even after exhausting the retries, the response could be 201 Success.

Two AM-Update requests for same Subscriber but different Sessions and retry success

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-238 Two AM-Update requests for same Subscriber but different Sessions and retry success



In this case, only concurrency is enabled for AM Update. AM Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. AM Service receives an AM Update request from AMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

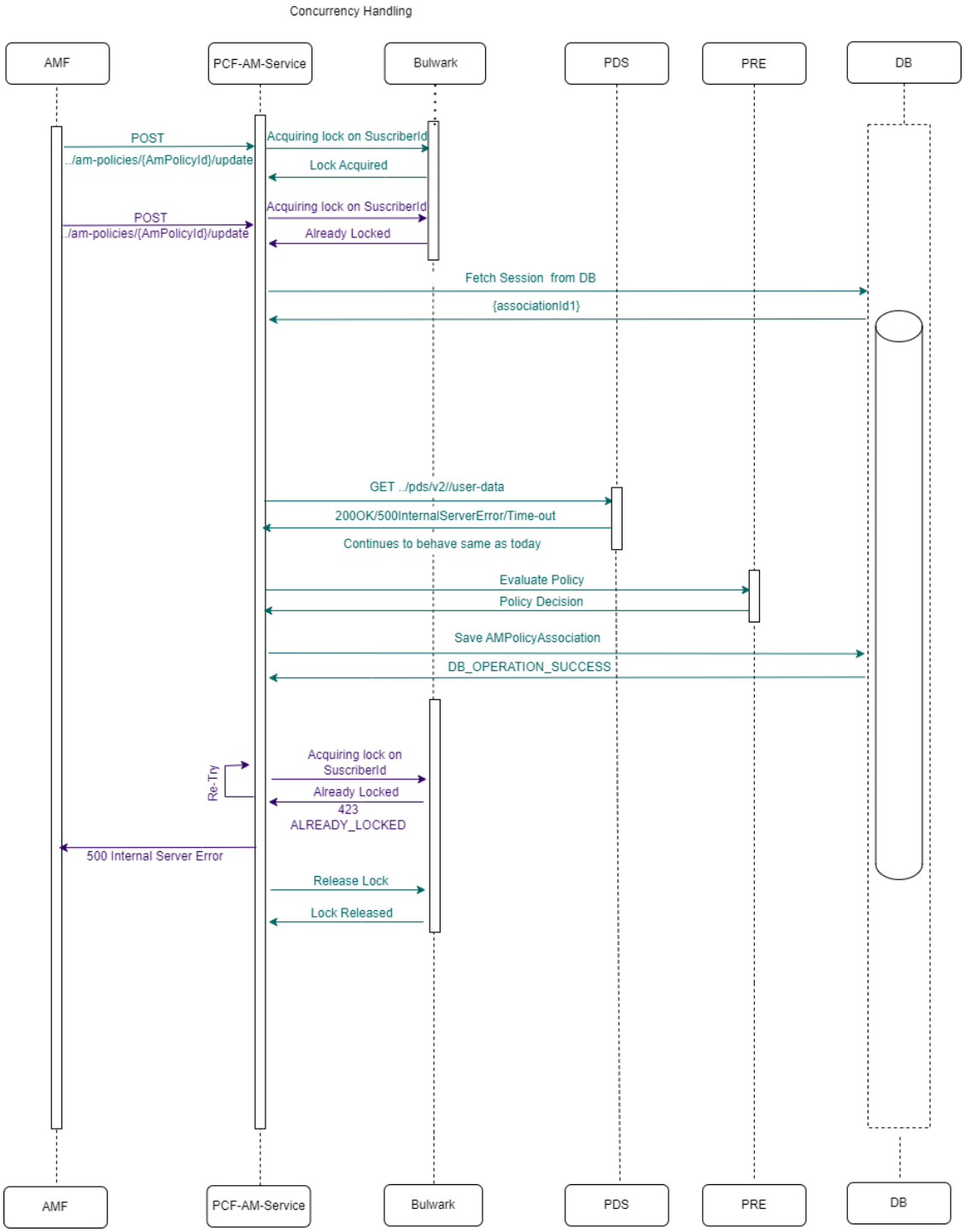
2. AM Service sends a lock request to Bulwark Service based on the configuration of RESOURCEID.SUFFIXLIST.
3. AM Service acquires a lock from Bulwark Service.
4. AM Service fetches the session details from the database and sends the update request to PDS.
5. AM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. AM policy association is update in the database.
7. After the successful completion of the update, AM Service sends a unlock release request to Bulwark Service to release the lock.

Two AM-Update requests for same Subscriber but different Sessions and retry failure (retry =1, CONCURRENCY.N15.UPDATE.ALLOW_ON_SERVICE_FAILURE = false)

Figure 4-239 Two AM-Update requests for same Subscriber but different Sessions and retry failure (retry =1, CONCURRENCY.N15.UPDATE.ALLOW_ON_SERVICE_FAILURE =

Copyright © 2019, 2026, Oracle and/or its affiliates.

false)



Concurrency is enabled for AM Update. AM Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. AM Service receives the first AM Update request from AMF.
2. AM Service sends a lock request to Bulwark Service based on what is configured in RESOURCEID.SUFFIXLIST.
3. AM Service acquires a lock for first request from Bulwark Service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

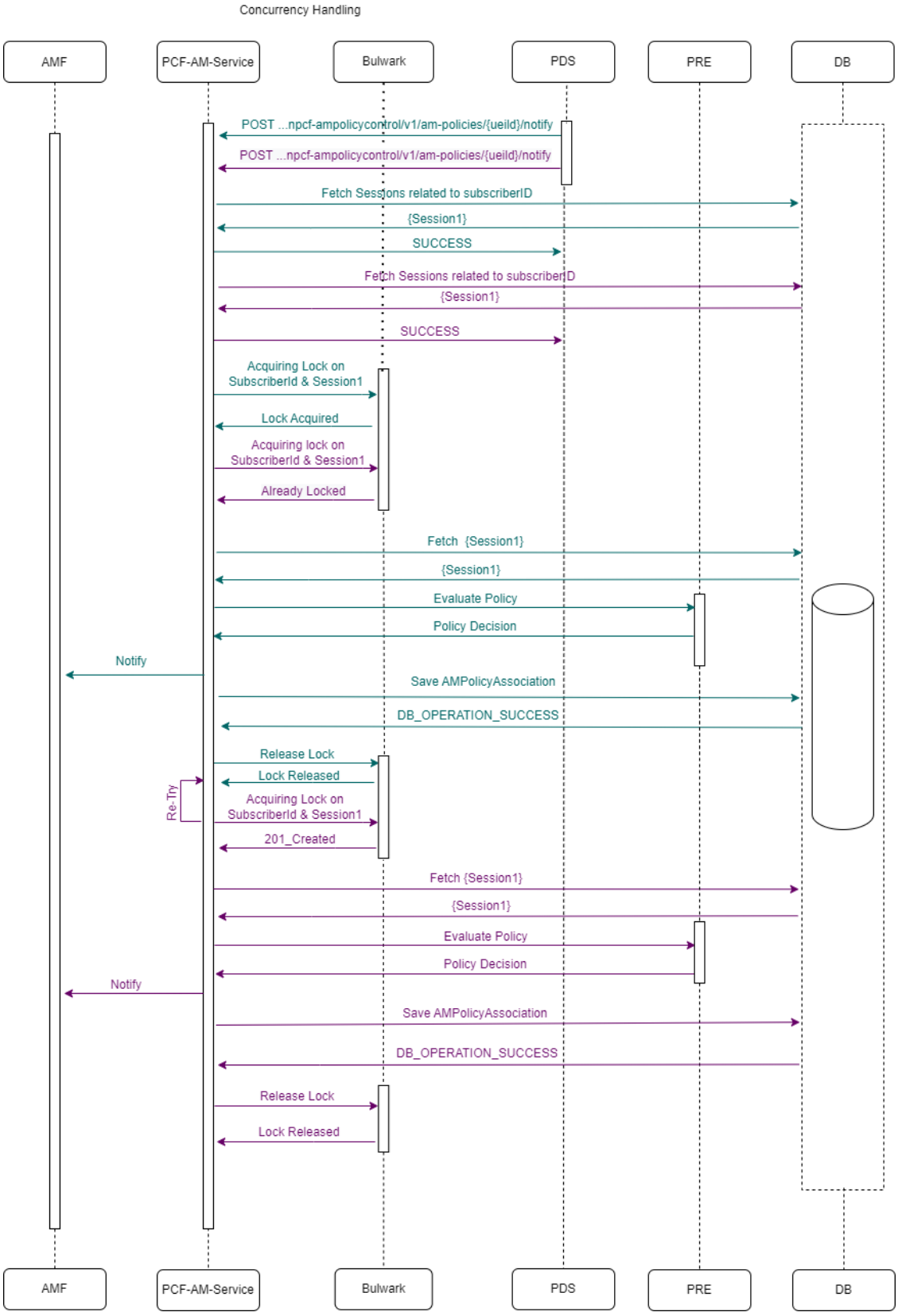
4. AM Service receives second AM Update request from AMF for the same subscriber.
5. AM Service sends a lock request to Bulwark Service for the second AM Update request.
6. Bulwark Service responds to AM Service for the second request with a 423 already locked message.
7. AM Service fetches the session details from the database for the first update request and sends the update request to PDS.
8. AM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
9. AM policy association is saved in the database.
10. After the successful completion of the request, AM Service sends a lock release request to Bulwark Service to release the lock for the first update request.
11. AM Service retries to acquire the lock for the second update request from Bulwark Service.
12. AM Service acquires a lock for the second update request, processes the update request.
13. After completing the update for the second request, AM Service sends an unlock request to Bulwark Service to release the lock for the second request.

> **Note**
>
> If CONCURRENCY.N15.UPDATE.ALLOW_ON_SERVICE_FAILURE is true and the request is allowed to be processed further even after exhausting the retries, the response could be 201 Success.

Two AM-Notify requests for same Subscriber each having 1 Session

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-240 Two AM-Notify requests for same Subscriber each having 1 Session



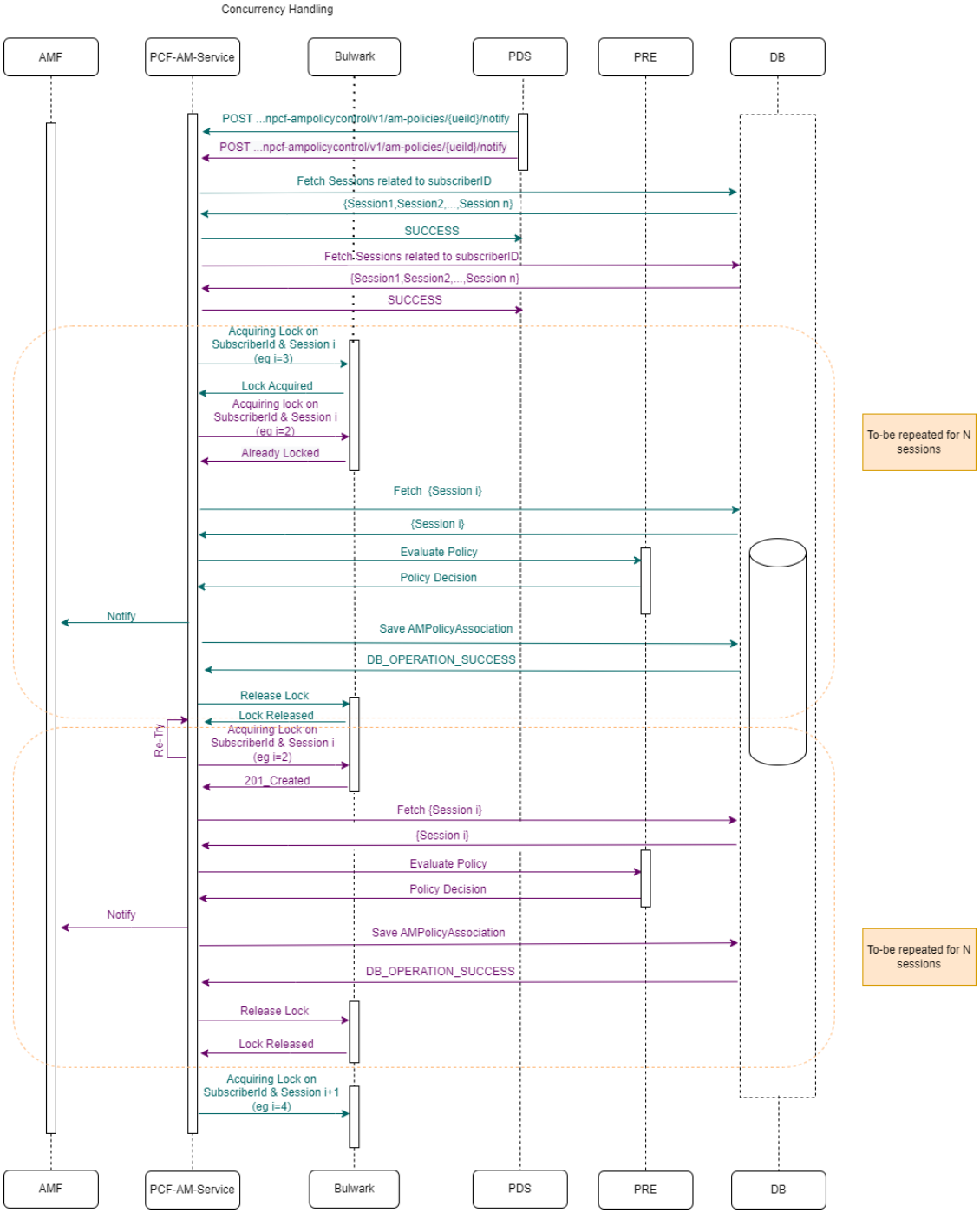
Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Notify request will be received at AM service from PDS.
2. AM service will fetch the Sessions related to the subscriber ID
3. AM will send request to Bulwark for lock acquisition. For lock acquisition, We will get Lock on subscriber ID & Session ID iteratively for **N** number of sessions.
4. Once the lock is acquired, AM service will again send a request to fetch sessions, in case it got updated.
5. Once we have the lock & updated sessions, AM service will re-auth all the sessions sequentially.
6. Then AMPolicyAssociation will be saved in DB.
7. If the DB update is success, AM service will ask for Releasing lock of Bulwark Service.
8. After lock is released successfully, the update-notify request will be success.

Two AM-Notify request for same Subscriber each having n Sessions

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-241 Two AM-Notify request for same Subscriber each having n Sessions



Concurrency is enabled for AM Notify. AM Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. PDS sends a notify request to AM service.
2. AM service fetches the corresponding sessions from database and sends a success response to PDS.
3. A notify request tries to acquire the lock from bulwark service and gets the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. The notify request starts processing by fetching each sessions one by one.
5. AM service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. AM policy association is saved in DB.
7. On successful save, a notify response is sent to AMF and the lock is released.
8. This process gets repeated for n sessions of the Notify request.

Managing Concurrency Handling for AM Service

Enable

You can enable the concurrency handling through Bulwark using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** Set value for the following parameters under the **Advanced Settings** section on the **PCF Access and Mobility** page:
  - CONCURRENCY.BULWARK_SERVICE_ENABLED
  - CONCURRENCY.N15.CREATE.ENABLED
  - CONCURRENCY.N15.CREATE.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.CREATE.LOCK_WAIT_DURATION
  - CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.TERMINATE.ENABLED
  - CONCURRENCY.N15.TERMINATE.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.TERMINATE.LOCK_WAIT_DURATION
  - CONCURRENCY.N15.UPDATE.ENABLED
  - CONCURRENCY.N15.UPDATE.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.UPDATE.LOCK_WAIT_DURATION
  - CONCURRENCY.N15.UPDATE_NOTIFY.ENABLED
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_WAIT_DURATION
  - RESOURCEID.SUFFIXLIST
  - ENABLE.ASSOCIATIONID.ENCODING
  - CONCURRENCY.N15.CREATE.ALLOW_ON_SERVICE_FAILURE
  - CONCURRENCY.N15.UPDATE.ALLOW_ON_SERVICE_FAILURE
  - CONCURRENCY.N15.UPDATE_NOTIFY.ALLOW_ON_SERVICE_FAILURE

Copyright © 2019, 2026, Oracle and/or its affiliates.

- CONCURRENCY.N15.TERMINATE.ALLOW_ON_SERVICE_FAILURE

> **Note**
>
> If you do not make these parameters as configurable, the AM service uses the default values for these parameters.

For more information about enabling the feature through CNC Console, see PCF Access and Mobility .

- **Enable using REST API:** Set the Keys and Values for **Advanced Settings** under PCF Session Management Service. For more information about enabling the feature through REST API, see "Access and Mobility Service" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the concurrency handling through Bulwark functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations under the **Advanced Settings** section on the **PCF Access and Mobility** page. For more information about configuring audit service, see PCF Access and Mobility.
- **Configure using REST API:**Set the Keys and Values for **Advanced Settings** under PCF Session Management Service. For more information about enabling the feature through REST API, see "Access and Mobility Service" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.123.3 Support for Concurrency Handling using Bulwark Service in UE

The Bulwark Service integrates with the UE service to handle the concurrent requests for the UE Create, UE Update, UE Delete, and UE Update-Notify procedures. The UE service integration with Bulwark service handles the concurrent requests for the same subscriber in a concurrent and efficient manner.

In case of multiple create, update, or delete requests for the same subscriber, the UE service requests a lock for the SUPI or GPSI value from the Bulwark service. Once the lock is acquired, the UE create, UE Update, UE delete, or UE Update-Notify request is executed for the SUPI or GPSI value with which the lock is requested. After the successful completion of the requests, the UE service sends a request to release the lock to Bulwark.

As the notification is locked, pending transaction comes into picture.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and UE Update:

Table 4-177 Pending Transaction and Concurrency in UE Update

Pending Transaction	Concurrency in UE Update	Use-Case
Enabled	Disabled	Single Key - Session level lock will be acquired. Pending-transaction call flow would work.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-177 (Cont.) Pending Transaction and Concurrency in UE Update

Pending Transaction	Concurrency in UE Update	Use-Case
Disabled	Enabled	Single Key - Subscriber level lock will be acquired. Update-Notify call flow with concurrency would work.
Enabled	Enabled	Multi-Key - Session Level & Subscriber Level locks will be acquired.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and update-notify:

Table 4-178 Pending Transaction and Concurrency in UE Update-Notify

Pending Transaction	Concurrency in Update-Notify	Use-Case
Enabled	Disabled	Single Key - Session level lock will be acquired. Pending-transaction call flow would work.
Disabled	Enabled	Single Key - Subscriber level lock will be acquired. UE-Update call flow would work.
Enabled	Enabled	Multi-Key - Session Level & Subscriber Level locks will be acquired.

When Bulwark-Service is Enabled, the following scenarios can occur between pending transaction and UE Update and UE update-notify:

Table 4-179 Pending Transaction and Concurrency in UE Update as well as UE Update-Notify

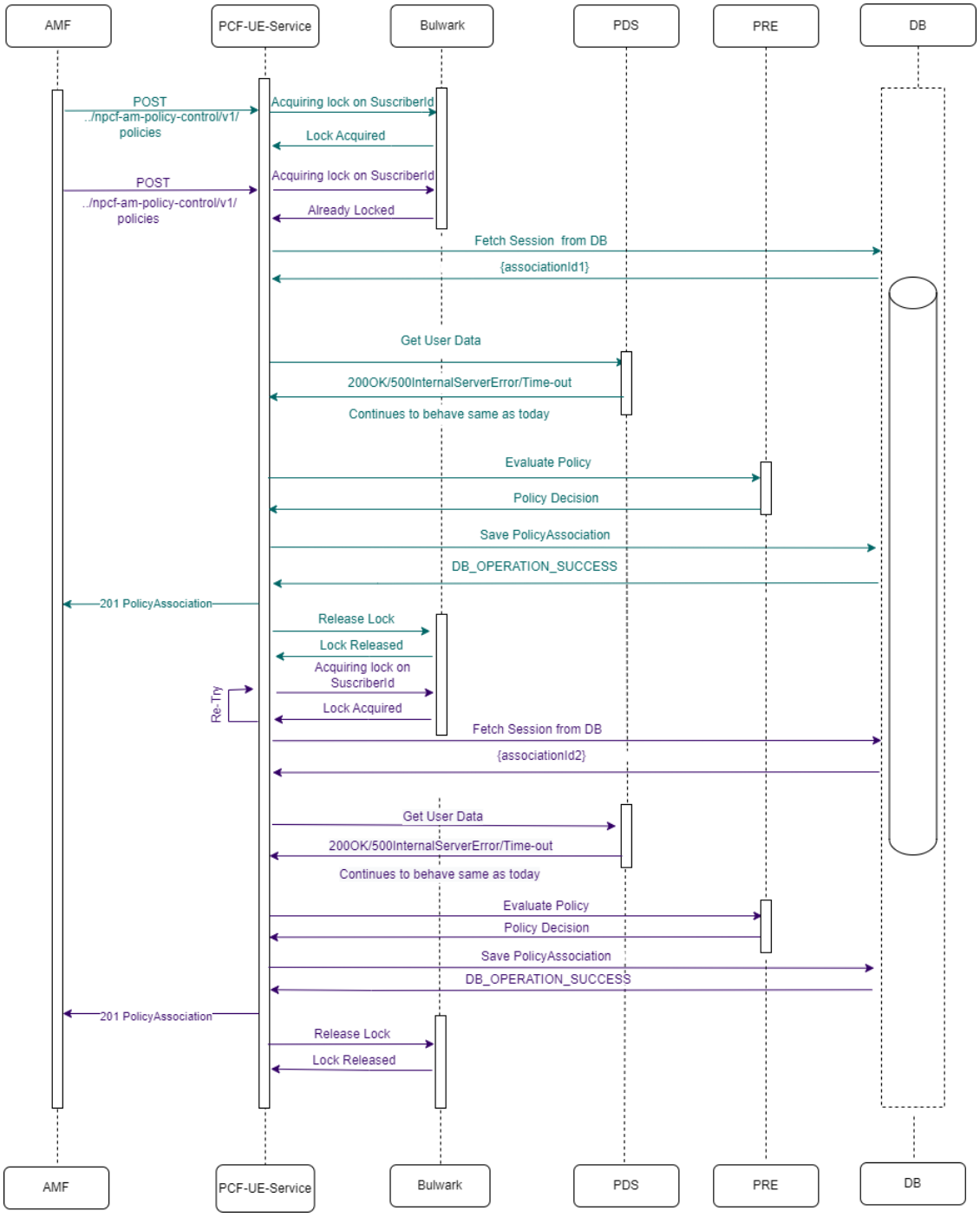
Pending Transaction	Concurrency in UE Update	Concurrency in UE Update-Notify	Use-Case
Enabled	Disabled	Disabled	Session Level Lock Acquired - during collision, lock acquisition fails at SessionID
Disabled	Enabled	Disabled	Subscriber Level lock acquired - during collision, lock acquisition fails at subscriberID
Disabled	Enabled	Enabled	Subscriber Level lock acquired - during collision, lock acquisition fails at subscriberID
Enabled	Enabled	Disabled	Session Level & Subscriber Level locks will be acquired - during collision, lock acquisition will fail at SessionID

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow for handling concurrent requests for UE Service

Two UE-Create requests for same Subscriber and retry success.

Figure 4-242 Two UE-Create requests for same Subscriber and retry success.



In this case, only concurrency is enabled for UE Create. UE Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

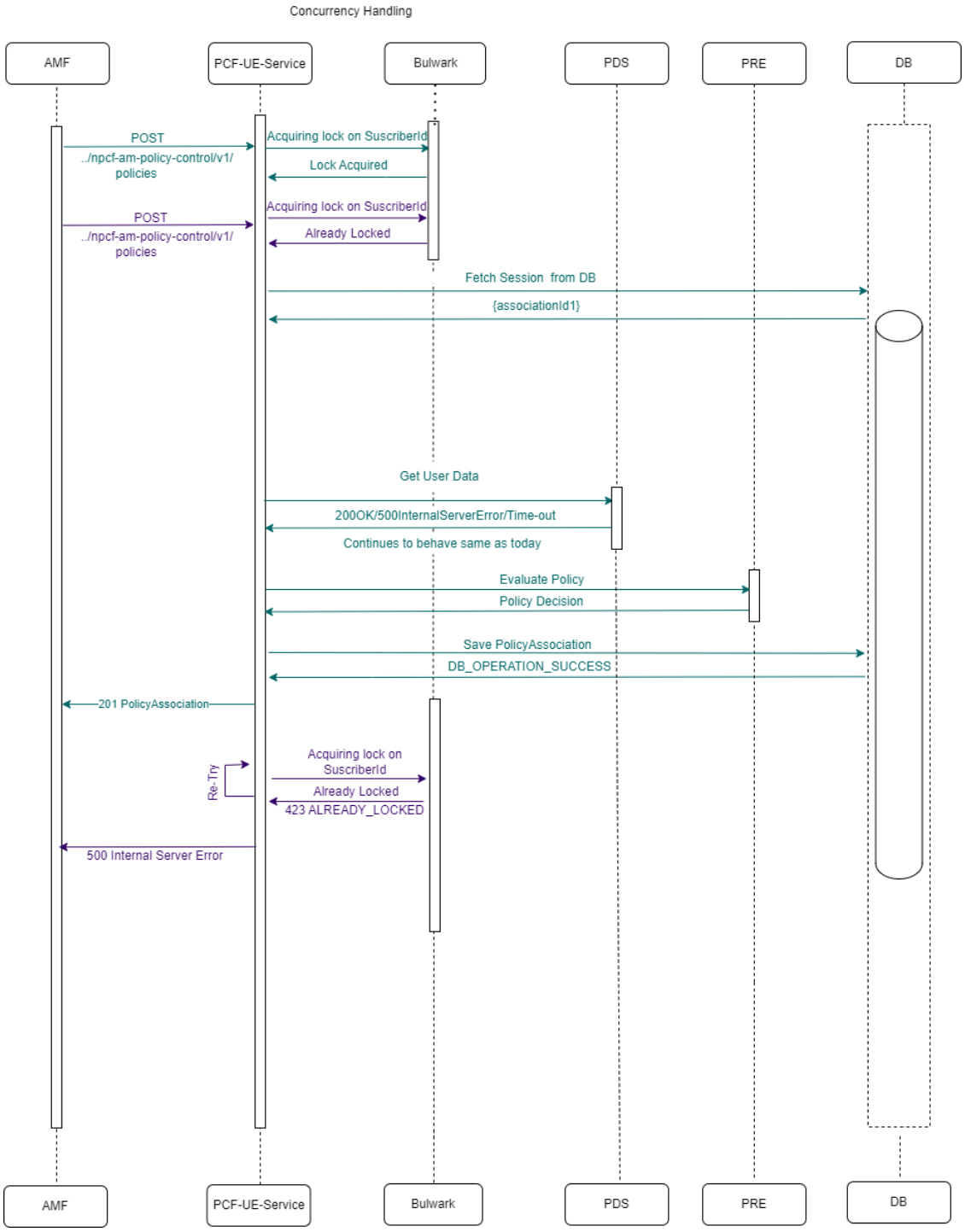
Copyright © 2019, 2026, Oracle and/or its affiliates.

1. UE Service receives an UE Create request from AMF.
2. UE Service sends a lock request to Bulwark Service based on the configuration of RESOURCEID.SUFFIXLIST.
3. UE Service acquires a lock from Bulwark Service.
4. UE Service fetches the session details from the database and sends the create request to PDS.
5. UE service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. UE policy association is saved in the database.
7. After the successful completion of the create, UE Service sends a unlock release request to Bulwark Service to release the lock.

Two UE-Create requests for same Subscriber and retry failure (retry =1)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-243 Two UE-Create requests for same Subscriber and retry failure (retry =1)



Concurrency is enabled for UE Create. UE Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. UE Service receives the first UE Create request from AMF.
2. UE Service sends a lock request to Bulwark Service based on what is configured in RESOURCEID.SUFFIXLIST.

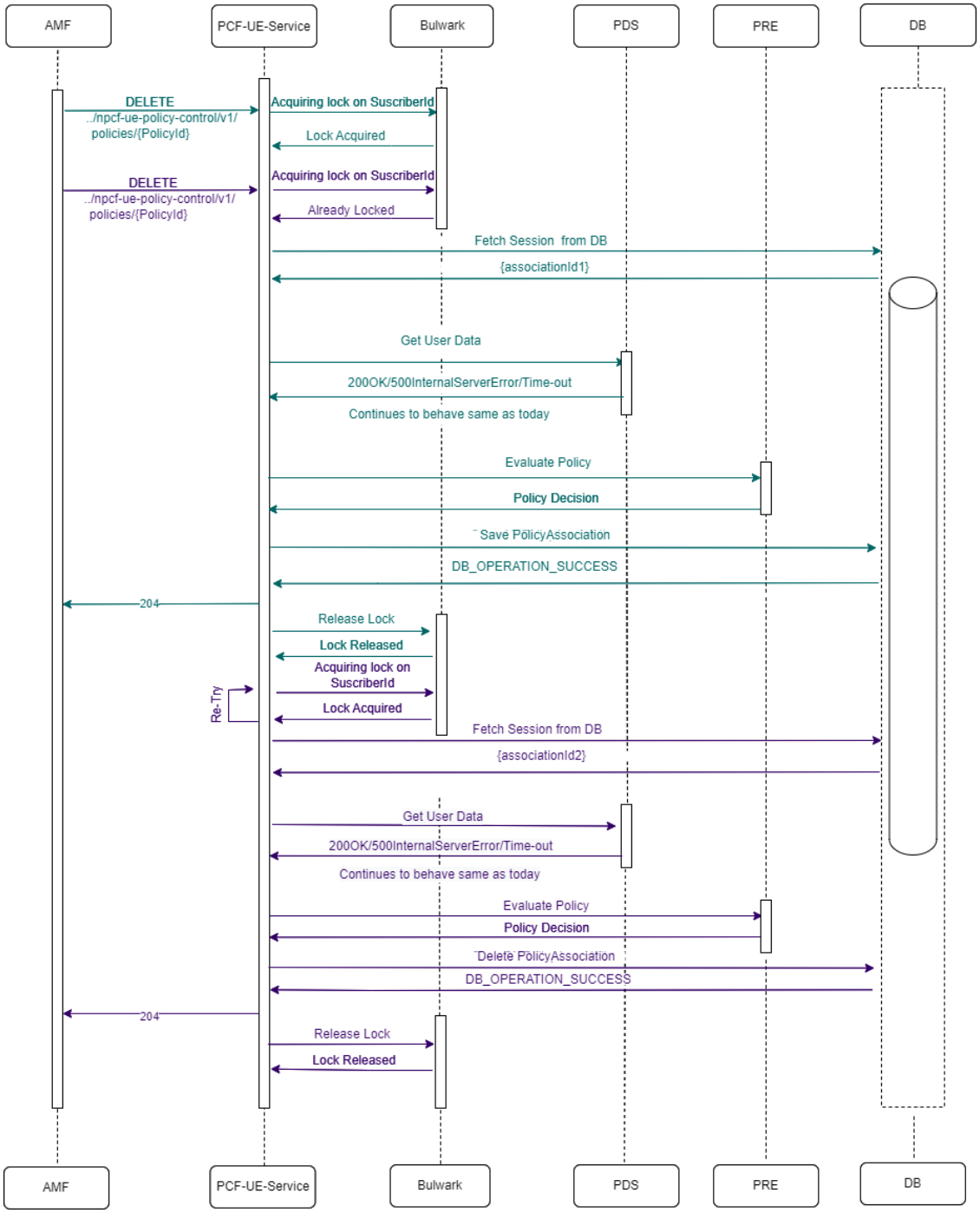
Copyright © 2019, 2026, Oracle and/or its affiliates.

3. UE Service acquires a lock for first request from Bulwark Service.
4. UE Service receives second UE Create request from AMF for the same subscriber.
5. UE Service sends a lock request to Bulwark Service for the second UE Create request.
6. Bulwark Service responds to UE Service for the second request with a 423 already locked message.
7. UE Service fetches the session details from the database for the first create request and sends the create request to PDS.
8. UE service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
9. UE policy association is saved in the database.
10. After the successful completion of the request, UE Service sends a lock release request to Bulwark Service to release the lock for the first create request.
11. UE Service retries to acquire the lock for the second create request from Bulwark Service.
12. UE Service acquires a lock for the second create request, processes the create request.
13. After completing the create for the second request, UE Service sends an unlock request to Bulwark Service to release the lock for the second request.

Two UE-Delete requests for same Subscriber and retry success.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-244 Two UE-Delete requests for same Subscriber and retry success.



In this case, only concurrency is enabled for UE Delete. UE Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. UE Service receives an UE Delete request from AMF.
2. UE Service sends a lock request to Bulwark Service based on the configuration of RESOURCEID.SUFFIXLIST.
3. UE Service acquires a lock from Bulwark Service.

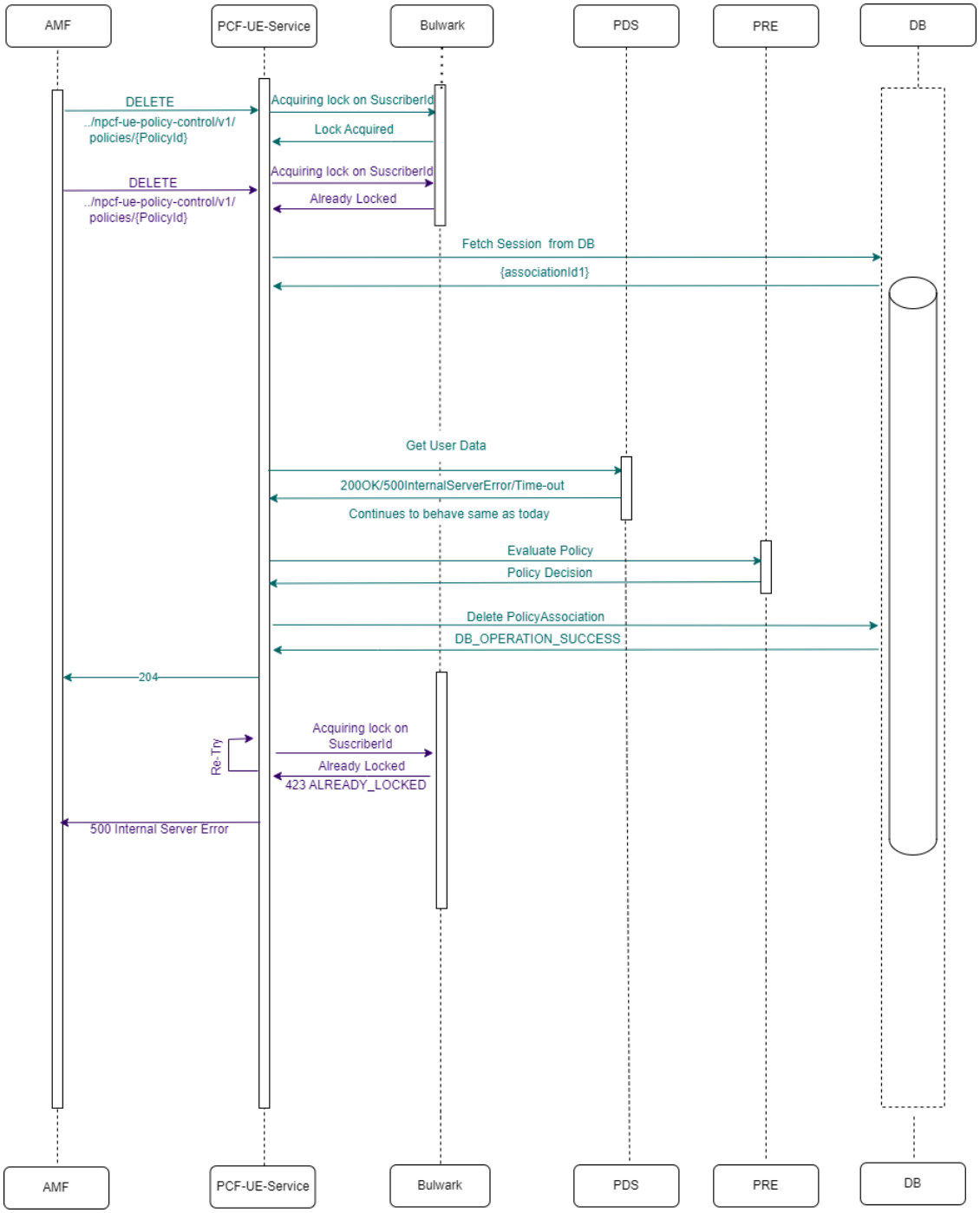
Copyright © 2019, 2026, Oracle and/or its affiliates.

4. UE Service fetches the session details from the database and sends the delete request to PDS.
5. UE service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. UE policy association is deleted in the database.
7. After the successful completion of the delete, UE Service sends a unlock release request to Bulwark Service to release the lock.

Two UE-Delete requests for same Subscriber and retry failure (retry =1)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-245 Two UE-Delete requests for same Subscriber and retry failure (retry =1)



Concurrency is enabled for UE Delete. UE Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. UE Service receives the first UE Delete request from AMF.
2. UE Service sends a lock request to Bulwark Service based on what is configured in RESOURCEID.SUFFIXLIST.
3. UE Service acquires a lock for first request from Bulwark Service.

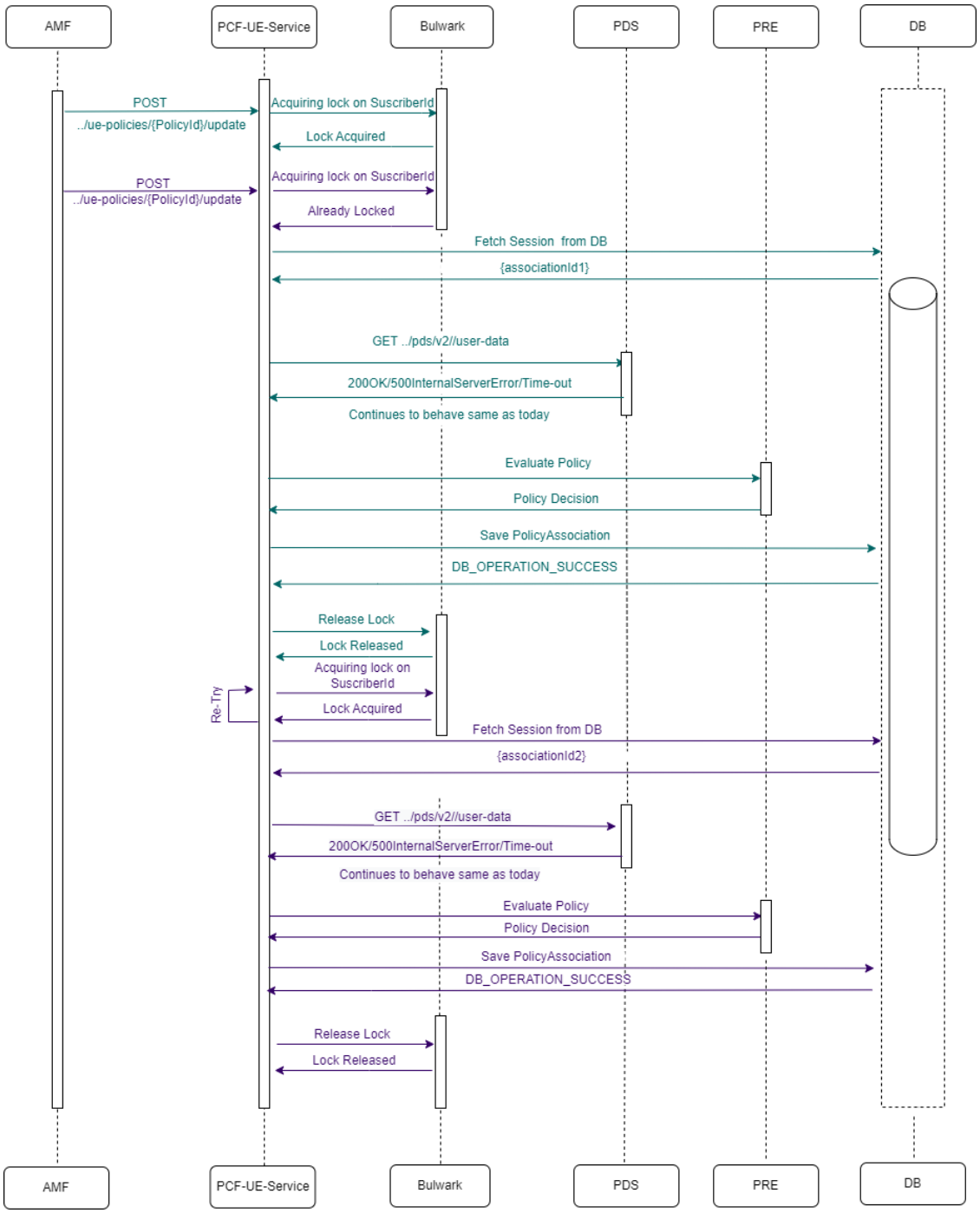
Copyright © 2019, 2026, Oracle and/or its affiliates.

4. UE Service receives second UE Delete request from AMF for the same subscriber.
5. UE Service sends a lock request to Bulwark Service for the second UE Delete request.
6. Bulwark Service responds to UE Service for the second request with a 423 already locked message.
7. UE Service fetches the session details from the database for the first delete request and sends the delete request to PDS.
8. UE service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
9. UE policy association is saved in the database.
10. After the successful completion of the request, UE Service sends a lock release request to Bulwark Service to release the lock for the first delete request.
11. UE Service retries to acquire the lock for the second delete request from Bulwark Service.
12. UE Service acquires a lock for the second delete request, processes the delete request.
13. After completing the delete for the second request, UE Service sends an unlock request to Bulwark Service to release the lock for the second request.

Two UE-Update requests for same Subscriber but different Sessions and retry success.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-246 Two UE-Update requests for same Subscriber but different Sessions and retry success.



In this case, only concurrency is enabled for UE Update. UE Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. UE Service receives an UE Update request from AMF.
2. UE Service sends a lock request to Bulwark Service based on the configuration of RESOURCEID.SUFFIXLIST.
3. UE Service acquires a lock from Bulwark Service.

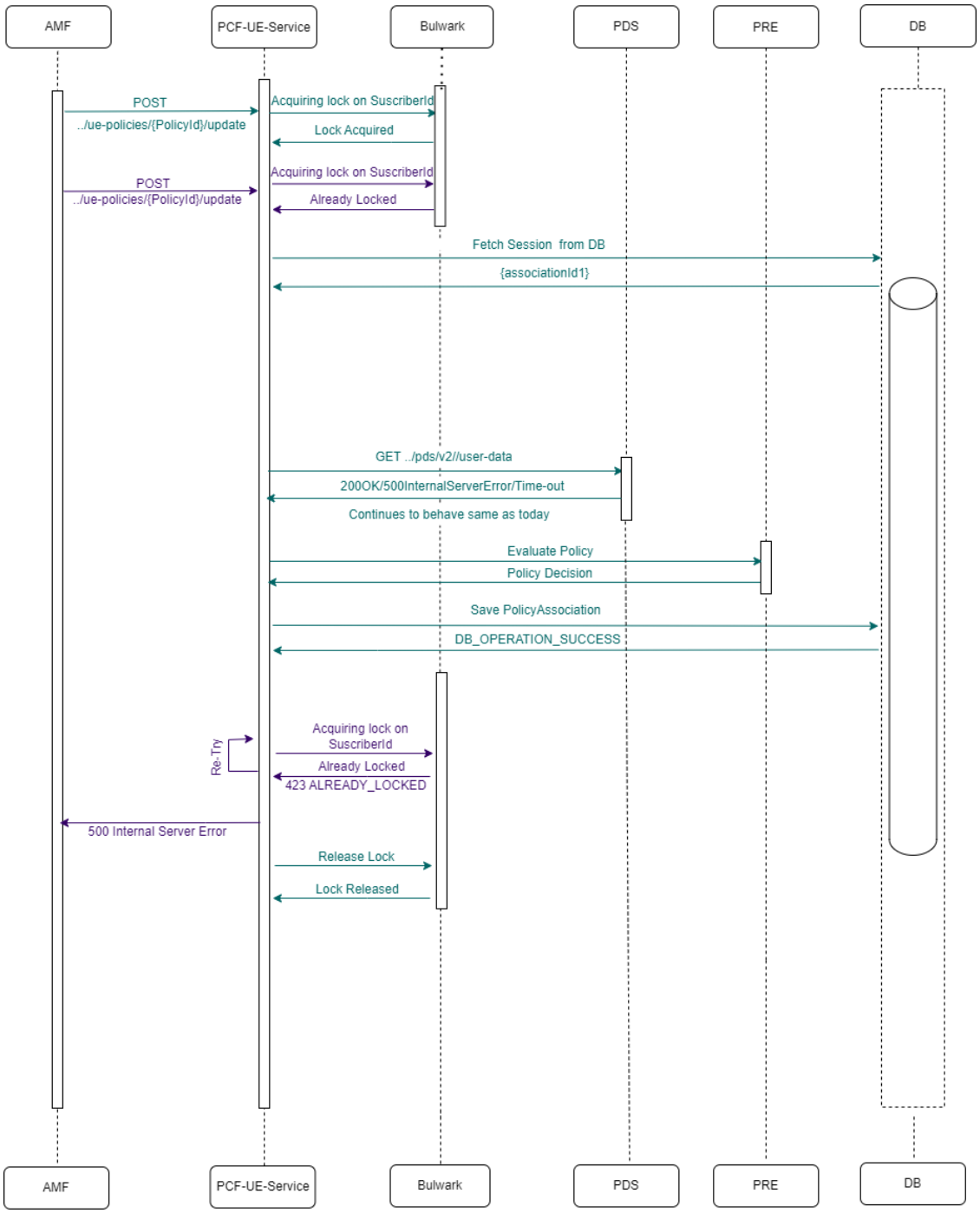
Copyright © 2019, 2026, Oracle and/or its affiliates.

4. UE Service fetches the session details from the database and sends the update request to PDS.
5. UE service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. UE policy association is update in the database.
7. After the successful completion of the update, AM Service sends a unlock release request to Bulwark Service to release the lock.

Two UE-Update requests for same Subscriber but different Sessions and retry failure (retry =1)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-247 Two UE-Update requests for same Subscriber but different Sessions and retry failure (retry =1)



Concurrency is enabled for UE Update. UE Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. UE Service receives the first UE Update request from AMF.
2. UE Service sends a lock request to Bulwark Service based on what is configured in RESOURCEID.SUFFIXLIST.
3. UE Service acquires a lock for first request from Bulwark Service.

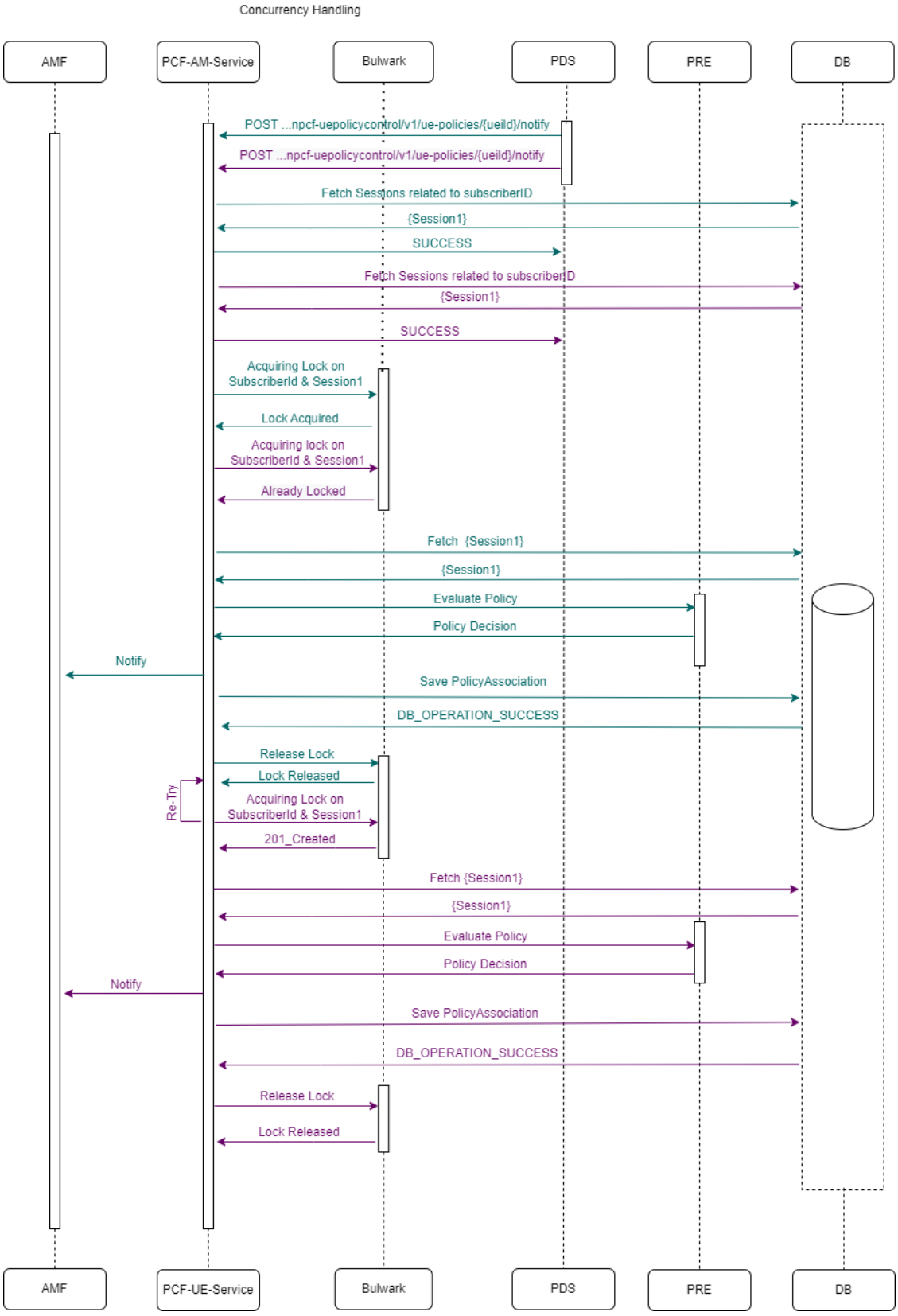
Copyright © 2019, 2026, Oracle and/or its affiliates.

4. UE Service receives second UE Update request from AMF for the same subscriber.
5. UE Service sends a lock request to Bulwark Service for the second UE Update request.
6. Bulwark Service responds to UE Service for the second request with a 423 already locked message.
7. UE Service fetches the session details from the database for the first update request and sends the update request to PDS.
8. UE service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
9. UE policy association is saved in the database.
10. After the successful completion of the request, UE Service sends a lock release request to Bulwark Service to release the lock for the first update request.
11. UE Service retries to acquire the lock for the second update request from Bulwark Service.
12. UE Service acquires a lock for the second update request, processes the update request.
13. After completing the update for the second request, UE Service sends an unlock request to Bulwark Service to release the lock for the second request.

Two UENotify requests for same Subscriber each having 1 session

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-248 Two UENotify requests for same Subscriber each having 1 session



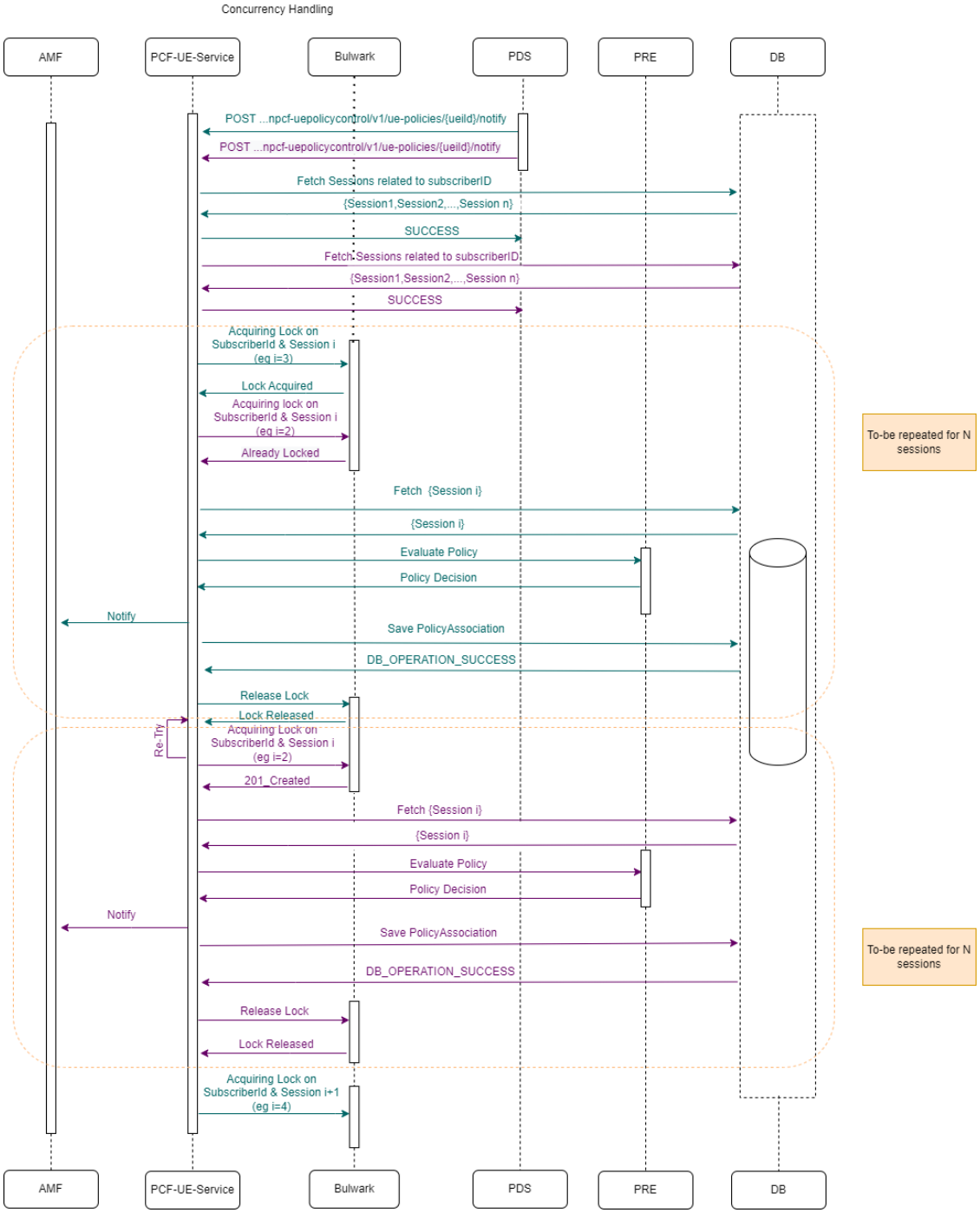
Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Notify request will be received at UE service from PDS.
2. UE service will fetch the Sessions related to the subscriber ID
3. UE will send request to Bulwark for lock acquisition. For lock acquisition, We will get Lock on subscriber ID & Session ID iteratively for **N** number of sessions.
4. Once the lock is acquired, UE service will again send a request to fetch sessions, in case it got updated.
5. Once we have the lock & updated sessions, UE service will re-auth all the sessions sequentially.
6. Then PolicyAssociation will be saved in DB.
7. If the DB update is success, UE service will ask for Releasing lock of Bulwark Service.
8. After lock is released successfully, the update-notify request will be success.

Two UENotify request for same Subscriber each having n sessions

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-249 Two UENotify request for same Subscriber each having n sessions



Concurrency is enabled for UE Notify. UE Service acquires a single key lock using what is configured in RESOURCEID.SUFFIXLIST as a default is SUPI.

1. PDS sends a notify request to UE service.
2. UE service fetches the corresponding sessions from database and sends a success response to PDS.
3. A notify request tries to acquire the lock from bulwark service and gets the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. The notify request starts processing by fetching each sessions one by one.
5. UE service sends a request to PRE for policy evaluation. PRE, in turn replies with the Policy Decision.
6. UE policy association is saved in DB.
7. On successful save, a notify response is sent to AMF and the lock is released.
8. This process gets repeated for n sessions of the Notify request.

Managing Concurrency Handling for UE Service

Enable

You can enable the concurrency handling through Bulwark using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** Set value for the following parameters under the **Advanced Settings** section on the **PCF UE Policy Service** page:
  - CONCURRENCY.BULWARK_SERVICE_ENABLED
  - CONCURRENCY.N15.CREATE.ENABLED
  - CONCURRENCY.N15.CREATE.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.CREATE.LOCK_WAIT_DURATION
  - CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.TERMINATE.ENABLED
  - CONCURRENCY.N15.TERMINATE.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.TERMINATE.LOCK_WAIT_DURATION
  - CONCURRENCY.N15.UPDATE.ENABLED
  - CONCURRENCY.N15.UPDATE.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.UPDATE.LOCK_WAIT_DURATION
  - CONCURRENCY.N15.UPDATE_NOTIFY.ENABLED
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_LEASE_DURATION
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_BACKOFF
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_COUNT
  - CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_WAIT_DURATION
  - RESOURCEID.SUFFIXLIST

> **Note**
>
> If you do not make these parameters as configurable, the UE service uses the default values for these parameters.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more information about enabling the feature through CNC Console, see PCF UE Policy Service .

- **Enable using REST API:** Set the Keys and Values for **Advanced Settings** under PCF Session Management Service. For more information about enabling the feature through REST API, see "UE Policy" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the concurrency handling through Bulwark functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations under the **Advanced Settings** section on the **PCF UE Policy Service** page. For more information about configuring audit service, see PCF UE Policy Service.
- **Configure using REST API:**Set the Keys and Values for **Advanced Settings** under PCF Session Management Service. For more information about enabling the feature through REST API, see "UE Policy" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.123.4 Support for Concurrency Handling using Bulwark Service in PCRF

PCRF-core supports the Bulwark service to handle the concurrent messages on Gx interface. PCRF-core interacts with Bulwark service using of lock/unlock message exchanges acquiring and releasing the User-IDs based lock upon receiving CCR-I/U-T messages.

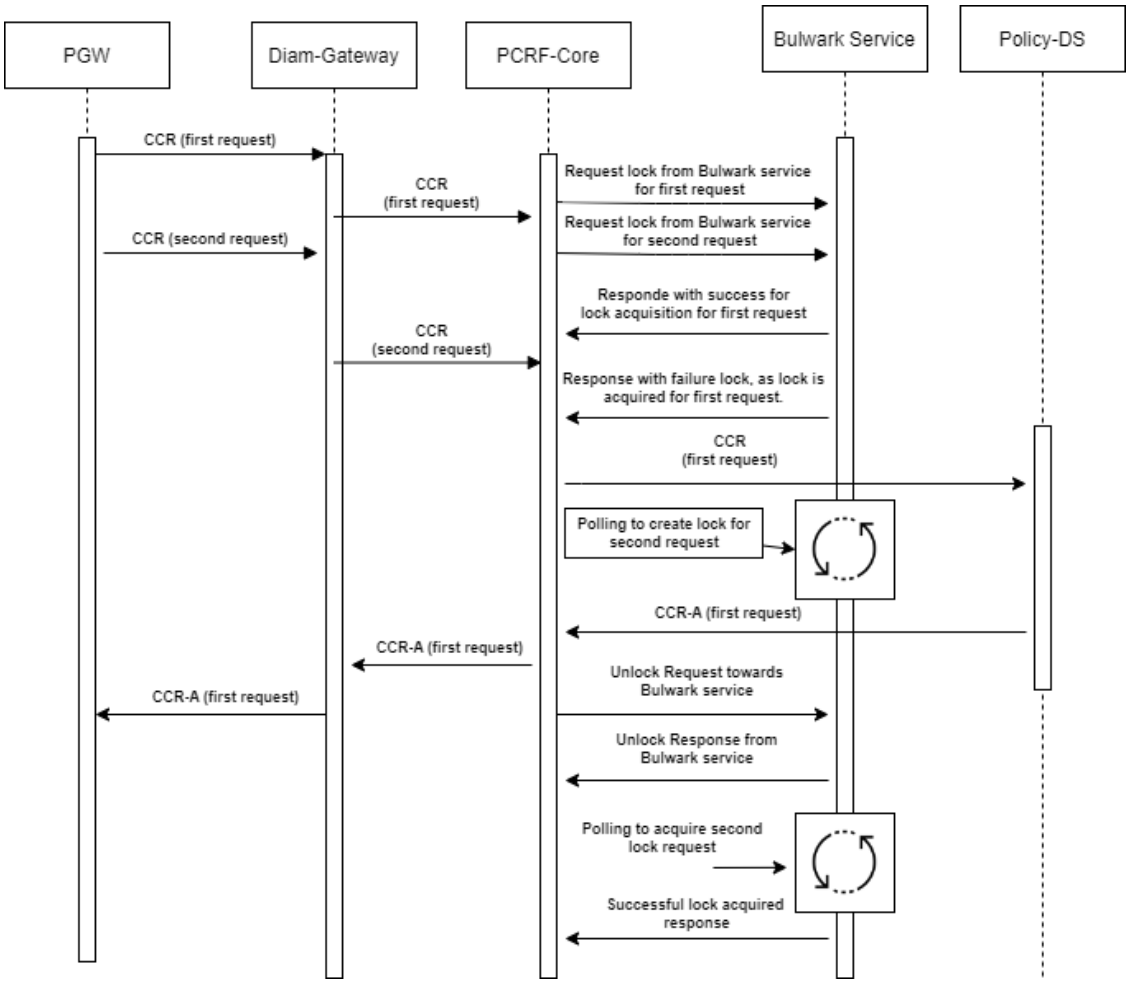
The PCRF-core sends the following parameters to request a lock:

- **Key:** The key is the identifier value with which the lock is identified. You can select either SUPI or GPSI value to be the key parameter for which the lock acquisition request must be made. By default, SUPI values are used for lock requests.
- **Lease Duration:** This value defines the duration for which lock is kept once the acquisition is successful. After this duration, the lock will be released automatically.
- **Lock Wait Timeout:** This defines the duration by which the Policy services wait for the response to get a lock. The same duration is used by Bulwark to poll for the lock in case the lock is not available. The Lock Wait timeout is also considered as the polling interval which sends the request towards Bulwark service periodically to acquire the lock for another create or delete request.
- **Retry Count:** This defines the count of retry attempts that are made by the Policy services if a lock request fails. In case all the retry attempts fail, the create or delete request is rejected. By default, 3 retry attempts are enabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow- CCR-I, CCR-U and CCR-T messages Integration with Bulwark Service

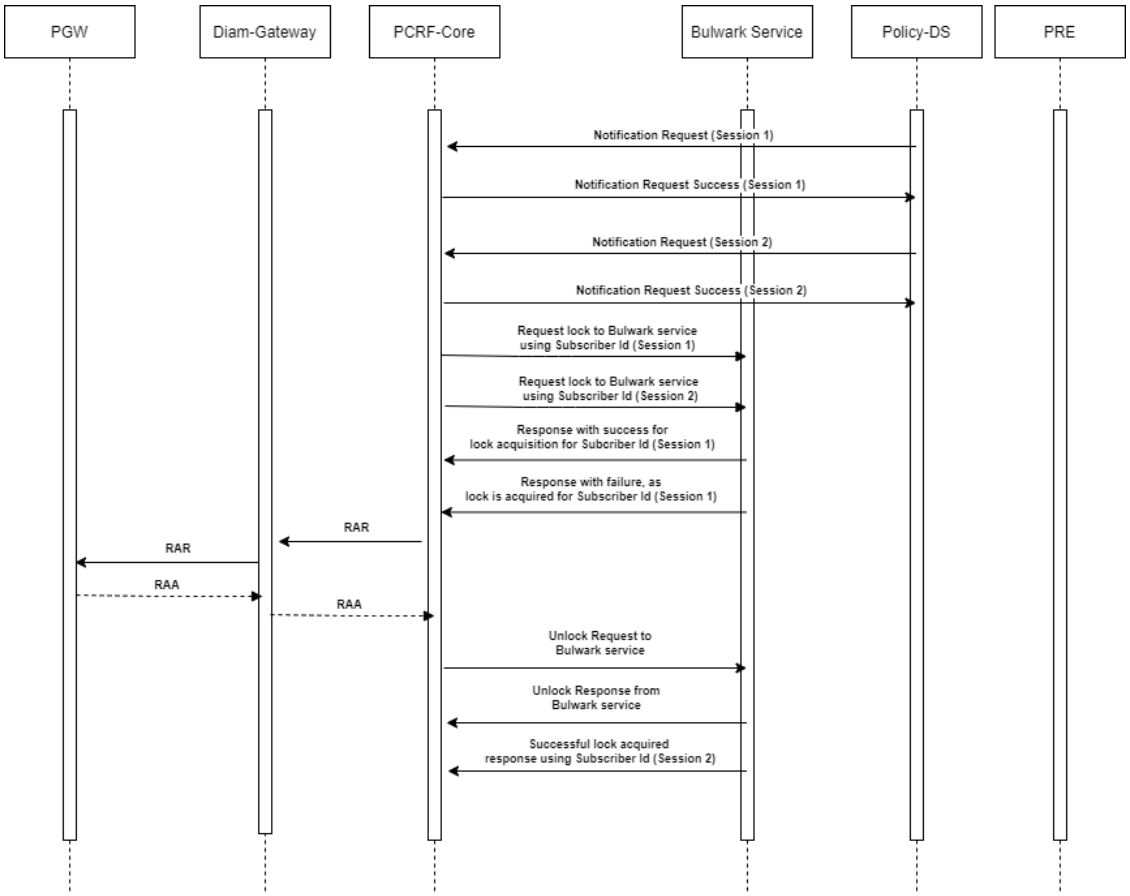
Figure 4-250 CCR-I, CCR-U and CCR-T messages Integration with Bulwark Service



Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow- PDS notification (RAR) Integration with Bulwark Service

Figure 4-251 Call Flow- PDS notification (RAR) Integration with Bulwark Service



Managing Concurrency Handling for PCRF-core

Enable

You can enable the concurrency handling for PCRF-Core using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** Set the keys and values of the following keys under the **Advanced Settings** section on the **PCRF Core Settings** page:

Table 4-180 General

Key	Value
CONCURRENCY.ENABLED	true/false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-181 List of Keys for Gx CCR-I

Key	Default Value
CONCURRENCY.GX.CREATE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.GX.CREATE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.CREATE.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.CREATE.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.CREATE.ENABLED	True
CONCURRENCY.GX.CREATE.ALLOW_ON_SERVICE_FAILURE	True

Table 4-182 List of Keys for Gx CCR-U

Key	Default Value
CONCURRENCY.GX.MODIFY.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.GX.MODIFY.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.MODIFY.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.MODIFY.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.MODIFY.ENABLED	True
CONCURRENCY.GX.MODIFY.ALLOW_ON_SERVICE_FAILURE	True

Table 4-183 List of Keys for Gx CCR-T

Key	Default Value
CONCURRENCY.GX.DELETE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.GX.DELETE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.DELETE.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.DELETE.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.DELETE.ENABLED	True
CONCURRENCY.GX.DELETE.ALLOW_ON_SERVICE_FAILURE	True

Table 4-184 List of Keys for Gx RAR

Key	Defualt Value
CONCURRENCY.GX.REAUTH.LOCK_REQUEST_RETRY_COUNT	2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-184 (Cont.) List of Keys for Gx RAR

Key	Defualt Value
CONCURRENCY.GX.REAUTH.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.REAUTH.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.REAUTH.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.REAUTH.ENABLED	True
CONCURRENCY.GX.REAUTH.ALLOW_ON_SERVICE_FAILURE	True

Table 4-185 List of Keys for SD Create

Key	Default Value
CONCURRENCY.SD.CREATE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.SD.CREATE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.SD.CREATE.LOCK_LEASE_DURATION	2000
CONCURRENCY.SD.CREATE.LOCK_WAIT_DURATION	3000
CONCURRENCY.SD.CREATE.ENABLED	True
CONCURRENCY.SD.CREATE.ALLOW_ON_SERVICE_FAILURE	True

Table 4-186 List of Keys for Rx AAR-I

Key	Default Value
CONCURRENCY.RX.CREATE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.RX.CREATE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.RX.CREATE.LOCK_LEASE_DURATION	2000
CONCURRENCY.RX.CREATE.LOCK_WAIT_DURATION	3000
CONCURRENCY.RX.CREATE.ENABLED	true
CONCURRENCY.RX.CREATE.ALLOW_ON_SERVICE_FAILURE	true

Table 4-187 List of Keys for Rx AAR-U

Key	Default Value
CONCURRENCY.RX.MODIFY.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.RX.MODIFY.LOCK_REQUEST_RETRY_BACKOFF	1000

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-187 (Cont.) List of Keys for Rx AAR-U

Key	Default Value
CONCURRENCY.RX.MODIFY.LOCK_LEASE_DURATION	2000
CONCURRENCY.RX.MODIFY.LOCK_WAIT_DURATION	3000
CONCURRENCY.RX.MODIFY.ENABLED	true
CONCURRENCY.RX.MODIFY.ALLOW_ON_SERVICE_FAILURE	true

Table 4-188 List of Keys for Rx STR

Key	Default Value
CONCURRENCY.RX.DELETE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.RX.DELETE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.RX.DELETE.LOCK_LEASE_DURATION	2000
CONCURRENCY.RX.DELETE.LOCK_WAIT_DURATION	3000
CONCURRENCY.RX.DELETE.ENABLED	true
CONCURRENCY.RX.DELETE.ALLOW_ON_SERVICE_FAILURE	true

Table 4-189 List of Keys for Additional Properties

Key	Default Value
bulwark.service.enabled	true
bulwark.service.http2.enabled	true
bulwark.service.url	http://10.75.241.7:30900/v1/locks
bulwark.service.connector.timeout	3000

For more information about enabling the feature through CNC Console, see Settings.

- **Enable using REST API:** Set the Keys and Values for **Advanced Settings** under PCRF Core Settings. For more information about enabling the feature through REST API, see "Core Services" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the concurrency handling for PDS Service using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations under the **Advanced Settings** section on the **PCRF Core Settings** page. For more information about the configuration, see Settings.
- **Configure using REST API:** Set the Keys and Values for **Advanced Settings** under PCRF Core Settings. For more information about enabling the feature through REST API, see "Core Services" section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observe

PCRF-Core provides the following metrics specific to concurrency handling in PCRF:

- occnp_http_bulwark_lock_request_total
- occnp_http_bulwark_lock_response_total
- occnp_http_bulwark_unlock_request_total
- occnp_http_bulwark_unlock_response_total

For more details on metrics, see PCRF Core Metrics.

4.123.5 Support for Concurrency Handling using Bulwark Service in PDS

When PDS receives concurrent notification requests for a subscriber (same SUPI or GPSI) of the same data source, processing multiple notification requests at the same time can result in inaccurate data.

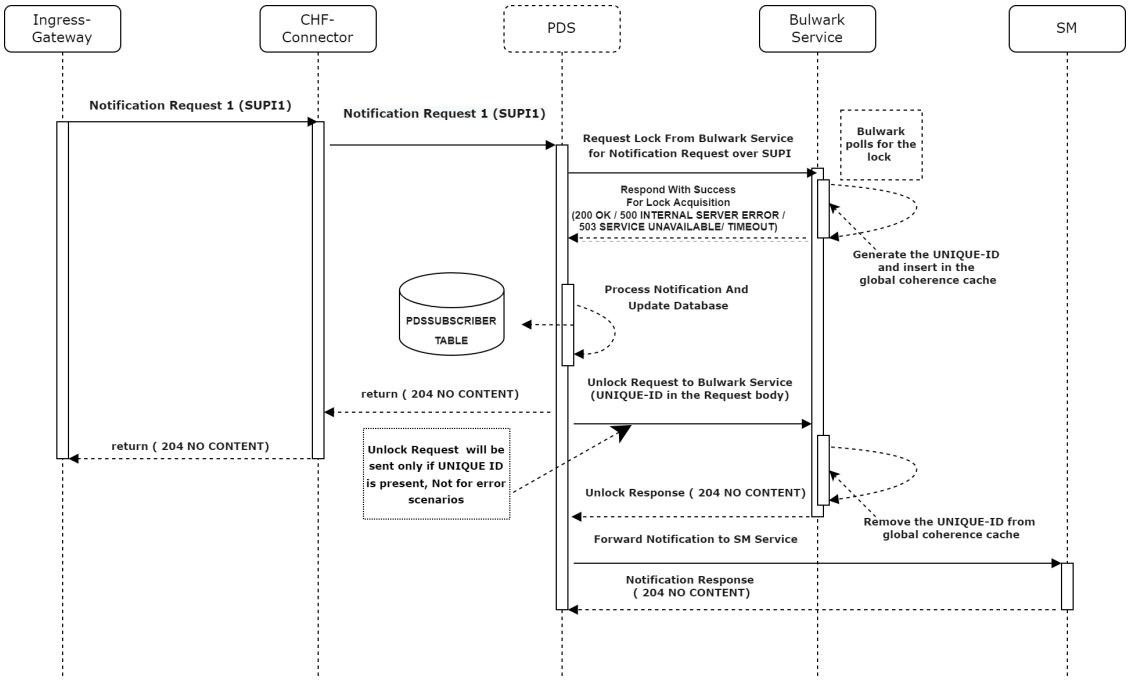
To avoid this issue, PDS is integrated with Bulwark Service. Bulwark Service provides lock and unlock mechanism over a SUPI or GPSI key and allows processing of only one notification at a time.

When PDS service receives multiple notifications from UDR, CHF or OCS, PDS requests for a lock to Bulwark service by calling the lock API service. Bulwark service approves lock for one request at a time. The other services retry to get the lock..

Once the lock is acquired, PDS service processes the notification for the SUPI or GPSI value with which the lock is requested. After the message is completed, PDS service sends a release lock request to Bulwark to release the lock.

Call Flow for Handling concurrent requests for PDS service

Figure 4-252 Call Flow - Bulwark Lock Request For CHF Notification



Copyright © 2019, 2026, Oracle and/or its affiliates.

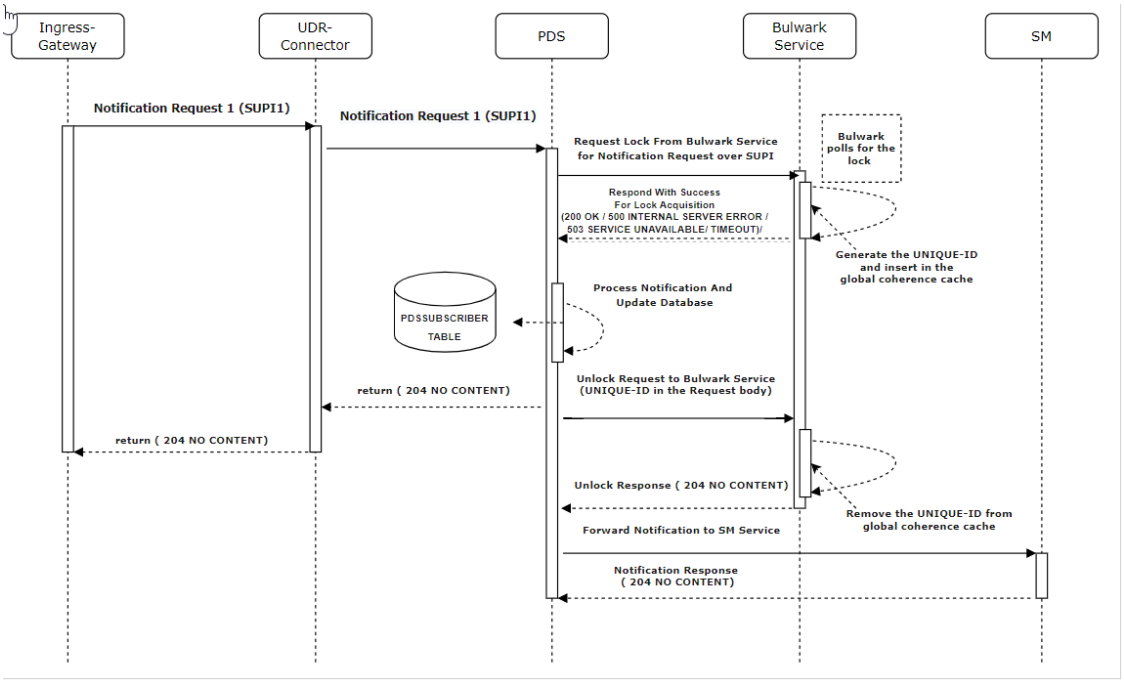
To enable the concurrency handling for CHF notifications, set the value of CONCURRENCY.BULWARK_ENABLED_FOR_CHF_NOTIFICATION to true.

In the above example, PDS receives notification request for SUPI1 from CHF through Ingress Gateway, CHF Connector.

1. PDS queries the PDS Subscriber table to fetch the SUPI or GPSI for the given sySessionID, based on CONCURRENCY.LOCK_REQUEST_KEY_TYPE_FOR_CHF_NOTIFICATION configuration in PDS Advanced Settings page.
2. PDS sends a lock request to Bulwark Service to acquire a lock for notification request over SUPI1.
3. Bulwark Service polls for the lock.
4. If the lock acquisition is successful:
    a. Bulwark Service generates a UniqueID for the lock and updates the same in the global coherence cache.
    b. Bulwark Service responds to PDS with 200 ok message.
    c. After PDS completes processing the notification request, it sends an Unlock request to Bulwark Service with the UniqueID in request parameters.
    d. Bulwark Service removes the UniqueID from the global coherence cache and responds to PDS with a 204 no content message.
    e. PDS forwards the notification request to core services and receives a response.
    f. If the lease duration expires before the processing of the notification request is complete, Bulwark Services releases the lock.
5. If the lock acquisition fails, PDS receives an error from Bulwark Service. If the same error code is configured in BULWARK_ERROR_CODES in PDS, PDS rejects the notification and responds with a 500 message to CHF connector. If the error code is not configured in BULWARK_ERROR_CODES, PDS continues to process the notification without the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-253 Call Flow - Bulwark Lock Request For UDR Notification



To enable the concurrency handling for UDR notifications, set the value of CONCURRENCY.BULWARK_ENABLED_FOR_UDR_NOTIFICATION to true.

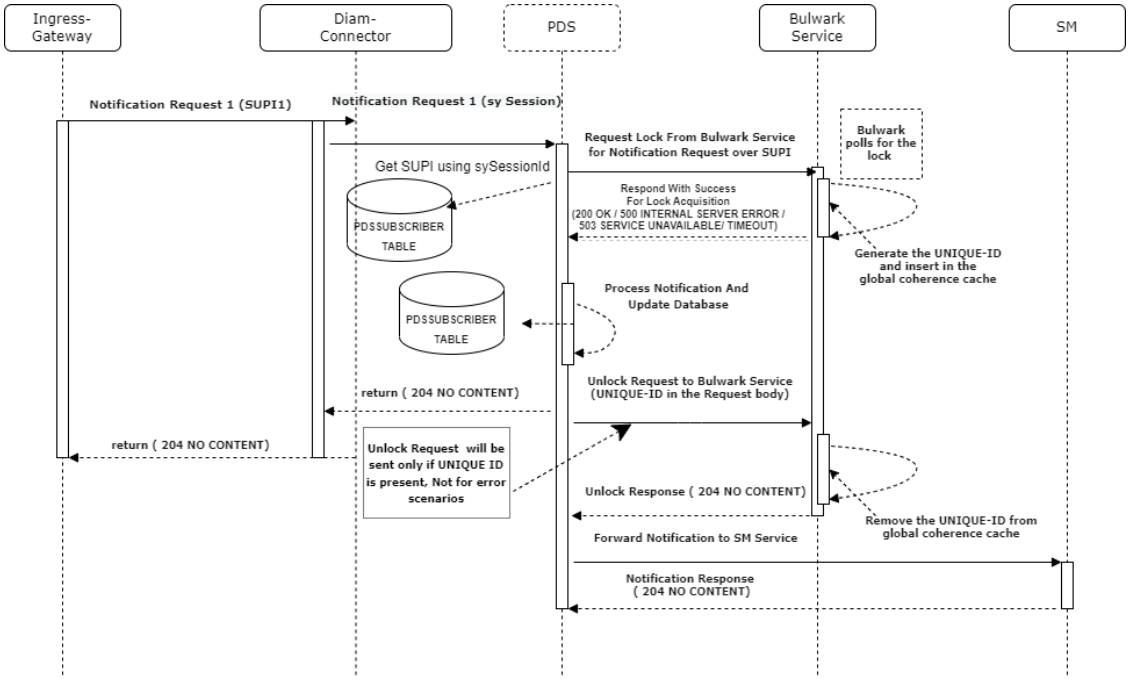
In the above example, PDS receives notification request for SUPI1 from UDR through Ingress Gateway, UDR Connector.

1. PDS queries the PDS Subscriber table to fetch the SUPI or GPSI for the given sySessionID, based on CONCURRENCY.LOCK_REQUEST_KEY_TYPE_FOR_UDR_NOTIFICATION configuration in PDS Advanced Settings page.
2. PDS sends a lock request to Bulwark Service to acquire a lock for notification request over SUPI1.
3. Bulwark Service polls for the lock.
4. If the lock acquisition is successful:
   a. Bulwark Service generates a UniqueID for the lock and updates the same in the global coherence cache.
   b. Bulwark Service responds to PDS with 200 ok message.
   c. After PDS completes processing the notification request, it sends an Unlock request to Bulwark Service with the UniqueID in request parameters.
   d. Bulwark Service removes the UniqueID from the global coherence cache and responds to PDS with a 204 no content message.
   e. PDS forwards the notification request to core services and receives a response.
   f. If the lease duration expires before the processing of the notification request is complete, Bulwark Services releases the lock.
5. If the lock acquisition fails, PDS receives an error from Bulwark Service. If the same error code is configured in BULWARK_ERROR_CODES in PDS, PDS rejects the notification

Copyright © 2019, 2026, Oracle and/or its affiliates.

and responds with a 500 message to UDR connector. If the error code is not configured in BULWARK_ERROR_CODES, PDS continues to process the notification without the lock.

Figure 4-254 Call Flow - Bulwark Lock Request For OCS Notification



To enable the concurrency handling for OCS notifications, set the value of CONCURRENCY.BULWARK_ENABLED_FOR_OCS_NOTIFICATION to true.

In the above example, PDS receives notification request for Sy Session from OCS through Ingress Gateway, Diameter Connector.

1. PDS queries the PDS Subscriber table to fetch the SUPI or GPSI for the given sySessionID, based on CONCURRENCY.LOCK_REQUEST_KEY_TYPE_FOR_OCS_NOTIFICATION configuration in PDS Advanced Settings page. .
2. PDS sends a lock request to Bulwark Service to acquire a lock for notification request over SUPI1.
3. Bulwark Service polls for the lock.
4. If the lock acquisition is successful:
   a. Bulwark Service generates a UniqueID for the lock and updates the same in the global coherence cache.
   b. Bulwark Service responds to PDS with 200 ok message.
   c. After PDS completes processing the notification request, it sends an Unlock request to Bulwark Service with the UniqueID in request parameters.
   d. Bulwark Service removes the UniqueID from the global coherence cache and responds to PDS with a 204 no content message.
   e. PDS forwards the notification request to core service and receives a response.
   f. If the lease duration expires before the processing of the notification request is complete, Bulwark Services releases the lock.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. If the lock acquisition fails, PDS receives an error from Bulwark Service. If the same error code is configured in BULWARK_ERROR_CODES in PDS, PDS rejects the notification and responds with a 500 message to OCS. If the error code is not configured in BULWARK_ERROR_CODES, PDS continues to process the notification without the lock.

Managing Concurrency Handling for PDS Service

Enable

You can enable the concurrency handling for PDS Service using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** Set value of the following keys to true under the **Advanced Settings** section on the **PDS Settings** page:
  - CONCURRENCY.BULWARK_ENABLED_FOR_CHF_NOTIFICATION
  - CONCURRENCY.BULWARK_ENABLED_FOR_OCS_NOTIFICATION
  - CONCURRENCY.BULWARK_ENABLED_FOR_UDR_NOTIFICATION

  Configuration of CONCURRENCY.BULWARK_ENABLED_FOR_CHF_NOTIFICATION, CONCURRENCY.BULWARK_ENABLED_FOR_OCS_NOTIFICATION and CONCURRENCY.BULWARK_ENABLED_FOR_UDR_NOTIFICATION are considered only if CONCURRENCY.BULWARK_ENABLED is set to true.

  CONCURRENCY.BULWARK_ENABLED is configured at the time of deployment.

  For more information about enabling the feature through CNC Console, see PDS Settings.
- **Enable using REST API:** Set the Keys and Values for **Advanced Settings** under PDS Settings. For more information about enabling the feature through REST API, see "PDS Settings" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the concurrency handling for PDS Service using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the feature configurations under the **Advanced Settings** section on the **PDS Settings** page. For more information about configuring audit service, see PDS Settings.
- **Configure using REST API:** Set the Keys and Values for **Advanced Settings** under PDS Settings. For more information about enabling the feature through REST API, see "PDS Settings" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observe

Policy provides the following metrics specific to concurrency handling for PDS call flows:

- server_request_total
- server_response_total

For more details on metrics, see Policy DS Metrics.

4.124 Support for Sd Interface in PCRF

Policy supports the Sd interface that enables it to communicate with the Traffic Detection Function (TDF). The Sd interface allows provisioning of the Application Detection and Control

Copyright © 2019, 2026, Oracle and/or its affiliates.

(ADC) rules from Policy for traffic detection and enforcement at the TDF through Solicited Application Reporting.

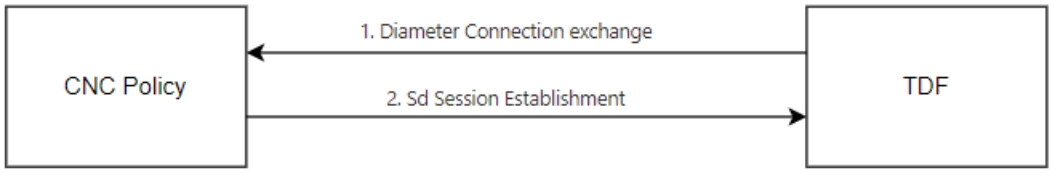
The Sd reference point exists between Policy and Charging Rules Function (PCRF) and a standalone TDF. Policy performs the following functionality for traffic detection through Sd interface:

- Establishment of session with TDF over Sd interface
- Termination of an existing TDF session
- Provisioning of ADC rules or decisions from for the purpose of traffic detection and enforcement at the TDF
- Reporting of the start and stop of detected applications and transfer of service data flow descriptions for detected applications, if available, from the TDF

The feature is supported for the Policy, PCRF, and the Converged Policy mode. It also supports the georedundant deployments of Policy.

The following diagram describes the session establishment between Policy and TDF:

Figure 4-255 TDF Session Establishment over Sd Interface



1. Policy acts as a diameter server for CER/CEA connection exchange. It accepts the diameter CER from TDF clients.

   > **Note**
   >
   > Policy supports the diameter CER only from the configured TDF clients.

   This establishes an Sd session as a result of IP-CAN (Gx) session establishment based on Policy action.
2. Policy sends a TDF-Session-Request (TSR) to the identified TDF in order to establish the session and provide the application detection information in the ADC rules. For more information, see 3GPP Technical specification, Release 16.4, Policy and Charging Control (PCC).

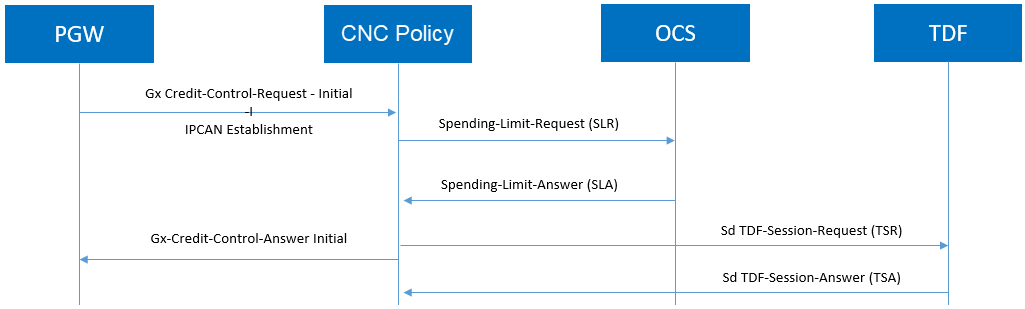
Call Flow

Call Flow for TDF Session

The following diagram shows a call flow between Policy and TDF through the asynchronous mode of communication between Gx and Sd interface:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-256 Call Flow for TDF Session



> **Note**
>
> Policy supports one Sd session per IPCAN Gx session to a RD. In case of multiple IPCAN, the new Sd Session is established to the same TDF for which the IPCAN session already exists. Multiple Sd sessions for the same Gx IPCAN session are not supported.

Managing Traffic Handling using Sd Interface

Enable

To enable the traffic handling through Sd interface functionality, Policy communicates with the OCS service. Therefore, it is required to enable the OCS Spending limit feature in PCRF-Core settings. You can enable OCS Spending limit using the CNC Console or REST API for Policy.

- **Enable using CNC Console:** Enable the OCS Spending limit functionality using the **OCS Spending Limit Attributes** on the **Settings** page for the PCRF Core service configurations. For more information about enabling the feature through CNC Console, see PCRF Core Service Configurations.
- **Enable using REST API:** Set values for the **ocsSpendingLimit.enable** parameter in the **Core Service** configuration API. For more information about enabling the feature through REST API, see "Core Service" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the traffic handling through Sd interface functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console:** Perform the following feature configurations using the CNC Console:
  - Set value for the TDF FQDN in the **Diameter Identity** parameter under the **PGW** section on the **Network Element** page. For more information about enabling the feature through CNC Console, see PGW.
  - Set the TDF service connection using the **Identity** parameter on the **Peer Nodes** page. For more information about enabling the feature through CNC Console, see Peer Nodes.
  - Set the TDF service connection using the **type** parameter on the **Peer Node Sets** page. For more information about enabling the feature through CNC Console, see Peer Node Sets.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Configure using REST API:** Policy provides the following REST API for traffic handling through Sd interface configuration:
  - Set values for the **neDiameterId** parameter in the **Network for PGW** configuration API. For more information about configuring the parameter through REST API, see "Network for PGW" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.
  - Set values for the **identity** parameter in the **Peer Nodes** configuration API. For more information about configuring the parameter through REST API, see "Peer Nodes" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.
  - Set values for the **type** parameter in the **Peer Node Sets** configuration API. For more information about configuring the parameter through REST API, see "Peer Node Sets" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

After the configurations, you can use the following blockly rules to establish traffic detection sessions with selected network element identity.

Policy supports the following blockly rules to create dynamic PCC Rules for the Sd interface:

- Establish traffic detection session with selected network element identity.
  The following screen capture shows a sample for the blockly:

Figure 4-257 Traffic Detection for Peer Node



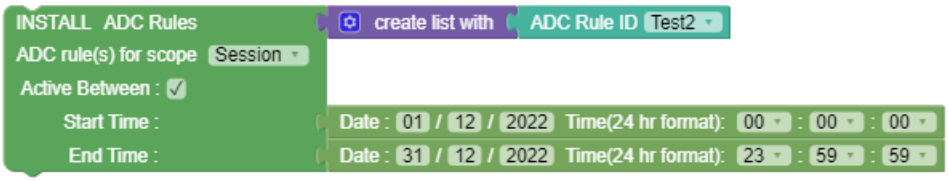
- Establish traffic detection session with selected Peer Node Set.
  The following screen capture shows a sample for the blockly:

Figure 4-258 Traffic Detection for Peer Node Sets



- Installation: To provision an ADC rule that has not been already provisioned. This blockly is used to install specified ADC rule(s) for selected scope active between the given start time and end time.
  The following screen capture shows a sample for the blockly:

Figure 4-259 Install with specified ADC Rules



Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> The Sd interface allows multiple rules to be installed with one ADC Charging Rule Install rule.

- Modification: To modify an installed ADC rule
- Removal: To remove an installed ADC rule
  The following screen captures show samples for the blockly:
  - To remove all ADC Rules

Figure 4-260 Remove all ADC Rules



  - To remove specified ADC Rules

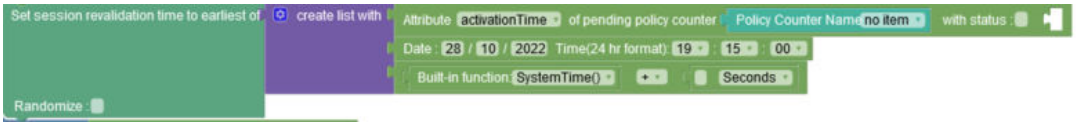
Figure 4-261 Remove specified ADC Rules



For more information, see "PCRF-Core Actions" in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

- Set Session Revalidation Time

Figure 4-262 Set Session Revalidation Time



Observe

Policy provides metrics specific to determine the successful TSR and RAR messages sent to TDF.

Policy provides TDF_CONNECTION_DOWN alert for this feature.

4.125 Support for Retrying Binding Registration on BSF and generating Alarm to Operator

The Retry Binding Registration on BSF feature enhances the binding registration functionality between SM Service and BSF. SM Service sends the binding registration requests to BSF through the Binding service. To manage the registration failure scenarios, Policy provides the Session Retry functionality. The Policy Binding service handles the Session Retry functionality and returns any of the following responses to the SM service:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Created without BSF Metadata:** The binding creation is successful in BSF
- **Failed with BSF Metadata:** The binding creation on BSF failed and the BSF metadata contains the problem Details of the failure. If the error code in the BSF Metadata does not match with the configured error code, it sends the termination notification in case the **Abort or Terminate** switch is enabled in SM configurations.
- **500 Internal Server Error:** An error occurred at the Binding service. It sends a termination notification if the **Abort or Terminate** flag is enabled in SM configurations

Starting with release 22.3.0, the Retry Binding Registration on BSF feature enhances the existing session retry mechanism by supporting multiple cycles of retry binding creation until a maximum number of attempts are reached or the response error code does not match with any of the configured error codes.

The following steps describes how PCF reattempts a binding request after receiving the failure response from BSF:

1. PCF sends a binding request to BSF and the initial request get failed.

   > **Note**
   >
   > When binding request to BSF fails, the binding service saves the binding context in its database and SM service is configured to reattempt after some time. During reattempt, SM service sends an update request so that a new request is sent to BSF instead of creating a new binding context.

2. PCF uses the Alternate Route Retry (ARR) functionality and sends the BSF registration requests to alternate BSFs.
3. In case all the session retry attempts configured in Policy fails, then Binding service returns to the SM service with the status code of the last binding request. The SM service evaluates if a recreate attempt must be triggered based on the following configurations:
   a. Recreate attempt feature is enabled
   b. Status code returned by Binding service matches with one of the error codes configured in the retry profile for BSF.

      > **Note**
      >
      > If no error codes have been configured in the retry profile for BSF, no recreate attempt is triggered.

   c. The maximum number of recreate attempts has not been reached. Based on the configurations, the SM service triggers the binding request after the duration configured through the BOT configuration is over.

      > **Note**
      >
      > The binding operation must be in asynchronous mode. For more information about configuration, see Managing Retrying Binding Registration on BSF.

4. If all the configurations are matched, then the SM service initiates a recreate attempt.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. In case of the failure of the recreate attempt, the SM service reattempts the requests for the number of times configured in the **Maximum Number of Attempts** parameter in the **Reattempts Profile**.
6. If all the recreate attempts get failed and the **Abort or Terminate Session on Binding Error** parameter value under the PCF Session Management configuration is set to **True**, then PCF sends the termination notification to the SMF. In case the parameter value is set to **False**, PCF does not terminate the SM session. For more information about configuration, see Managing Retrying Binding Registration on BSF .

> **Note**
>
> When the value of **Abort or Terminate Session on Binding Error** parameter is set to `true`, the binding session is deleted only if the error received on the request is NOT a timeout error.

Handling of Pending Operations by SM Service

The SM service maintains a record of the pending binding requests in the Pending Operations database table. For any binding create request failure, if the error response matches with the configured error codes, then SM service creates a record in the Pending Operations database table with the key details. The Pending Operations table can be configured using the **Audit** configurations of the **PCF Session Management** configurations.

Handling of Pending Operations by Audit Service

The Policy Audit service controls the notification flow for binding registrations. If enabled, the Audit service records the pending operation details in the Policy database and reports it to the SM Service in case of BSF registration failure reaches the threshold value configured by the operator.

In case of registration failure with multiple BSF instances, the database entries increases and causes congestion in the SM service while trying to process all of the pending binding requests. To handle such scenarios, SM service continuously calls the Audit Service API to check on the number of records in the table and validate if it has crossed the threshold value. On receiving the notification, the SM service rejects all the SM Create requests with a DNN for which binding has to be setup. The rejection of requests is stopped once the *PendingOperation* table records reaches below the set threshold.

For more information on configuring the *PendingOperation* settings, see Audit Service Configurations in the Managing Retrying Binding Registration on BSF .

Site Takeover

The *PendingOperation* table contains the details of the site that is used to process the failed SM Create requests for PCF Binding. Each site processes the entries that belong to its site. In case a site goes down and the operator wants another site to process the pending operations, the Site Takeover functionality can be enabled. For this it is necessary to create a site takeover profile specifying the site id of the site that is failing. For more information on configuring the alternate site for takeover, use the **Site Takeover** Configurations on the CNC Console for Policy.

Managing Retrying Binding Registration on BSF

Enable and Configure

You can enable and configure Retrying Binding Registration on BSF using the CNC Console or REST API for Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Configure using CNC Console:** Perform the following feature configurations using the CNC Console:
  - Configure the Reattempt profile for BSF retry registration requests using the **Reattempts Profile** page. For more information, see Reattempts Profile.
  - Configure the error codes for which the reattempt must be initiated using the **Attempt Alternate Route for Following Requests** under the **Alternate Routing Settings** of the **Retry Profile** page. For more information, see Retry Profiles.
  - Enable the Retry BSF Registration functionality using the **Binding Configuration** section on the **PCF Session Management** page. For more information, see PCF Session Management.
  - Configure the Pending Operation table using the **Audit** section on the **PCF Session Management** page. For more information, see PCF Session Management.
  - Configure an alternate site that can take over the current site to manage the pending binding records in case of failure using the **Site Takeover** page. For more information, see Site Takeover.
  - You can use the **Set Binding Registration to** blockly rule to indicate if Binding Registration is required for managing the pending operation table of the Audit service.
  - To configure the frequency with which SM service calls the Audit service API for checking the Pending Operation table threshold, use the **Advance Settings** section on **PCF Session Management** page. For more information, see PCF Session Management.
- **Configure using REST API:** Perform the following feature configurations using the REST API Interface for Policy:
  - Configure the Reattempt profile for BSF retry registration requests using the **Reattempts Profile** configuration API.
  - Configure the error codes for which the reattempt must be initiated using the **alternateRoutingSettings.errorCodesList** parameter in the **Retry Profile** configuration API.
  - Enable the Retry BSF Registration functionality using the **BindingConfiguration** parameters of the **Session Management Service** configuration API.
  - Configure the Pending Operation table using the **Audit** parameters of the **Session Management Service** configuration API.
  - Configure an alternate site that can take over the current site to manage the pending binding records in case of failure using the **siteTakeover** configuration API.
    For more information about configuring the parameters through REST API, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observe

Policy uses the following metrics to observe the Retrying Binding Registration on BSF functionality:

- occnp_pending_binding_reattempts_total
- occnp_pending_binding_terminate_all_attempts_failed_total
- occnp_pending_binding_reattempt_fail_total
- occnp_pending_operation_threshold_reached_total
- occnp_reject_sm_create_threshold_reached_total
- occnp_audit_db_records_count_belonging_to_site

Copyright © 2019, 2026, Oracle and/or its affiliates.

Policy uses the following alerts to monitor the pending operations:

- pcf_pending_binding_records_count
- pcf_pending_binding_site_takeover
- pcf_pending_binding_threshold_limit_reached

4.126 Controlled Shutdown of an Instance

Policy supports controlled shutdown feature to provide the partial or complete isolation of the site from the network so that the operator can perform necessary recovery procedures when required. It helps the operator to perform the recovery procedures as per the requirement.

The site isolation is achieved by shutting down the load at gateways (Ingress Gateway, Egress Gateway, and Diameter Gateway) and updating the NF status as SUSPENDED at NRF.

> **Note**
>
> Ingress Gateway Service must be enabled for the working of this feature.

Operational State

The site can be in one of the three possible operational states NORMAL, PARTIAL SHUTDOWN, or COMPLETE SHUTDOWN. The operational state can move to any of the states from the current state, there is no definitive order of state change. Currently, the operational state is stored in the common config server of the Ingress Gateway. It is read by Ingress Gateway, Egress Gateway, Diameter Gateway, and App-info periodically and action is triggered based on the current state.

> **Note**
>
> Since the operational state is stored in config server, the service instances will detect the state change after the config refresh is done. If the config refresh interval is set as 5 seconds, then the pods may recognize the operational state change after 5 seconds.

The operational state can be modified through CNC Console or REST API. Operation state configuration stored in the common config server will be read by the following services:

- Ingress Gateway
- Egress Gateway
- Diameter Gateway
- App-info
- Audit Service

> **Note**
>
> If the Disaster Recovery procedure is performed when the config backup was taken when the system was in PARTIAL or COMPLETE SHUTDOWN state, then manual intervention may be required to change the operational state back to NORMAL state.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Load Control

Gateways enforce load control when the system is in a PARTIAL or COMPLETE SHUTDOWN state. The level of load control varies based on the shutdown state. When in a PARTIAL SHUTDOWN state, no new session establishments are allowed so session creation messages will be rejected (with configured error code) in this state. When in complete shutdown, no messages are allowed.

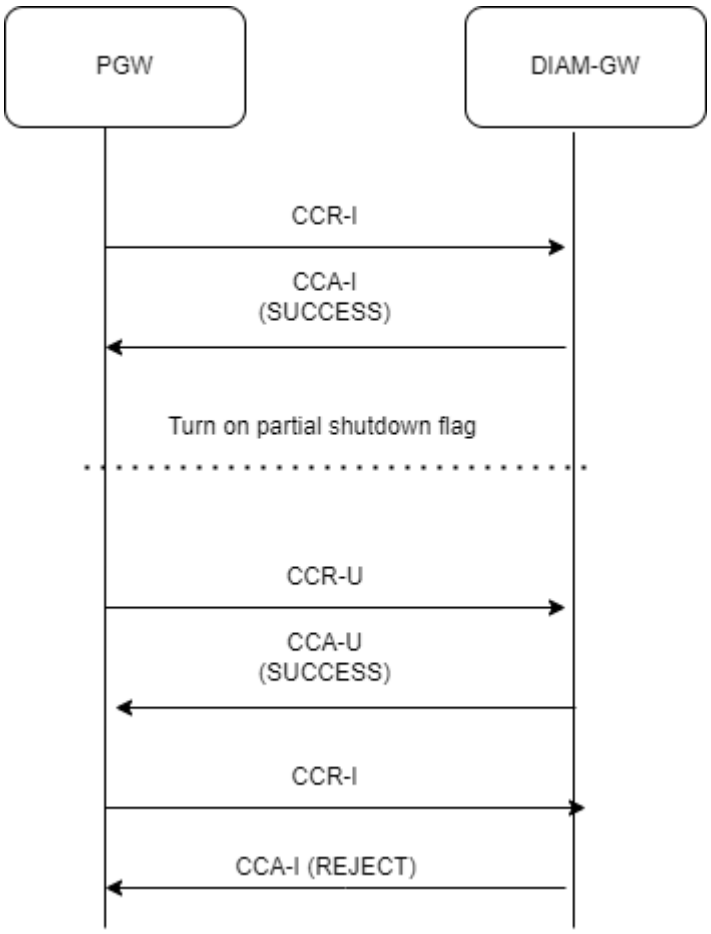
> **Note**
>
> When the system is in COMPLETE SHUTDOWN state, audit service triggered notification or diameter messages will be rejected at respective gateways.

Call Flow for Diameter Gateway

NORMAL State: If the Controlled shutdown operational state is NORMAL, then the Diameter Gateway processes the message as normal.

PARTIAL SHUTDOWN: If the controlled shutdown operational state is PARTIAL SHUTDOWN, then the Diameter Gateway accepts only in-session messages and rejects all CCR-I and AAR-I messages.

Figure 4-263 Call Flow for Diameter Gateway PARTIAL SHUTDOWN

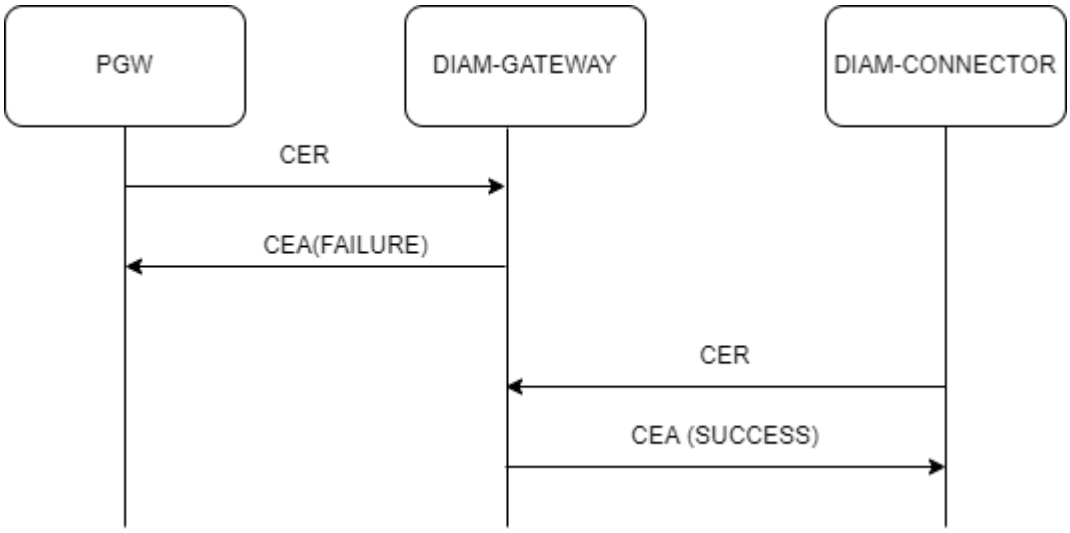


Copyright © 2019, 2026, Oracle and/or its affiliates.

When the operational mode is NORMAL, CCR-I is success. When operational mode is changed to PARTIAL SHUTDOWN, CCR-U is success but CCR-I is rejected.

COMPLETE SHUTDOWN: If the controlled shutdown operational state is COMPLETE SHUTDOWN, then the Diameter Gateway rejects all the messages.

Figure 4-264 Call Flow for Diameter Gateway COMPLETE SHUTDOWN



When the operational mode is COMPLETE SHUTDOWN, CER is rejected when coming from external NF, but is successful when coming from backend.

Call Flow for Egress Gateway

NORMAL State: If the Controlled shutdown operational state is NORMAL, then the Egress Gateway processes the message as normal.

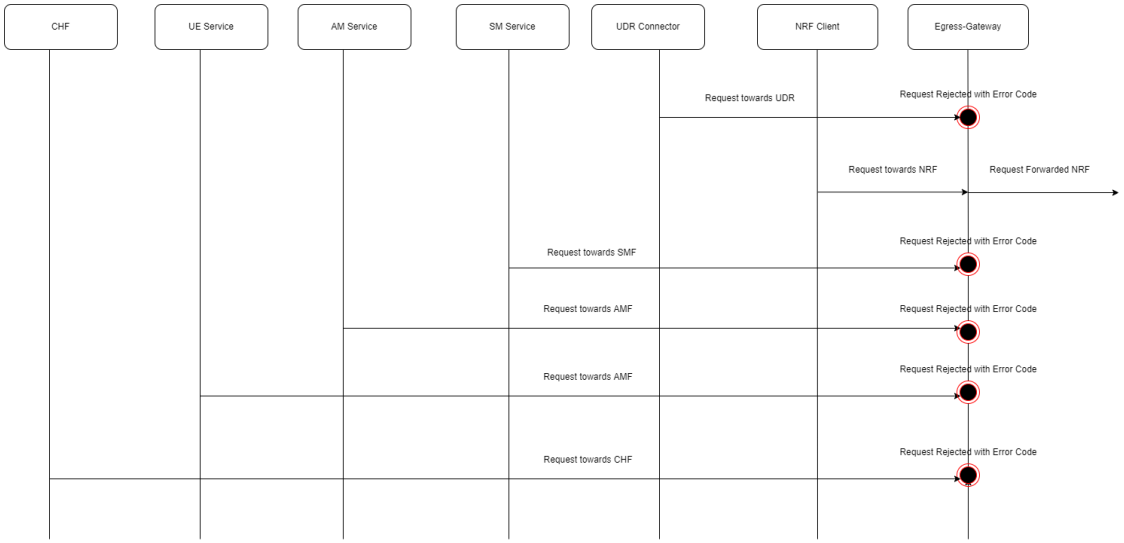
PARTIAL SHUTDOWN: If the controlled shutdown operational state is PARTIAL SHUTDOWN, then the Egress Gateway processes the message as normal.

COMPLETE SHUTDOWN: If the controlled shutdown operational state is COMPLETE SHUTDOWN, then the Egress Gateway processes the request as follows:

- Forward all requests received from NRF Client.
- Reject all requests received from any other services like UDR Connector, SM Service, AM Service, UE Service, and CHF Connector.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-265 Call Flow for Egress Gateway COMPLETE SHUTDOWN



SM-Policy data request from UDR connector towards Egress Gateway will not be processed in case of COMPLETE SHUTDOWN.

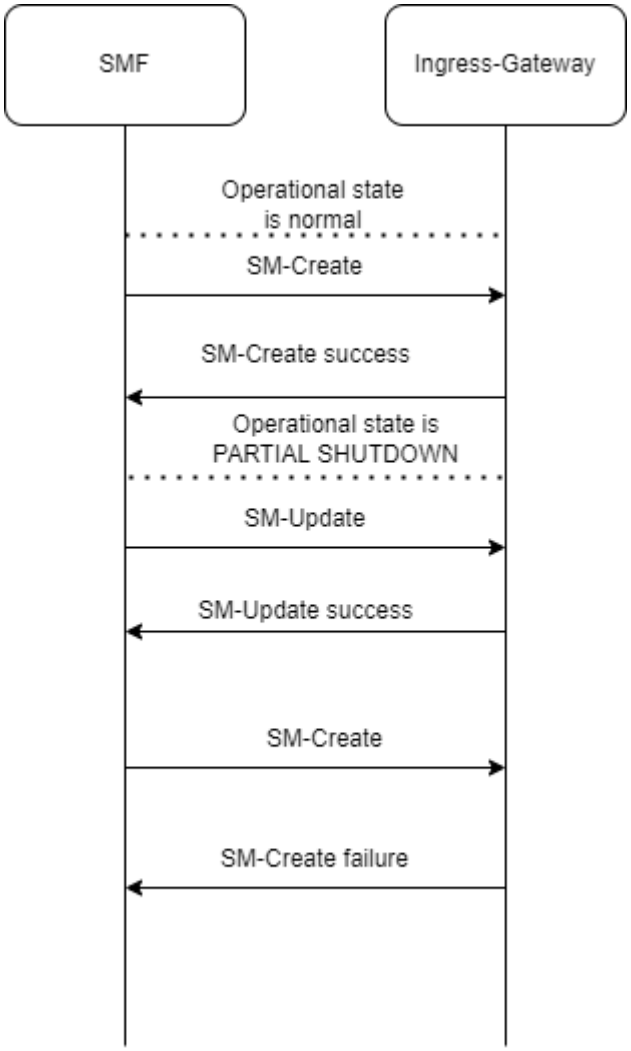
Call Flow for Ingress Gateway

NORMAL State: If the Controlled shutdown operational state is NORMAL, then the Ingress Gateway processes the message as normal.

PARTIAL SHUTDOWN: If the controlled shutdown operational state is PARTIAL SHUTDOWN, then the Ingress Gateway accepts only in-session messages and rejects all SM-Create requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-266 Call Flow for Ingress Gateway PARTIAL SHUTDOWN

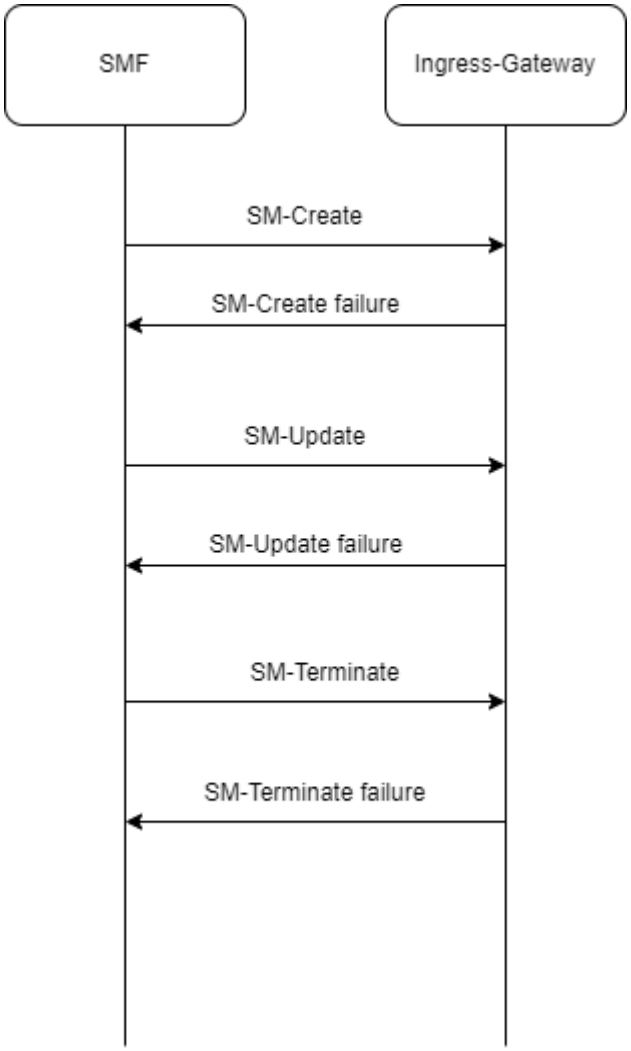


When the operational mode is NORMAL, SM-Create is success. When operational mode is changed to PARTIAL SHUTDOWN, SM-Update is success but SM-Create is rejected.

COMPLETE SHUTDOWN: If the controlled shutdown operational state is COMPLETE SHUTDOWN, then the Ingress Gateway rejects all incoming requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-267 Call Flow for Ingress Gateway COMPLETE SHUTDOWN



In Ingress Gateway COMPLETE SHUTDOWN, all the requests coming from external NFs are rejected.

App-info

App-info calculates the service status of the NF periodically, and this calculation has three possible outcomes viz Running, Not Running, and Deregister. Whenever the system's operation state is changed to PARTIAL or COMPLETE SHUTDOWN and the calculated status is "Running" then the status will be overridden and changed to "Not Running".

Audit Service

The **Disabling Audit on Controlled Shutdown** feature allows you to gracefully shut down audit and timer services in a controlled manner. When enabled, this feature ensures that during a **COMPLETE_SHUTDOWN**, the Audit Service and Timer Service are temporarily disabled, preventing interruptions and ensuring a smooth shutdown process. This feature is particularly useful for maintenance or upgrade scenarios where you need to pause auditing activities without losing data or disrupting ongoing operations.

Depending on the **operationalState**, the system behaves as follows:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **NORMAL / PARTIAL_SHUTDOWN**: Audit and Timer Services continue to function as usual.
- **COMPLETE_SHUTDOWN**:
  - **Audit Service**: All audit operations are interrupted, including stale session notifications and record deletions. All entries in `audit_schedule_table` are transitioned to `CTRL_SHUTDOWN_INTRPT` state, except those already in DEREGISTERED or INTERRUPTED states. The **Audit Now** and **Audit Resume** functionalities are disabled. But, the **Audit Pause** functionality remains enabled. The audit service supports registration, deregistration, and fetch requests.
  - **Timer Service**: Timer expiry is disabled. The timer expiry notifications are paused during this state.

> **Note**
>
> Once the system returns to **NORMAL** or **PARTIAL_SHUTDOWN**, the Audit Service resumes normal operations, and all audit entries which are in `CTRL_SHUTDOWN_INTRPT` state are moved back to the *QUEUED* state.

If the current version has the **enableControlledShutdown** flag enabled and the **operationalState** is set to **COMPLETE_SHUTDOWN**, follow these steps before initiating a rollback:

1. Manually transition all audit records to the **INTERRUPTED** state by clicking the **Audit Pause** button in the CNC Console.
2. After the rollback is completed, manually move these records back to the **QUEUED** state to resume auditing.

> **Note**
>
> Failure to complete the audit record state transition process will leave audit records stuck in the **COMPLETE_SHUTDOWN** state, blocking audits from restarting after a rollback to a version that doesn't support this feature.

Managing Controlled Shutdown of an instance

Enable

You can enable or disable the Controlled Shutdown feature by using the `enableControlledShutdown` parameter in the custom.yaml file. This parameter is set as `false` by default. You can enable it by setting its value as `true`. For more information, see *Controlled Shutdown Configurations* section in the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, Fault Recovery Guide*.

Configure

Diameter Gateway and Ingress Gateway can be configured through CNC Console. For more information, see Controlled Shutdown Configurations.

For SBI, it is mandatory to configure *SBI Ingress Error Mapping* for each route that needs to be rejected during a complete shutdown. These routes must be explicitly mapped to the intended error code through CNC Console configuration.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For diameter, in the event of a complete shutdown, if there are no configurations for diameter error mapping, any new connection attempt is rejected using the default result code `DIAMETER_UNABLE_TO_COMPLY (5012)`.

Egress Gateway routes configuration for controlled shutdown is done through Helm. For more information, see the *Controlled Shutdown Configurations* section in the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, Fault Recovery Guide*.

Observe

Metrics

Policy provides the following metrics specific to controlled shutdown feature:

- system_operational_state
  For more information, see CM Service Metrics.
- diam_controlled_shutdown_message_reject_total
  For more information, see Diameter Gateway Metrics.
- audit_schedule_current_status
  For more information, see Audit Service Metrics.
- occnp_audit_schedule_status_total
  For more information, see Audit Service Metrics.

Alerts

Policy provides the following alerts for controlled shutdown feature:

- SYSTEM_IMPAIRMENT_MAJOR
- SYSTEM_IMPAIRMENT_CRITICAL
- SYSTEM_OPERATIONAL_STATE_NORMAL
- SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN
- SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN

For more information, see Common Alerts.

4.127 Enhancement to use Cached NRF Discovery Responses

Policy communicates with different Network Functions (NFs) through the NRF-Client discovery service. As a Consumer NF, Policy registers with NRF and discovers the required Producer NF through the NRF Client discovery feature.

PCF is enabled to maintain a cache of the NF Profiles discovered autonomously through the NRF Client management. The cache stores the NF Profiles with the NF Type and locality details of the discovered NFs.

> **Note**
>
> Policy supports the enhancement to use Cached NRF discovery responses in case of failure and unusable producers for autonomous discovery only.

PCF is enabled to cache the discovered NF Profiles from NRF for autonomous discovery for producer NFs, such as CHF and BSF. It uses the cache to perform the following functions:

Copyright © 2019, 2026, Oracle and/or its affiliates.

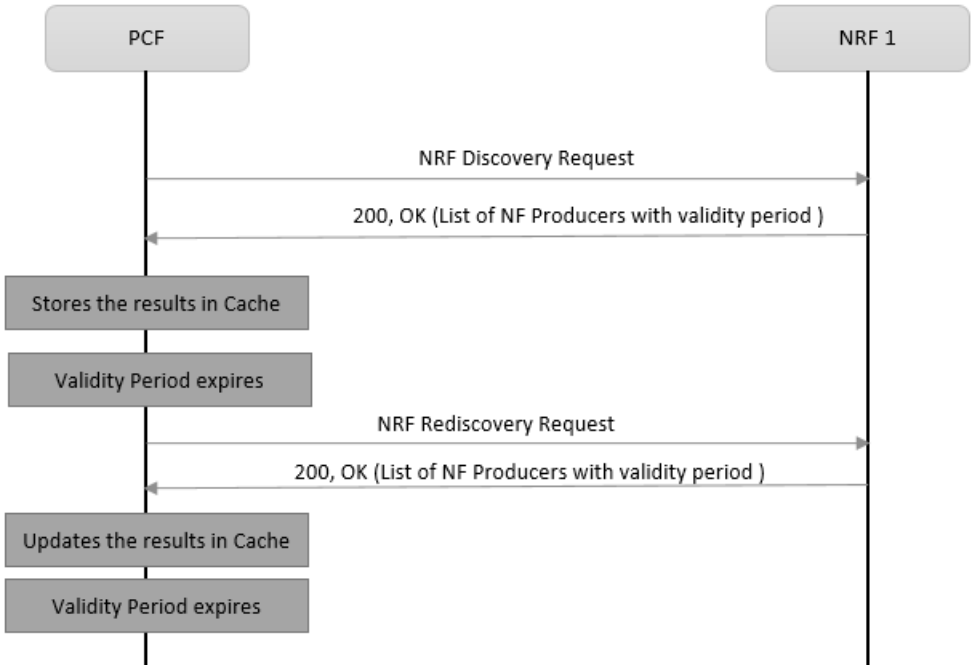
- Rediscovers the NF Profiles for which the validity time is expired
- Rediscovers the NF Profiles when all the discovered profiles for a particular query parameter are in the **Suspended** state, irrespective of their validity time. **Note:** PCF does not use the NFs in the suspended state.
- Uses the expired discovered profiles, which are in the **Registered** state in case the NRF is unreachable during rediscovery

NF Discovery and Rediscovery Based using PCF Cache

The following call flow describes an example of PCF performing the NF discovery through NRF Client and maintaining a cache:

The call flow is described as follows:

Figure 4-268 Call Flow - NRF Rediscovery



1. During PCF deployment, operators provide a list of NFTypes, which must be automatically subscribed by the NRF Client. NRF triggers the NRF discovery operation for the set of NfTypes provided for auto-subscription.
2. NRF sends the discovery response to the PCF with the query parameters. At runtime, when there is any change in the profiles, the NRF notifies PCF about the changed profiles.
3. PCF stores the producer NF details and their query parameters in a cache. It uses the validity period parameter to calculate the expiry time the producer NF profile. Once the validity period is over, the NF profile is considered **Expired** and PCF rediscovers the NF profiles. The expiry duration can be any of the following values:
   - The validity period included in the discovery response from the NRF Client
   - The value configured in the **validityTime** parameter through the Policy Custom Values YAML file.

   Whichever is the minimum value for the validity period is considered the expiry duration.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Example:

During PCF deployment, the **nrf-client.profile.validityTime** parameter value is configured as 60 seconds. And the validityPeriod provided by NRF during discovery is as follows:

- For UDR: 30 seconds
- For CHF: 150 seconds
- For BSF: 90 seconds

Then, the expiry duration for the respective producer NFs is as follows:

- For UDR: 30 seconds
- For CHF: 60seconds
- For BSF: 60 seconds

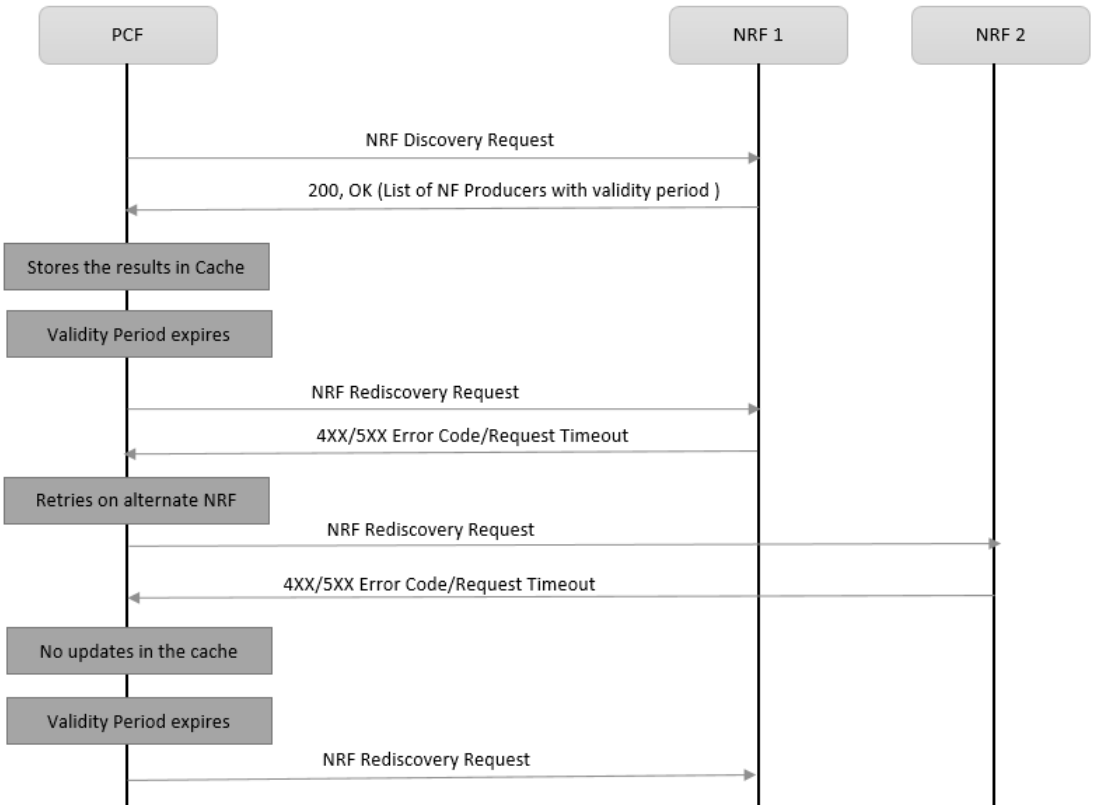
4. In case, the validity period for a producer NF expires, then PCF sends the rediscovery request to the NRF and updates the cache with the latest response.

> **Note**
>
> In case of an empty response from NRF, PCF considers it as valid response and stores in the cache for both for initial discovery and rediscovery. It sends a rediscovery request once the empty response expires.

NF Discovery Error Scenario

The call flow is described as follows:

Figure 4-269 Call Flow - NF Discovery Error Scenario



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. In the case of an Expired NF producer, PCF sends a rediscovery request to NRF.
2. PCF may attempt to send an NRF discovery request to another NRF. If another NRF still responds with an error or still timeout, PCF continues using the cache for the expired producer and after the validity time, it sends another NRF discovery request.
3. If the NRF rediscovery fails and NRF sends an error response to PCF, then the PCF keeps on using the expired records available in the cache.
4. PCF continues sending the rediscovery requests to NRF based on the expiry duration for the producer NF.

> **Note**
>
> If all the NF producers available in the PCF cache are suspended, then PCF rejects the NRF discovery request. When the cache is not yet expired, and there is no available NFs in the cache due to all of the cached NFs having gone into suspend status, ignore the TTL & trigger a discovery request to the NRF.

Managing the Enhancement to use Cached NRF Discovery Responses

Enable

To enable the PCF cache for NRF Discovery results set value of the **nrf-client.profile.cacheDiscoveryResults parameter** to **true** using the Custom Values YAML file for Policy.

Configure

You need to configure the Cache of NRF Discovery Result functionality while deploying the PCF. The following parameters must be updated in the Custom Values YAML file for Policy:

Table 4-190 NRF Rediscovery Parameters

Parameter	Description
discoveryRefreshInterval	This attribute defines the maximum ValidityPeriod at which the discovery results shall be refreshed. The ValidityPeriod received in the discovery response shall be capped at this value. If ValidityPeriod received in discovery results is 60s. The validityPeriod shall be capped to 10s as per configuration. If ValidityPeriod received in discovery results is 5s. No capping shall be applied and valdiityPeriod shall be considered as 5s. Default: 10
discoveryDurationBeforeExpiry	This attributes defines the rate at which the NF shall resend discovery requests to NRF. The value shall be configured in terms of percentage(1-100). if the discovery ValidityPeriod is 10s(after applying the capped value of discoveryRefreshInterval), then the discovery requests shall be sent at discoveryDurationBeforeExpiry * 10/100.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-190 (Cont.) NRF Rediscovery Parameters

Parameter	Description
enableDiscoveryRefresh	Feature flag to enable Automatic Discovery Refresh. Default: false
enableRediscoveryIfNoProdNFs	Feature flag to enable automatic rediscovery in case no producer NF is available. Default: false
offStatesForRediscoveryIfNoProdNFs	The NF producer status for which discovery request must be sent to NRF. It indicates the nfStatus to be considered for unavailability of all profiles and performing Rediscovery: Provide comma separated value for desired states. Possible values: • SUSPENDED • UNDISCOVERABLE • DEREGISTERED
discoveryRetryInterval	The Retry Interval after a failed autonomous discovery request.

4.128 Limiting the Number of Sessions

Limiting the Number of Sessions feature is implemented to manage and control the usage of resources. When this feature is enabled, Policy allows you to configure the maximum number of active sessions. It avoids multiple policy association table entries for a subscriber, in the respective policy service database tables (such as SMPolicyAssociations, AMPolicyAssociations, and UEPolicyAssociations)

Limiting the number of sessions for AM service and UE Policy service

The following are the parameters used to enable maximum sessions limit for each of the services:

- **Enable Max Session Limit** parameter for AM Service
- **Enable Max Session Limit** parameter for UE Policy Service

When the Policy service receives request for a new session and if the maximum sessions limit for the subscriber is enabled, it checks if there are existing sessions for the same subscriber (SUPI).

If the number of sessions for the same subscriber (SUPI) exceeds the **Max Session Limit Per User** configured, it creates a policy association for the new session in its respective database and deletes the oldest session based on the session created timestamp. The policy service initiates a local delete request.

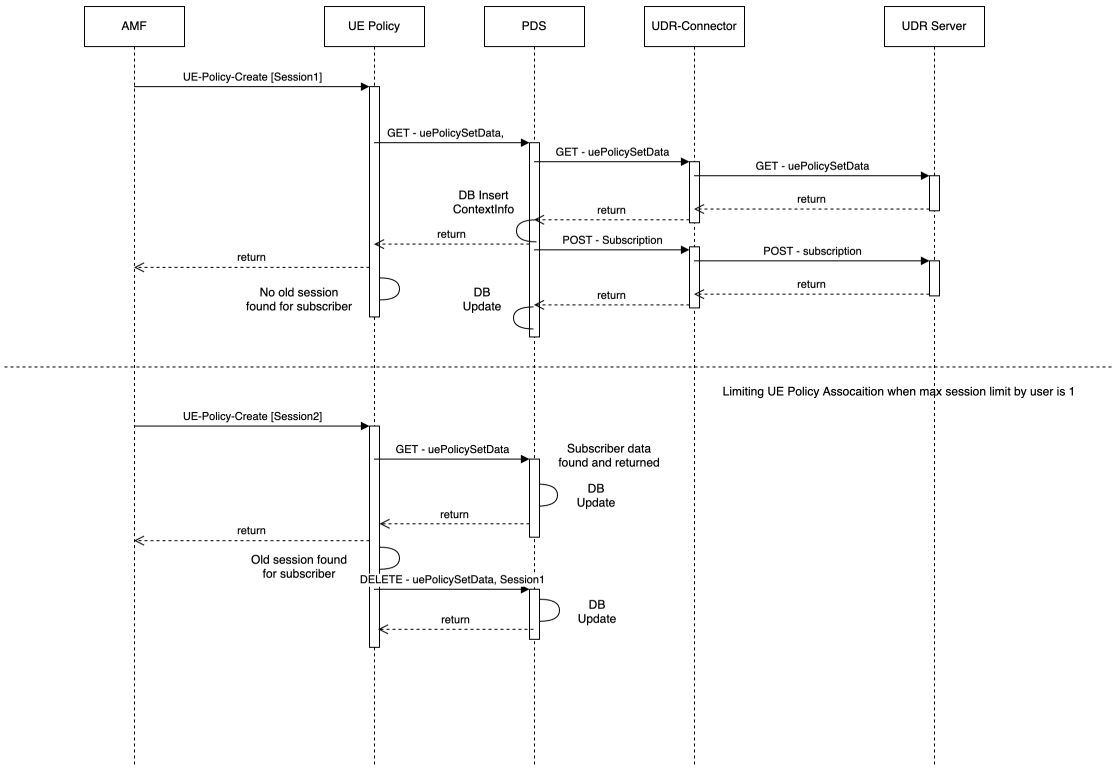
Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> In Kubernetes deployment resource AM Service and UE Policy Service, the `LIMITING_SESSION_DELETE_DELAY_MILLIS` environment variable is configured to set a delay for initiating the local delete of the older session when the number of sessions for a subscriber (SUPI) exceeds the Max Session Limit Per User. The default value of `LIMITING_SESSION_DELETE_DELAY_MILLIS` is 3000 milliseconds.

For example, if the **Max Session Limit Per User** configured for UE Policy Service is 2. When a third session is created for a subscriber with two existing sessions, the UE Policy Service creates a UEPolicyAssociation for the new session and deletes the oldest session from UE Policy database. The policy service initiates a local delete request.

> **Note**
>
> The oldest session is deleted only from the local policy service and PolicyDS databases if the number of sessions exceeds the **Max Session Limit Per User**.

Figure 4-270 Limiting the number of sessions for UE Policy Service



Copyright © 2019, 2026, Oracle and/or its affiliates.

Limiting the number of sessions per subscriber and DNN+SNSSAI for SM service and PCRF Core service

Whenever there is a CREATE request for a new SM session or PCRF Core session, Policy queries the database using SUPI or GPSI or using both SUPI and GPSI. There are two levels at which the number of sessions can be limited and both levels are independent to each other:

Limiting the maximum number of bindings at DNN + SNSSAI level

This is the first level of limiting the bindings at Binding service.

When limiting the maximum number of bindings at DNN + SNSSAI, Binding service limits the bindings based on the context owner (SM service/ PCRF Core service).

> **Note**
>
> SNSSAI is considered depending on the Binding configuration in CNC Console.

You can enable and configure limiting the number of bindings at DNN + SNSSAI level by configuring **Max Session Limit By APN** field in **Binding Service** page under **Service Configurations** in CNC Console.

The default limit is 2 per DNN+SNSSAI+IP domain combination.

Limiting the maximum number of bindings at user level

This is the second level of limiting the bindings at Binding service.

On top of the first level limit, user level limiting is applied. Based on the timestamp, sessions older than the configured limit, (irrespective of the DNN+SNSSAI limit) are marked as stale and are cleanedup.

You can enable limiting the number of bindings at user level using **Session Limit By User** field in **Binding Service** page under **Service Configurations** in CNC Console.

You can configure the number of bindings at user level by configuring **Max Session Limit By User** field in **Binding Service** page under **Service Configurations** in CNC Console.

The default limit is 10 per user level.

> **Note**
>
> Binding service identifies the sessions as stale and it notifies SM service or PCRF Core service based on the context owner to perform the clean up.

Example 1: If Binding session Limit at DNN+SNSSAI level is configured as 2 for internet sessions, after the first two sessions are created for the user, if Binding service receives request for the creation of 3rd session, it creates the 3rd session and marks the 1st session as stale.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-191 Binding Session Limit at DNN+SNSSAI level -2

Session ID	Context Owner	DNN+SNSSAI	Last Modified Time	isStale	Comments
Session1	PCF-SM	Internet	'2021-05-05 01:00:00'	0	First session creation for internet session
Session2	PCF-SM	Internet	'2021-05-05 02:00:00'	0	Second session creation for internet session
Session3	PCF-SM	Internet	'2021-05-05 03:00:00'	0	Third session creation for internet session At this point DNN+SNSSAI limit exceeds. Binding service marks Session1 as stale by changing the value of isStale to 1. It indicates SM service to cleanup Session1.

Example 2: If the Binding session limit for the user is configured at level 5, after creating the first five sessions for the user, if Binding service receives request for 6th session, it creates the 6th session and marks the 1st session as stale.

Table 4-192 Binding Session Limit at User level - 5

Session ID	Context Owner	DNN+SNSSAI	Last Modified Time	isStale	Comments
Session1	PCF-SM	Internet	'2021-05-05 01:00:00'	0	First session creation for internet session
Session2	PCF-SM	Internet	'2021-05-05 02:00:00'	0	Second session creation for internet session
Session3	PCF-SM	ims	'2021-05-05 03:00:00'	0	First session creation for IMS session
Session4	PCF-SM	ims	'2021-05-05 04:00:00'	0	Second session creation for IMS session
Session5	PCF-SM	gaming	'2021-05-05 05:00:00'	0	First session creation for gaming session

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-192 (Cont.) Binding Session Limit at User level - 5

Session ID	Context Owner	DNN+SNSSAI	Last Modified Time	isStale	Comments
Session6	PCF-SM	gaming	'2021-05-05 04:00:00'	0	Second session creation for gaming session At this point user limit exceeds. Binding service marks Session1 as stale by changing the value of isStale to 1. It indicates SM service to cleanup Session1.

> **Note**
>
> The Binding Service applies session limiting based on the lastModifiedTime of bindings. When the configure limit is exceeded, the oldest sessions are marked as stale and selected for cleanup, ensuring that the most recent sessions are retained.

Managing Limiting the Number of Sessions

Enable

By default, this feature is disabled for AM Service and UE Policy Service and enabled for SM service and PCRF Core service on the Policy deployment.

You can enable the Limiting the Number of Sessions functionality using the CNC Console or REST API for Policy.

- **Enable using CNC Console**:
  - To enable the feature for AM Service, set the value of **Enable Max Session Limit** flag to `true` under **Access and Mobility** page.
    For more details on enabling the flag for AM Service, see PCF Access and Mobility.
  - To enable the feature for UE Policy Service, set the value of **Enable Max Session Limit** flag to `true` under **UE Policy Service** page.
    For more details on enabling the flag for UE Policy Service, see PCF UE Policy Service.
  - To enable limiting the number of sessions at user level (for SM service and PCRF Core), set the value of **Session Limit By User** flag to `true` under **Binding Service** page.
    For more details on enabling the **Session Limit By User** flag, see Binding Service.
  - To enable limiting the number of sessions at DNN + SNSSAI level, configure **Max Session Limit By APN** field under **Binding Service** page.
    For more details on enabling and configuring limiting number of sessions at DNN + SNSSAI level using **Max Session Limit By APN** field , see Binding Service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Enable using REST API**:
  - To enable the feature for AM Service, set the value as `true` for **enableLimitingSessionByPerUser** parameter under the System group in the `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam` REST API.
  - To enable the feature for UE Policy Service, set the value as `true` for **enableLimitingSessionByPerUser** parameter under the System group in the `{apiRoot}/oc-cnpolicy-configuration/v1/services/pcfue` REST API.
  - To enable limiting the number of sessions at user level (for SM service and PCRF Core), set the value of **enableSessionLimitByUser** parameter to `true` in `{apiRoot}/oc-cnpolicy-configuration/v1/services/binding` REST API.
  - To enable limiting the number of sessions at DNN + SNSSAI level, configure **maxSessionLimitByApn** parameter in `{apiRoot}/oc-cnpolicy-configuration/v1/services/binding` REST API.

  For more details on enabling the flag using REST API, see *Converged Policy REST Specifications* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure the Limiting the Number of Sessions functionality using the CNC Console or REST API for Policy.

- **Configure using CNC Console**:
  To configure Limiting Number of Sessions feature for AM Service and UE Policy Service, perform the feature configurations under the System group on the respective service configurations page. For more information, see the following sections:
  - PCF Access and Mobility
  - PCF UE Policy Service

  To configure limiting the number of sessions per subscriber and DNN+SNSSAI for SM service and PCRF Core service, configure **Session Limit By User**, **Max Session Limit By User**, and **Max Session Limit By APN** fields under **Binding Service** page. For more information, see Binding Service.
- **Configure using REST API**: Policy provides the following REST API to configure the Limiting the Number of Sessions functionality:
  - **AM service**: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfam
  - **UE Policy service**: {apiRoot}/oc-cnpolicy-configuration/v1/services/pcfue
  - **Limiting the number of sessions per subscriber and DNN+SNSSAI for SM service and PCRF Core service**: {apiRoot}/oc-cnpolicy-configuration/v1/services/binding

Observe

The following metrics are added to AM Service metrics:

- session_info_request_total
- session_info_response_total

The following metrics are added to UE Policy Service metrics:

- session_info_request_total
- session_info_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

For more details on these metrics, see the following sections:

- AM Service Metrics
- UE Service Metrics

Logging

Below is the sample log that can be seen in **pcf-am** once the Max Session limit is hit, and the older session will be deleted.


```
{"instant":
{"epochSecond":1669193988,"nanoOfSecond":609281261},"thread":"pool-4-
thread-15","level":"DEBUG","loggerName":"ocpm.pcf.service.am.core.LimitingSess
ionManager","message":"Limiting Number of Sessions Feature is enabled :
true","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","
threadId":1181,"threadPriority":5,"messageTimestamp":"2022-11-23T08:59:48.609+
0000"}


{"instant":
{"epochSecond":1669193988,"nanoOfSecond":614094447},"thread":"pool-4-
thread-15","level":"DEBUG","loggerName":"ocpm.pcf.service.am.core.LimitingSess
ionManager","message":"Existing Session count :3 exceed max session count
limit:
2","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thr
eadId":1181,"threadPriority":5,"messageTimestamp":"2022-11-23T08:59:48.614+000
0"}
{"instant":
{"epochSecond":1669193988,"nanoOfSecond":614431105},"thread":"pool-4-
thread-15","level":"DEBUG","loggerName":"ocpm.pcf.service.am.core.LimitingSess
ionManager","message":"The stale association Ids to be deleted are
[5d0ff3a0-0b47-42ab-8fe2-829934465619]","endOfBatch":false,"loggerFqcn":"org.a
pache.logging.slf4j.Log4jLogger","threadId":1181,"threadPriority":5,"messageTi
mestamp":"2022-11-23T08:59:48.614+0000"}


{"instant":
{"epochSecond":1669193991,"nanoOfSecond":624093788},"thread":"pool-4-
thread-16","level":"INFO","loggerName":"ocpm.cne.common.logging.http.HttpLogge
r","marker":{"name":"SUBSCRIBER"},"message":"HttpLog: {type:
'CLIENT_REQUEST', requestId:
'supi;imsi-450081000000002-894f996b-5f94-43f8-9f49-de2753b8c02e', uri:
'http://10.233.74.200:8000/pds/v2/user-data?
reqParam=%7B%22amPolicyDataReq%22%3A%7B%22subscription%22%3Atrue%2C%22resetCon
text%22%3Afalse%2C%22processEtag%22%3Afalse%7D%2C%22ssvEnabled%22%3Afalse%2C%2
2resetContextSSV%22%3Afalse%7D&param=%7B%22user%22%3A%7B%22userIds%22%3A%7B%22
gpsiSet%22%3A%5B%22msisdn-12345678901234%22%5D%2C%22supiSet%22%3A%5B%22imsi-45
0081000000002%22%5D%7D%7D%2C%22request%22%3A%7B%22requestType%22%3A%22DELETE%2
2%2C%22operationType%22%3A%22DELETE%22%2C%22contextOwner%22%3A%22PCF_AM%22%2C%
22contextId%22%3A%225d0ff3a0-0b47-42ab-8fe2-829934465619%22%2C%22notificationI
nfo%22%3Anull%7D%2C%22dnn%22%3A%22NA%22%2C%22gpsi%22%3A%22msisdn-1234567890123
4%22%2C%22sliceinfo%22%3A%7B%22sst%22%3A%22NA%22%2C%22sd%22%3A%22NA%22%7D%2C%2
2supi%22%3A%22imsi-450081000000002%22%7D', method: 'DELETE', headers:
'{subscriber-logging=[supi;imsi-450081000000002, supi;imsi-450081000000002],
Accept=[*/*], User-Agent=[Jetty/9.4.49.v20220914], Host=[10.233.74.200:8000],
Accept-Encoding=[gzip]}', body:
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

''}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":1184,"threadPriority":5,"messageTimestamp":"2022-11-23T08:59:51.624+0
000"}

{"instant":
{"epochSecond":1669193991,"nanoOfSecond":647017328},"thread":"pool-4-
thread-17","level":"INFO","loggerName":"ocpm.pcf.service.am.serviceconnector.P
olicyConnector","message":"Policy Request sent to : http://ross-helm-occnp-
pre:8000/v1/policy/engine/pcf-am httpHeader:{subscriber-
logging=[supi;imsi-450081000000002, supi;imsi-450081000000002]} {\"request\":
{\"requestType\":\"AMF\",\"operationType\":\"DELETE\"},\"policyAssociation\":
{\"associationId\":\"5d0ff3a0-0b47-42ab-8fe2-829934465619\",\"createdTimestamp
\":\"2022-11-23T08:59:22.073387212Z\",\"user\":
{\"lastModificationTimestamp\":1669193988612,\"cid\":0,\"userIds\":
{\"LASTACCESSTIME\":\"2022-11-23
08:59:22\",\"PEI\":\"imei-100120010030110\",\"SUPI\":\"imsi-450081000000002\",
\"SITEID\":\"fe7d992b-0541-4c7d-ab84-
c6d70b1b0123\",\"GPSI\":\"msisdn-12345678901234\"},\"amPolicyData\":
{\"lastErrorcode\":null,\"subscCats\":[\"Sliver\"]}},\"policyAssociation\":
{\"request\":{\"notificationUri\":\"http://10.233.14.139:8080/amf/
notify\",\"supi\":\"imsi-450081000000002\",\"gpsi\":\"msisdn-12345678901234\",
\"accessType\":\"3GPP_ACCESS\",\"pei\":\"imei-100120010030110\",\"userLoc\":
{\"nrLocation\":{\"tai\":{\"plmnId\":
{\"mcc\":\"460\",\"mnc\":\"30\"},\"tac\":\"000C27\"},\"ncgi\":{\"plmnId\":
{\"mcc\":\"460\",\"mnc\":\"30\"},\"nrCellId\":\"187900000\"},\"ueLocationTimes
tamp\":\"2019-03-20T14:32:22.222Z\"}},\"servingPlmn\":
{\"mnc\":\"30\",\"mcc\":\"460\"},\"ratType\":\"NR\",\"servAreaRes\":
{\"restrictionType\":\"ALLOWED_AREAS\",\"areas\":[{\"tacs\":
[\"t015\"],\"areaCodes\":\"a014\"}],\"maxNumOfTAs\":1},\"rfsp\":10,\"suppFeat\
":\"0000000000000000\"},\"triggers\":[\"LOC_CH\",\"PRA_CH\"],\"servAreaRes\":
{\"restrictionType\":\"ALLOWED_AREAS\",\"areas\":[{\"tacs\":
[\"12\"],\"areaCodes\":\"123\"}],\"maxNumOfTAs\":1},\"rfsp\":1,\"pras\":
{\"1\":{\"praId\":\"1\",\"trackingAreaList\":[{\"plmnId\":
{\"mcc\":\"111\",\"mnc\":\"11\"},\"tac\":\"1111\"}]}},\"suppFeat\":\"0\"},\"po
licyAssociationRequest\":{\"notificationUri\":\"http://10.233.14.139:8080/amf/
notify\",\"supi\":\"imsi-450081000000002\",\"gpsi\":\"msisdn-12345678901234\",
\"accessType\":\"3GPP_ACCESS\",\"pei\":\"imei-100120010030110\",\"userLoc\":
{\"nrLocation\":{\"tai\":{\"plmnId\":
{\"mcc\":\"460\",\"mnc\":\"30\"},\"tac\":\"000C27\"},\"ncgi\":{\"plmnId\":
{\"mcc\":\"460\",\"mnc\":\"30\"},\"nrCellId\":\"187900000\"},\"ueLocationTimes
tamp\":\"2019-03-20T14:32:22.222Z\"}},\"servingPlmn\":
{\"mnc\":\"30\",\"mcc\":\"460\"},\"ratType\":\"NR\",\"servAreaRes\":
{\"restrictionType\":\"ALLOWED_AREAS\",\"areas\":[{\"tacs\":
[\"t015\"],\"areaCodes\":\"a014\"}],\"maxNumOfTAs\":1},\"rfsp\":10,\"suppFeat\
":\"0000000000000000\"},\"userSubscription\":true,\"sbiBinding\":
{},\"modelObjectId\":\"5d0ff3a0-0b47-42ab-8fe2-829934465619\"},\"user\":
{\"isVisiting\":null,\"userIds\":{\"LASTACCESSTIME\":\"2022-11-23
08:59:22\",\"PEI\":\"imei-100120010030110\",\"SUPI\":\"imsi-450081000000002\",
\"SITEID\":\"fe7d992b-0541-4c7d-ab84-
c6d70b1b0123\",\"GPSI\":\"msisdn-12345678901234\"},\"smPolicyData\":null,\"amP
olicyData\":{\"lastErrorcode\":null,\"subscCats\":
[\"Sliver\"]},\"uePolicySet\":null,\"spendingLimitStatus\":null,\"operatorSpec
ificData\":null,\"shUserData\":null,\"ldapUserData\":null,\"ocsSpendingLimitSt
atus\":null,\"custom\":null}}","endOfBatch":false,"loggerFqcn":"org.apache.log
ging.slf4j.Log4jLogger","threadId":1185,"threadPriority":5,"messageTimestamp":

Copyright © 2019, 2026, Oracle and/or its affiliates.

"2022-11-23T08:59:51.647+0000"}

{"instant":
{"epochSecond":1669193991,"nanoOfSecond":679435548},"thread":"pool-4-
thread-18","level":"DEBUG","loggerName":"ocpm.cne.common.db.JdbcTable","messag
e":"trying to execute sql : delete from AmPolicyAssociation where k
= ?","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":1190,"threadPriority":5,"messageTimestamp":"2022-11-23T08:59:51.679+0
000"}
{"instant":
{"epochSecond":1669193991,"nanoOfSecond":683701171},"thread":"pool-4-
thread-18","level":"DEBUG","loggerName":"ocpm.cne.common.db.JdbcTable","messag
e":"deleted 1 records from table AmPolicyAssociation with key
5d0ff3a0-0b47-42ab-8fe2-829934465619","endOfBatch":false,"loggerFqcn":"org.apa
che.logging.slf4j.Log4jLogger","threadId":1190,"threadPriority":5,"messageTime
stamp":"2022-11-23T08:59:51.683+0000"}

Below is the sample log that can be seen in **pcf-ue** once the Max Session limit is hit, and the older session will be deleted.

{"instant":
{"epochSecond":1669195257,"nanoOfSecond":357845539},"thread":"pool-3-
thread-9","level":"DEBUG","loggerName":"ocpm.pcf.service.uepolicy.core.Limitin
gSessionCountManager","message":"The limiting no of sessions feature is
enabled","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger
","threadId":1342,"threadPriority":5,"messageTimestamp":"2022-11-23T09:20:57.3
57+0000"}

{"instant":
{"epochSecond":1669195257,"nanoOfSecond":363242218},"thread":"pool-3-
thread-9","level":"DEBUG","loggerName":"ocpm.pcf.service.uepolicy.core.Limitin
gSessionCountManager","message":"Checking if limit of association Ids is
exceeded","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogge
r","threadId":1342,"threadPriority":5,"messageTimestamp":"2022-11-23T09:20:57.
363+0000"}
{"instant":
{"epochSecond":1669195257,"nanoOfSecond":363456742},"thread":"pool-3-
thread-9","level":"DEBUG","loggerName":"ocpm.pcf.service.uepolicy.core.Limitin
gSessionCountManager","message":"The association ids to be deleted are
[ocpm.pcf.service.uepolicy.model.UePolicyAssociationImpl@3f172e31]","endOfBatc
h":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":1342,"
threadPriority":5,"messageTimestamp":"2022-11-23T09:20:57.363+0000"}

{"instant":
{"epochSecond":1669195260,"nanoOfSecond":377243552},"thread":"pool-3-
thread-10","level":"INFO","loggerName":"ocpm.pcf.service.uepolicy.serviceconne
ctor.UserServiceConnector","message":"Sent DELETE Request: http://ross-helm-
occnp-policy-ds:8000/pds/v2/user-data?
param=%7B%0A%20%20%22user%22%20%3A%20%7B%0A%20%20%20%20%22userIds%22%20%3A%20%
7B%0A%20%20%20%20%20%20%22gpsiSet%22%20%3A%20%5B%20%22msisdn-10000000018%22%20
%5D%2C%0A%20%20%20%20%20%20%22supiSet%22%20%3A%20%5B%20%22imsi-450081000000018
%22%20%5D%0A%20%20%20%20%7D%0A%20%20%7D%2C%0A%20%20%22request%22%20%3A%20%7B%0
A%20%20%20%20%22requestType%22%20%3A%20%22DELETE%22%2C%0A%20%20%20%20%22operat
ionType%22%20%3A%20%22DELETE%22%2C%0A%20%20%20%20%22contextOwner%22%20%3A%20%2

Copyright © 2019, 2026, Oracle and/or its affiliates.

2PCF_UE%22%2C%0A%20%20%20%20%22contextId%22%20%3A%20%22e5c1d501-7761-409a-895c-
ed17d224ba99%22%2C%0A%20%20%20%20%22notificationInfo%22%20%3A%20null%0A%20%20%7D%2C%0A%20%20%22dnn%22%20%3A%20%22NA%22%2C%0A%20%20%22sliceinfo%22%20%3A%20%7B%0A%20%20%20%20%22sd%22%20%3A%20%22NA%22%2C%0A%20%20%20%20%22sst%22%20%3A%20%22NA%22%0A%20%20%7D%2C%0A%20%20%22supi%22%20%3A%20%22imsi-450081000000018%22%2C%0A%20%20%22gpsi%22%20%3A%20%22msisdn-10000000018%22%0A%7D&reqParam=%7B%0A%20%20%22ssvEnabled%22%20%3A%20false%2C%0A%20%20%22resetContextSSV%22%20%3A%20false%0A%7D","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":1349,"threadPriority":5,"messageTimestamp":"2022-11-23T09:21:00.377+0000"}

{"instant":
{"epochSecond":1669195260,"nanoOfSecond":378500887},"thread":"SimpleAsyncTaskExecutor-57289","level":"DEBUG","loggerName":"ocpm.pcf.service.uepolicy.client.LoggingInterceptor","message":"Sending http request:
Request2f16511d\n[\n\tDELETE http://ross-helm-occnp-egress-gateway:8000/namf-comm/v1/ue-contexts/imsi-450081000000018/n1-n2-messages/subscriptions/1234\n\t3gpp-sbi-target-apiroot: http://nf1stub.ross-ns.svc:8080\n\toc-access-token-request-info: {\"targetNfType\":\"AMF\",\"scope\":\"namf-comm\"}
\n\t3gpp-Sbi-Max-Rsp-Time: 3000\n\t3gpp-Sbi-Sender-Timestamp: Wed, 23 Nov 2022 09:21:00.377 GMT\n\tContent-Length: 0\n\tHost: ross-helm-occnp-egress-gateway:8000\n\tConnection: Keep-Alive\n\tAccept-Encoding: gzip\n\tUser-Agent: okhttp/
4.9.3\n]","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":68288,"threadPriority":5,"messageTimestamp":"2022-11-23T09:21:00.378+0000"}

{"instant":
{"epochSecond":1669195260,"nanoOfSecond":425336983},"thread":"pool-3-thread-11","level":"INFO","loggerName":"ocpm.pcf.service.uepolicy.serviceconnector.PolicyServiceConnector","message":"Ready to send Policy Request to Policy Engine Service: http://ross-helm-occnp-pre:8000/v1/policy/engine/pcf-ue,
{\"requestType\":\"AMF\",\"operationType\":\"TERMINATE\",\"policyAssociationRequest\":{\"notificationUri\":\"http://10.233.14.139:8080/amcs/v1/uepc-status\",\"supi\":\"imsi-450081000000018\",\"gpsi\":\"msisdn-10000000018\",\"accessType\":\"3GPP_ACCESS\",\"pei\":\"imeisv-9902267900440101\",\"userLoc\":
{\"nrLocation\":{\"tai\":{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"tac\":\"004743\"},\"ncgi\":{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"nrCellId\":\"000000000\"}}},\"servingPlmn\":{\"mnc\":\"05\",\"mcc\":\"450\"},\"ratType\":\"NR\",\"guami\":{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"},\"suppFeat\":\"def\"},\"policyAssociation\":{\"request\":{\"notificationUri\":\"http://
10.233.14.139:8080/amcs/v1/uepc-status\",\"supi\":\"imsi-450081000000018\",\"gpsi\":\"msisdn-10000000018\",\"accessType\":\"3GPP_ACCESS\",\"pei\":\"imeisv-9902267900440101\",\"userLoc\":
{\"nrLocation\":{\"tai\":{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"tac\":\"004743\"},\"ncgi\":{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"nrCellId\":\"000000000\"}}},\"servingPlmn\":{\"mnc\":\"05\",\"mcc\":\"450\"},\"ratType\":\"NR\",\"guami\":{\"plmnId\":
{\"mcc\":\"450\",\"mnc\":\"05\"},\"amfId\":\"010041\"},\"suppFeat\":\"def\"},\"triggers\":[],\"suppFeat\":\"0\"},\"user\":
{\"subscription\":false}}","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":1353,"threadPriority":5,"messageTimestamp":"2022-11-23T09:21:00.425+0000"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

```
{"instant":
{"epochSecond":1669195260,"nanoOfSecond":520217022},"thread":"pool-3-
thread-12","level":"DEBUG","loggerName":"ocpm.cne.common.db.JdbcTable","messag
e":"trying to execute sql : delete from UePolicyAssociation where k
= ?","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":1356,"threadPriority":5,"messageTimestamp":"2022-11-23T09:21:00.520+0
000"}
{"instant":
{"epochSecond":1669195260,"nanoOfSecond":525313719},"thread":"pool-3-
thread-12","level":"DEBUG","loggerName":"ocpm.cne.common.db.JdbcTable","messag
e":"deleted 1 records from table UePolicyAssociation with key
e5c1d501-7761-409a-895c-
ed17d224ba99","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jL
ogger","threadId":1356,"threadPriority":5,"messageTimestamp":"2022-11-23T09:21
:00.525+0000"}
```


4.129 Handling Stale Data in PDS

Policy supports handling the stale PDS subscriber data for the following services:

- SM Service
- AM Service
- UE Policy Service

When there is no existing session for the subscriber

When a policy service receives request for a new session from an external NF, it sends a GET request to PDS to fetch the user or the subscriber data.

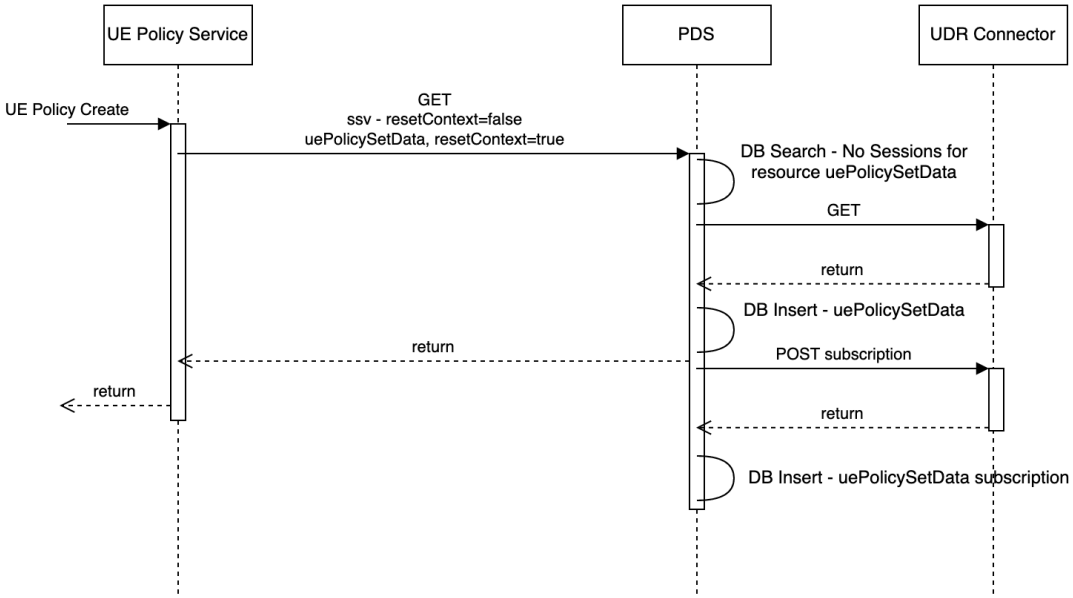
If resetContextSmPolicyData, resetContextAmPolicyData, or resetContextUePolicySetData flag set to true
If it is a new session for the subscriber, there will be no session information for the subscriber in the respective policy service database. While sending the GET request to PDS, the policy service sets the value of the `resetContextSmPolicyData`, `resetContextAmPolicyData`, or `resetContextUePolicySetData` flag to `true`.

PDS sends a GET request to UDR Connector to fetch the user or the subscription data for the subscriber. According to the response, PDS updates the subscriber data in PolicyDS database.

Also, as there is no existing session information in PolicyDS database, PDS sends a POST subscription request to UDR Connector to create a subscription. After it receives a response from the UDR Connector, PDS inserts the subscription details to its database and returns the same to the policy service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-271 resetContextUePolicySetData set to true when there are no existing sessions for UE Policy service



When there are existing sessions for the subscriber

When a policy service receives request for a new session from an external NF, it sends a GET request to PDS to fetch the SSV and the subscription data.

If resetContextSmPolicyData, resetContextAmPolicyData, or resetContextUePolicySetData flag set to false

If there are existing sessions for the subscriber, while sending the GET request to PDS, the policy service sets the value of the `resetContextSmPolicyData`, `resetContextAmPolicyData` or `resetContextUePolicySetData` flag to `false`.

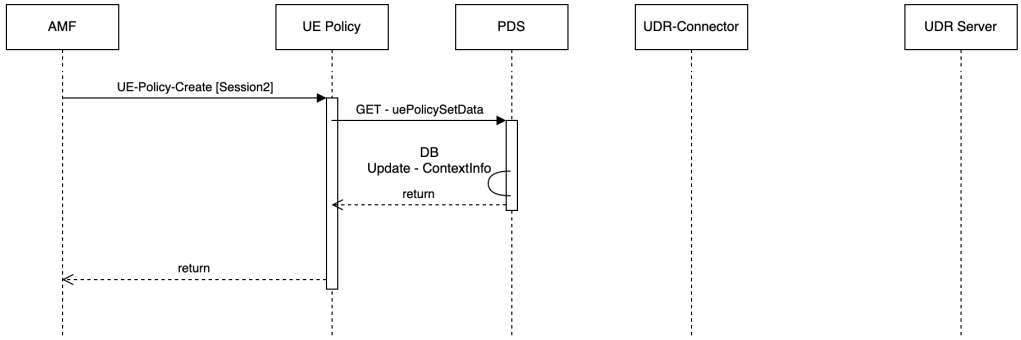
As `resetContextSmPolicyData`, `resetContextAmPolicyData` or `resetContextUePolicySetData` flag is set to `false`, PDS does not attempt to get the data from UDR Connector.

PDS updates the PolicyDS database as per the request received from the policy service. It responds to the policy service with the data present in PolicyDS database.

If `CONCURRENT_REQUEST_GUARD_TIME` is configured, PDS removes the sessions which are older than the guard time.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-272 resetContextUePolicySetData set to false when there are existing sessions for UE Policy service



Revalidation of the subscriber data in PDS

If the revalidation configuration is enabled for PDS, that is, if `Enable Fetch and Resubscribe` is set to `true`, and there is already existing information for the subscriber in its database, if the number of sessions exceeds the `Max Sessions Count`, PDS sends a GET request to re-fetch the subscription data from UDR Connector.

PDS sends a subscription request to UDR Connector with the stored subscription details from its PolicyDS database.

The parameters in reqParam or Headers in the request to UDR Connector indicates whether UDR Connector should send a GET request or a PUT request to UDR for subscription. If `oc-replace-put-with-get` in the request header is disabled, UDR Connector sends a PUT request to UDR for the Policy data subscription. If `oc-replace-put-with-get` in the request header is enabled, UDR Connector sends a GET request to UDR for the Policy data subscription.

If the subscription details are validated successfully, UDR Connector responds with a 200 ok message.

If the validation fails and UDR sends a `404-NOT FOUND` or any other 4xx/5xx error response, UDR Connector forwards the error response to PDS.

If Error Handling is disabled in PDS

If Error Handling is disabled in PDS, PDS sends a POST subscription request to UDR Connector to create a subscription. UDR Connector forwards the POST subscription request to UDR Server. If UDR Server responds with a `204 created` response for the POST subscription request, UDR Connector forwards the response to PDS with the subscription details received from UDR Server. PDS inserts the subscription details to the PolicyDS database and returns the same to the policy service.

If UDR sends a 4xx/5xx error response for the POST subscription request, UDR Connector forwards the error response to PDS.

PDS removes the existing subscription details from PolicyDS database and sends an unsuccessful response to the requester Policy service (SM service, AM service, or UE Policy service).

If Error Handling is enabled in PDS

If Error Handling is enabled in PDS, and PDS receives a `404 NOT FOUND` response from UDR for the GET request and if `HTTP_POST_ON_404_GET_REVALIDATION_RESPONSE_ENABLED`

Copyright © 2019, 2026, Oracle and/or its affiliates.

parameter is enabled in the request header, PDS removes the subscription information from the header and sends a POST request to UDR.

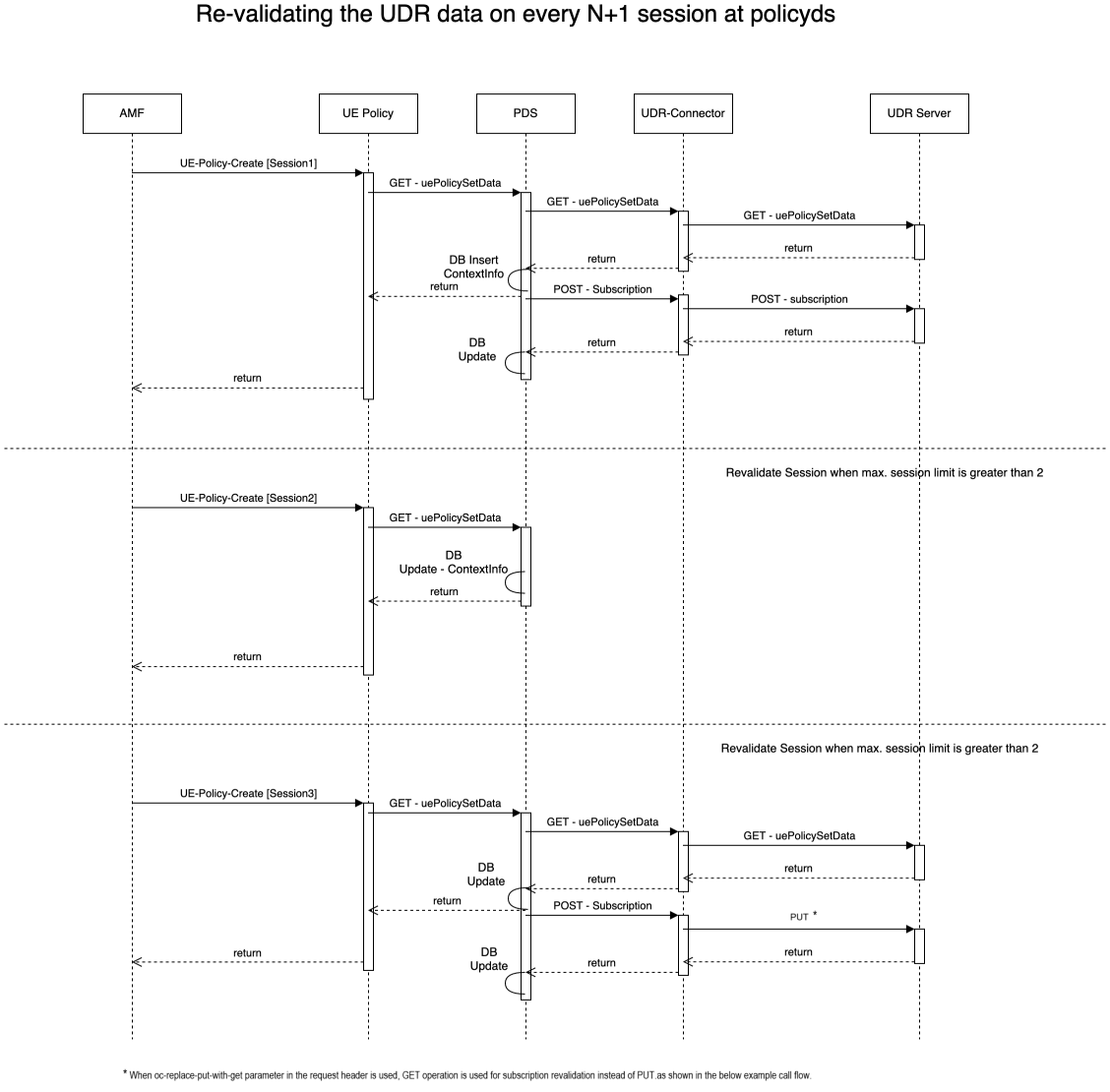
If PDS receives any other 4xx/5xx error response from UDR for the GET request, PDS verifies the Error Code Configuration and accordingly handles the resubscribe call flow. PDS removes the `DataSourceInfo` from the request header and sends a POST subscription request to UDR Connector, which in turn forwards the request to UDR. If the subscription is successful, UDR responds with a `204 Created` message with the subscription details. PDS updates the details in PolicyDS database.

If UDR responds with a 4xx/5xx error response for the POST subscription request, PDS removes the subscription details from PolicyDS database and sends an unsuccessful response to Policy service (SM service, AM service, or UE Policy service) indicating subscription revalidation failure.

Example:

Here is an example call flow for revalidation of the subscription data for UE Policy Service sessions.

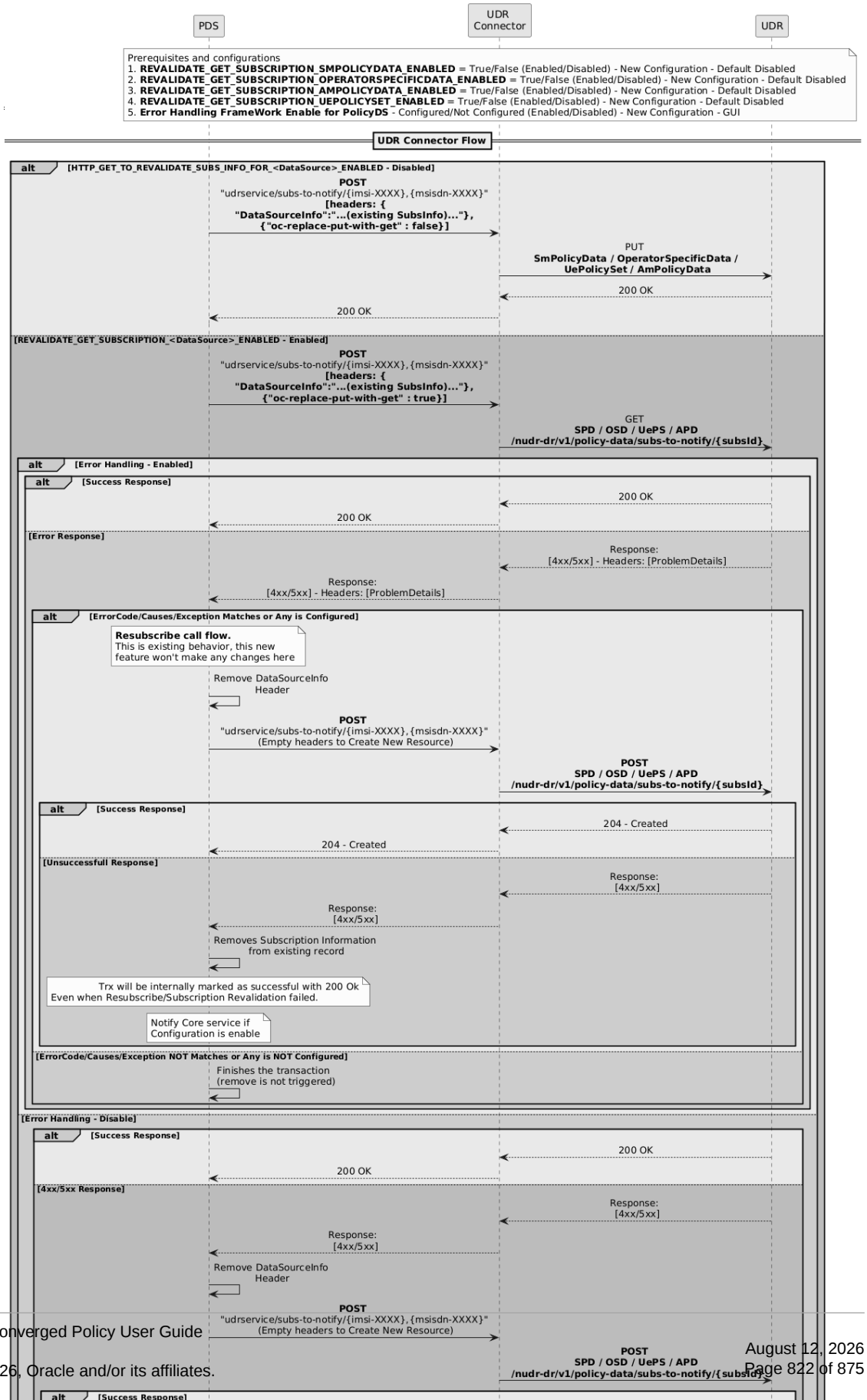
Figure 4-273 Revalidation of the subscription data for UE Policy Sessions



* When oc-replace-put-with-get parameter in the request header is used, GET operation is used for subscription revalidation instead of PUT.as shown in the below example call flow.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-274 Example call flow to show use of PUT or GET operation for subscription revalidation depending on the configuration of oc-replace-put-with-get in the request header.



Copyright © 2019, 2026, Oracle and/or its affiliates.

Managing Handling PDS Stale Sessions

Enable

You can enable `resetContextSmPolicyData`, `resetContextAmPolicyData` and `resetContextUePolicySetData` flags in `custom-values.yaml` file and also using the following Advanced settings keys:

- `USER.RESET_CONTEXT_SM_POLICY_DATA_ON_SM_CREATE`
- `USER.RESET_CONTEXT_AM_POLICY_DATA_ON_AM_CREATE`
- `USER.RESET_CONTEXT_UE_POLICY_DATA_ON_UE_CREATE`

.

For more information on the Advanced Settings keys, see

- PCF Session Management
- PCF Access and Mobility
- PCF UE Policy Service

For more information about the resetContext flags for SM Service, AM Service and UE Policy Service, see *Customizing Policy* chapter *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

To enable the PDS revalidation functionality:

You can enable the PDS revalidation functionality using the CNC Console or REST API for Policy.

- **Enable using CNC Console**:
  To enable the PDS revalidation functionality using the CNC Console, set the value of **Enable Fetch and Resubscribe** flag to `true` in the **PDS** page.

  For more details about **Enable Fetch and Resubscribe** flag, see PDS.

  To enable, the error handling for PDS service, navigate to **Error Configurations** page under **Error Handling**, select `policyds` from the **Select Service Name** dropdown, and enable **Enable Error Handler Configurations** button. For more information, see Error Configurations.
- **Enable using REST API**:
  To enable the PDS revalidation functionality, set the value as `true` for **enableFetchAndResubscribe** parameter under the Common group in the `{apiRoot}/oc-cnpolicy-configuration/v1/services/pds/pdsSettings` REST API.

  For more details on enabling the flag using REST API, see *Policy REST Specifications* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Configure

You can configure `resetContextSmPolicyData`, `resetContextAmPolicyData` and `resetContextUePolicySetData` flags in `custom-values.yaml` file and also using the following Advanced settings keys:

- `USER.RESET_CONTEXT_SM_POLICY_DATA_ON_SM_CREATE`
- `USER.RESET_CONTEXT_AM_POLICY_DATA_ON_AM_CREATE`
- `USER.RESET_CONTEXT_UE_POLICY_DATA_ON_UE_CREATE`

Copyright © 2019, 2026, Oracle and/or its affiliates.

.

For more information on the Advanced Settings keys, see

- PCF Session Management
- PCF Access and Mobility
- PCF UE Policy Service

For more information about the resetContext flags for AM Service and UE Policy Service, see *Customizing Policy* chapter *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

To configure usage of PUT or GET operation for subscriber data revalidation from UDR, configure the following Advanced Settings keys on **PDS Settings** page:

- ENABLE_ERROR_HANDLING_FOR_REVALIDATION
- PDS_ERROR_HANDLER_ENABLED
- REVALIDATE_GET_SUBSCRIPTION_SMPOLICYDATA_ENABLED
- REVALIDATE_GET_SUBSCRIPTION_OPERATORSPECIFICDATA_ENABLED
- REVALIDATE_GET_SUBSCRIPTION_AMPOLICYDATA_ENABLED
- REVALIDATE_GET_SUBSCRIPTION_UEPOLICYSET_ENABLED

For more information, see PDS Settings.

To enable the PDS revalidation functionality:

You can configure the PDS revalidation functionality to handle the stale PDS data using the CNC Console or REST API for Policy.

- **Configure using CNC Console**:
  To configure PDS revalidation functionality in PDS, perform the feature configurations on **PDS** page. For more details, see PDS.
- **Configure using REST API**: Policy provides {apiRoot}/oc-cnpolicy-configuration/v1/services/pds/pdsSettings REST API to configure the PDS revalidation functionality.

> **Note**
>
> In case of PDS subscriber data revalidation for UE and AM policy services, the value of DNN, SD and SST parameters must be `NA`.

To configure error handling for PDS

To configure the error handling for PDS service, navigate to **Error Configurations** page under **Error Handling**, select `policyds` from the **Select Service Name** dropdown, and perform the **Error Handler Templates of policyds** configurations. For more information, see Error Configurations.

Observe

Metrics

The following metrics are used to support the PDS revalidation functionality:

Metrics in PDS:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- revalidation_request
- revalidation_response

Metrics in UDR:

- ocpm_udr_tracking_response_total
- ocpm_udr_tracking_request_total
- ocpm_udr_tracking_request_timeout_total

For details on the metrics, see UDR Metrics.

Alerts

The following alerts are triggered when the number of 404 unsuccessful revalidation responses from UDR for GET request from PDS cross certain threshold value in a given time period:

- UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT
- UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT
- UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT

The following alerts are triggered when the number of unsuccessful revalidation responses other than 404 errors from UDR for the GET request from PDS cross certain threshold value in a given time period:

- UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT
- UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT
- UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Logging

Below is the sample log from Policy-ds when MaxSessionLimit is hit for revalidation.


```
{"instant":
{"epochSecond":1669192175,"nanoOfSecond":908706032},"thread":"boundedElastic-2
9","level":"DEBUG","loggerName":"ocpm.uds.policyds.workflow.flowtask.dbtask.Ab
stractDBFlowTask","message":"Comparing Existing Dnn Slice count Map :
{NA:NA:NA=1} with Configured Max Dnn Slice Count
        Map : {NA:NA:NA=1}
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":7491,"threadPriority":5,"messageTimestamp":"2022-11-23T08:29:35.908+0000
"}{"instant":
{"epochSecond":1669192175,"nanoOfSecond":909143676},"thread":"boundedElastic-2
9","level":"INFO","loggerName":"ocpm.uds.policyds.workflow.flowtask.dbtask.Abs
tractDBFlowTask","message":"Revalidation is required so going to fetch
updated data for source type:

SpendingLimitData","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.L
og4jLogger","threadId":7491,"threadPriority":5,"messageTimestamp":"2022-11-23T
08:29:35.909+0000"}  {"instant":
{"epochSecond":1669192175,"nanoOfSecond":910933620},"thread":"boundedElastic-2
9","level":"DEBUG","loggerName":"ocpm.uds.policyds.workflow.flowtask.dbtask.Ab
stractDBFlowTask","message":"Comparing Existing Dnn Slice count Map :
{NA:NA:NA=1} with Configured Max Dnn Slice Count
        Map : {NA:NA:NA=1}
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":7491,"threadPriority":5,"messageTimestamp":"2022-11-23T08:29:35.910+0000
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
"}{"instant":
{"epochSecond":1669192175,"nanoOfSecond":911364865},"thread":"boundedElastic-2
9","level":"INFO","loggerName":"ocpm.uds.policyds.workflow.flowtask.dbtask.Abs
tractDBFlowTask","message":"Revalidation is required so going to fetch
updated data for source type:

AmPolicyData","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jL
ogger","threadId":7491,"threadPriority":5,"messageTimestamp":"2022-11-23T08:29
:35.911+0000"} {"instant":
{"epochSecond":1669192175,"nanoOfSecond":915496199},"thread":"boundedElastic-2
9","level":"INFO","loggerName":"ocpm.uds.policyds.rest.client.WebClientService
Impl","message":"Req
        body{\"amPolicyDataReq\":
{\"subscription\":false,\"params\":null,\"resetContext\":false,\"processEtag\"
:false},\"ssvEnabled\":false,\"resetContextSSV\":false}
        sent to URL http://ross-helm-occnp-udr-connector:8000/userservice/user-data/
imsi-450081000000024,msisdn-12345678901234 with
        header {uber-trace-id=[a398635f494761ab:a398635f494761ab:0:0,
        37b688bf4531ac85:37b688bf4531ac85:0:0],
          oc-data-source-route-info=[{\"amPolicyData\":{\"dataSourceInfo\":
{\"dataSourceId\":\"fe7d992b-0541-4c7d-ab84-555552222222:94d8d19a-
b0d9-4d6d-994f-39a49ed5c111\",\"host\":\"nf1stub.ross-
ns.svc\",\"port\":8080},\"subscriptionResourceInfo\":
{\"subscriptionId\":\"http://nf1stub.ross-ns.svc:8080/nudr-dr/v1/policy-data/subs-to-notify/
1\",\"host\":\"nf1stub.ross-ns.svc\",\"port\":8080,\"subscriptionData\":\"{\\
\"policyDataSubscription\\\":{\\\"notificationUri\\\":\\\"https://ross-helm-occnp-
ingress-gateway:443/udrservice/notification/imsi-450081000000024\\\",\\
\"monitoredResourceUris\\\":[\\\"http://nf1stub.ross-ns.svc:8080/nudr-dr/v1/policy-data/ues/
imsi-450081000000024/am-data\\\"],\\\"supportedFeatures\\\":\\\"f\\\"}}
\"},\"nfBindingInfo\":{},\"otherAttr\":{\"processETag\":false}}}]}

","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":7491,"threadPriority":5,"messageTimestamp":"2022-11-23T08:29:35.915+0000
"} {"instant":
{"epochSecond":1669192175,"nanoOfSecond":922192005},"thread":"boundedElastic-2
9","level":"INFO","loggerName":"ocpm.uds.policyds.rest.client.WebClientService
Impl","message":"Req bodynull sent to URL http://ross-helm-occnp-chf-connector:8000/
chfservice/spending-limit/imsi-450081000000024?
gpsi=msisdn-12345678901234&plmn.mcc=460&plmn.mnc=30&asyncQuery=false&resetContext=false
with
        header {uber-trace-id=[a398635f494761ab:a398635f494761ab:0:0,
        37b688bf4531ac85:37b688bf4531ac85:0:0,
bc38f03768302c41:bc38f03768302c41:0:0],
        3gpp-Sbi-Max-Rsp-Time=[2700],
          oc-data-source-route-info=[{\"spendingLimitStatus\":
{\"dataSourceInfo\":{\"dataSourceId\":\"fe7d992b-0541-4c7d-
ab84-666666666666:chf1\",\"host\":\"nf1stub.ross-
ns.svc\",\"port\":8080},\"subscriptionResourceInfo\":
{\"subscriptionId\":\"http://nf1stub.ross-ns.svc/nchf-spendinglimitcontrol/v1/subscriptions/
1\",\"host\":\"nf1stub.ross-ns.svc\",\"port\":8080},\"nfBindingInfo\":
{},\"otherAttr\":{}}}]}

","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":7491,"threadPriority":5,"messageTimestamp":"2022-11-23T08:29:35.922+0000
"}
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

4.130 Support for User-Agent Header

User-Agent header helps the producer Network Function (NF) to identify the consumer NF that has sent the request. To implement this, 3GPP introduced the use of User-Agent header for consumers to include the same in service requests. Additionally, producers may require to support the validation of the User-Agent headers to complete the request identification process in the network.

With the integration of this feature, User-Agent header helps the producer Network Function (NF) to identify the consumer NF that has sent the request.

The following format is used to generate User-Agent header:

<NF Type>-<Instance-Id> <FQDN>

where, `<NF Type>` is the type of the Network Function.

`<Instance-Id` is the instance ID of the NF.

`<FQDN>` is the FQDN of the NF.

Example: `PCF-54804518-4191-46b3-955c-ac631f953ed8 pcf1.east.5gc.mnc012.mcc234.3gppnetwork.org`

There is no configuration required at PCF for incoming user-agent header. By default, PCF validates the format of the user-agent header and updates the ingress metrics.

When the User-Agent header is missing in the incoming requests sent to PCF then the corresponding metric will not be able to retrieve information from whom it is requesting the service. Nonetheless, the request will be fulfilled without any issues.

For the generation of the User-Agent header when it is enabled through Helm configurations and header information is missing, then it will be picked from the OAuthClient module to generate the header.

If the User-Agent header is present in the request towards Policy, then the value present in the header is overwritten or forwarded based on the `overwriteHeader` flag. If the flag is set to true, then the header is overwritten.

> **Note**
>
> `nfInstanceId` and `nfType` are picked from `userAgentHeader` configuration, if available. Otherwise, they are picked from `oauthClient` configuration. This does not require oauthClient to be enabled but mandates oauth client configuration to be present. If `nfInstanceId` and `nfType` are not available in both oauth client configurations and in User-Agent configuration, then the startup probe fails.

The header is applied to every outgoing message generated from Egress Gateway that includes the SMF, UE, and AM interfaces.

Managing Support for User-Agent Header

Enable

You can enable the User-Agent Header feature using REST or Helm configuration.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Helm: Set the value of the parameter `userAgentHeaderValidationConfigMode` to Helm in the custom-values.yaml file. For more information, see the *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.
- REST API: Set the value of the parameter `userAgentHeaderValidationConfigMode` to REST in the custom-values.yaml file. REST configuration from the JSON bodies sent to path: "*/pcf/nf-common-component/v1/egw/useragentheader*" is stored in a database under the common_config table. For more information, see the *Oracle Communications Cloud Native Core, Converged Policy REST Specifications Guide*.

Configure

You can configure the User-Agent Header using REST or Helm.

Following is a sample configuration for User-Agent Header in custom-values.yaml.file:

```
userAgentHeaderConfigMode: HELM
userAgentHeader:
  enabled: false # flag to enable or disable the feature
  nfType: "PCF" # NF type of consumer NF
  nfInstanceId: "2d8e8e68-24ad-11ed-861d-0242ac120002" # NF type of consumer
NF
  addFqdnToHeader: true # Flag to add fqdn. If enabled then user-agent header
will be
generated along with the fqdn configured otherwise fqdn will not be added
  nfFqdn: "oracle1.pcf.pacific.org" #fqdn of NF. This is not the fqdn of
gateway
  overwriteHeader: true
```

To configure the User-Agent header at Egress Gateway using REST API, see user-Agent Header in *Oracle Communications Cloud Native Core, Converged Policy REST Specifications Guide*.

Observe

Policy provides the following metric specific to User-Agent Header feature:

- oc.ingressgateway.http.requests

For more information, see User-Agent Header Metrics section.

4.131 Support for Spending Limit Status Reporting

Policy provides an option to enable spending limit status in each of the create, update, and delete requests from the Policy Services (SM Service, AM Service, and UE Policy Service).

The Spending Limit control service enables the Policy services to retrieve policy counter status information per subscriber from CHF.

That is, by subscribing to spending limit reporting (CHF Data), Policy services can receive notifications on Policy Counters from CHF.

PolicyDS handles the cases when multiple services subscribe to spending limit reporting as follows:

When one service subscribes to a given policy counter, another service subscribes for another policy counter, then PDS takes the policy counters from the last request and both services are subscribed to receive notifications for those policy counters.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For example:

If UE Policy Service subscribes for PC1 and PC2 and AM Service subscribes for PC3, both UE Policy Service and AM Service will receive notification only for PC3.

Whenever there is create, update, and delete requests from the Policy Services (SM Service, AM Service, and UE Policy Service), Policy checks if CHF Data flag is enabled. If the CHF Data flag is enabled, it allows interaction between PDS and CHF through CHF Connector to retrieve the CHF data,

Policy allows subscription to Spending Limit Control service (`Nchf_SpendingLimitControl_Subscribe`), which provides notification of changes in the status of the policy counters available and to retrieve the status of the policy counters for which the subscription is accepted.

That is, it provides:

- initial spending limit retrieval
- intermediate spending limit report retrieval

Also, Policy allows asynchronous interaction between PDS and CHF when `Async CHF Query Enabled` flag is set to `true` in the respective service configuration for SM service, AM service, or UE Policy service.

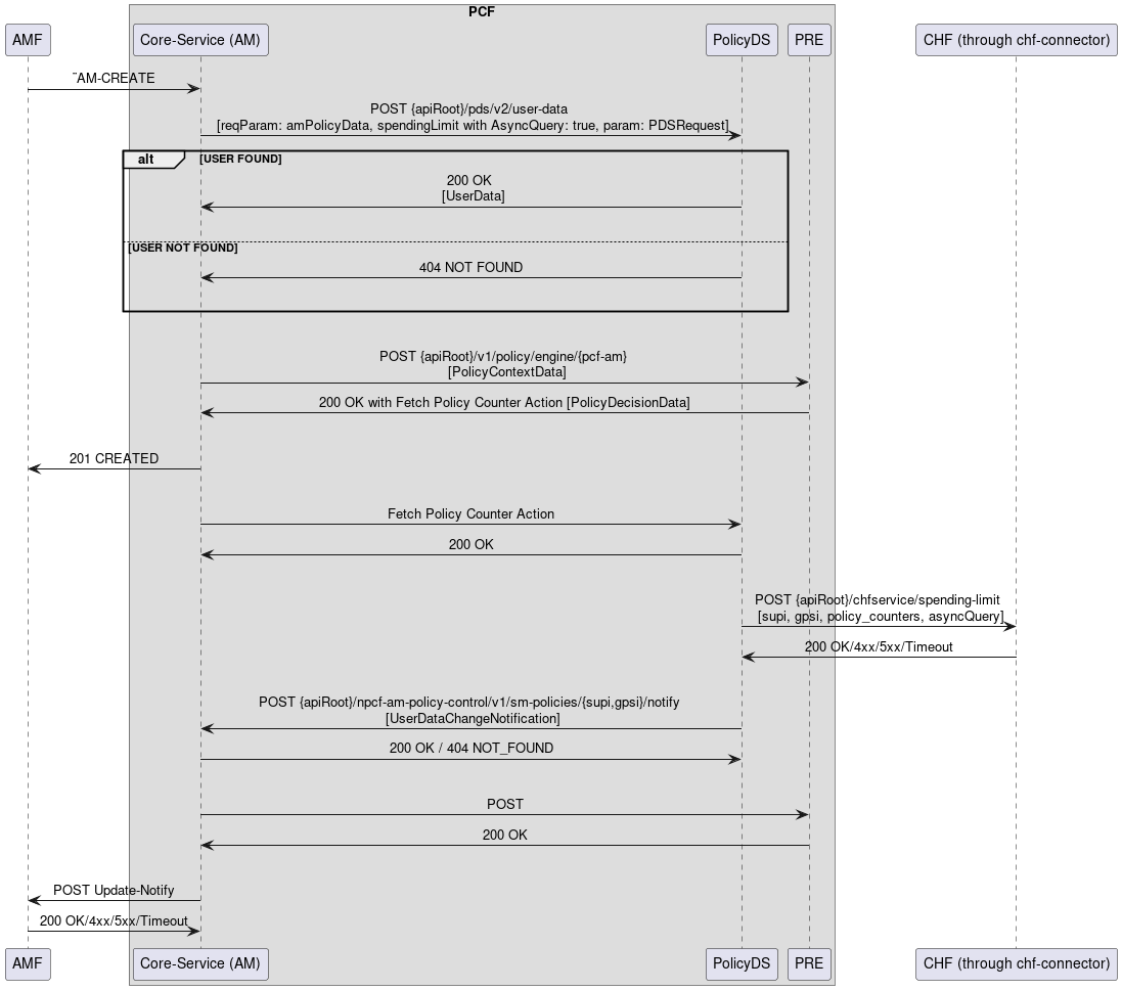
> **Note**
>
> For AM and UE Policy service, this feature supports only asynchronous flow.

Call Flow

Below is an example for retrieving CHF Data for AM Service:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-275 Spending limit status report for AM Service



Subscription create:

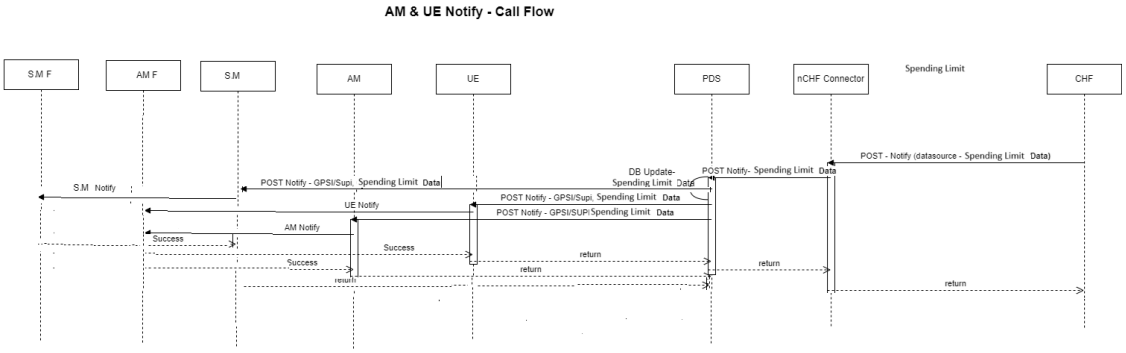
1. AM Service receives request for a new session from AMF.
2. AM Service checks if CHF Data flag is enabled.
3. AM Service sends a GET request to PDS to fetch the user data. If Async CHF Query Enabled flag is also enabled, it sets AsyncQuery to true in the request parameters.
4. If the user data is present in PolicyDS database, PDS responds to AM Service with 200 OK message.
5. If the requested data is not present in PolicyDS, PDS responds to AM Service with a 404 NOT FOUND message. PDS sends a request to UDR through UDR Connector to fetch the UserData.
6. AM Service, sends a POST request to PRE. Using the fetch policy counter blockly AM identifies the policy counters for which the information is requested.
7. After receiving a 200 OK response from PRE, AM Service sends a 201 created message to AMF.
8. AM sends another request to PDS of type REQUEST-PC. Since this REQUEST-PC flow is asynchronous, PDS responds immediately with a 204 OK message to AM.

Copyright © 2019, 2026, Oracle and/or its affiliates.

9. In asynchronous way, PDS contacts CHF through CHF Connector to subscribe for the policy counters that PRE returned to AM Service.
10. After receiving the information from CHF, PDS sends a notification to AM Service with the SpendingLimit data.
11. AM Service processes this information and if needed it sends an update notify to AMF Service.

Notification call flow from CHF to SM service, AM service, and UE Policy service

Figure 4-276 Update notification to SM service, AM service, and UE Policy service



Whenever CHF detects that the status of a policy counter(s) has changed, it sends a notification to PDS.

1. The change notification can be generated for any of the following reasons.
   a. Change in status of Policy counters.
   b. Future change in status of policy counters along with time at which it will change.
   c. Policy counter identifier is no longer applicable to subscriber.
2. The update notification can include:
   - SUPI
   - GPSI
   - Policy counter status as event information
   - Pending policy counter statuses and their activation times as event information
3. PDS updates its database and sends a POST request to SM Service, AM Service or UE Service.
4. SM Service, AM Service or UE Policy Service processes the notification and if required it sends an update notify to SMF or AMF respectively.
5. SM Service, AM Service and UE Policy Services accept the message and respond with a 204 No content message back to CHF through PDS and CHF connector.

Intermediate spending limit report transaction from the CHF

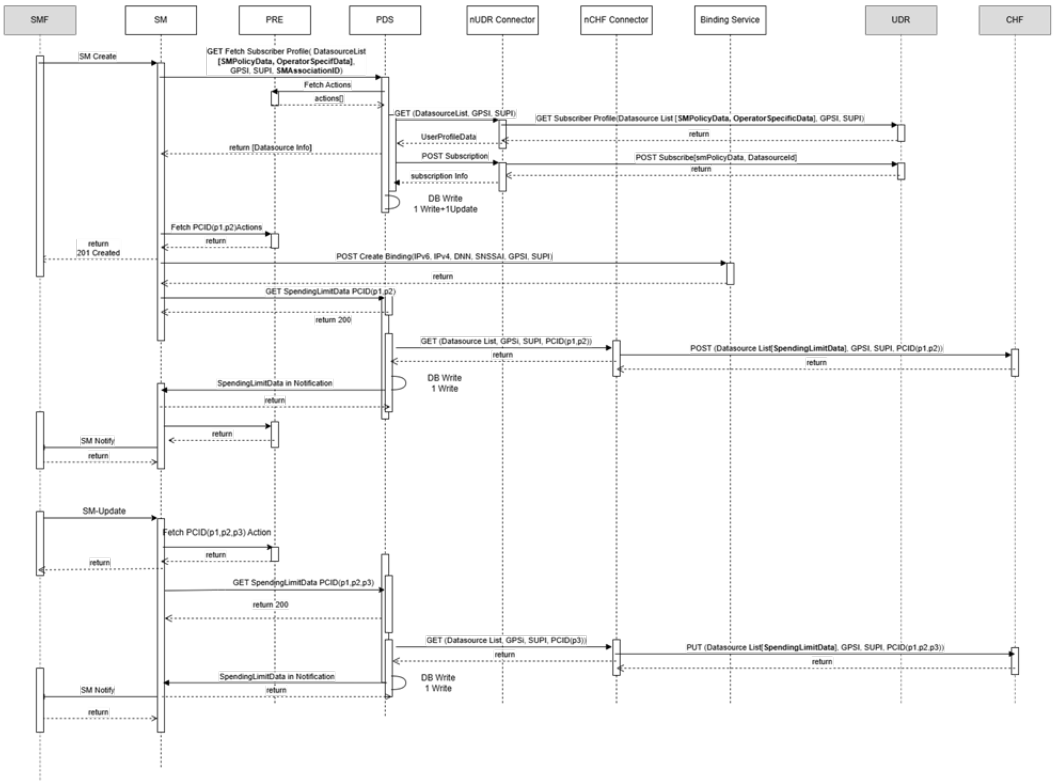
CHF provides an intermediate spending limit report transaction containing pending policy counter statuses and their activation times for a previously provided policy counter.

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. PDS forwards the details to SM Service, AM Service and UE Policy Service. The Policy services replaces the existing pending policy counter statuses and their activation times if any in their respective databases.
2. If the intermediate spending limit report transaction from the CHF includes no pending policy counter statuses and their activation times are included for a policy counter, the Policy services cancels all the previously provided pending policy counter statuses and their activation times for that particular policy counter.

Below is an example for retrieving intermediate spending limit with specific policy counter Id by SM service.

Figure 4-277 Intermediate Spending Limit with Specific Policy Counter ID for SM Service



1. SM service receives a CREATE request from SMF and it sends a request to PDS to fetch the subscriber profile.
2. PDS interacts with PRE to fetch the corresponding actions and then sends a request to UDR through nUDR Connector to get the subscriber profile as requested by SM service.
3. UDR queries the UDR database and responds to PDS with User Profile data through nUDR Connector.
4. As this is for a CREATE request, PDS sends a POST request to UDR through nUDR to create a subscription. UDR responds with the subscription details.
5. PDS saves the subscription details in PolicyDS database and responds to SM service with the subscription information.

Copyright © 2019, 2026, Oracle and/or its affiliates.

6. SM service interacts with PRE to fetch the Policy Counters with specific IDs.
7. SM service sends a POST request to Binding service to create session binding. Binding service responds to SM service with the session binding details.
8. SM service sends a request to PDS to get the spending limit data for the Policy Counters specifying the IDs.
9. PDS sends a request to CHF through nCHF Connector to subscribe for the spending limit data for the given Policy Counter IDs and receives a successful response.
10. PDS saves the details received from CHF in PolicyDS database and also responds to SM service with the spending limit data.
11. SM service responds to SMF with the received details for the CREATE request.
12. Whenever SM service receives an UPDATE request from SMF with a specific Policy Counter ID, SM service interacts with PRE to retrieve the corresponding actions from PRE.
13. SM service sends a GET request to PDS to update the spending limit data for the Policy Counter ID.
14. PDS sends a PUT request to CHF through nCHF Connector to update the spending limit data for the given Policy Counter ID and receives a successful response.
15. PDS saves the updated details in PolicyDS database and responds to SM service.
16. In turn, SM service responds to SMF.

Managing Support for Spending Limit Status Reporting

Enable

By default, Spending Limit Status Report feature is not enabled on the Policy deployment. You can enable this functionality using the CNC Console.

To enable this feature for SM Service, enable **CHF Data** flag under **User group** on the **PCF Session Management** page.

To enable this feature for AM Service, enable **CHF Data** flag under **User group** on the **PCF Access and Mobility** page.

To enable this feature for UE Policy Service, enable **CHF Data** flag under **User group** on the **PCF UE Policy** page.

For more details on enabling the flag for SM Service, see PCF Session Management.

For more details on enabling the flag for AM Service, see PCF Access and Mobility.

For more details on enabling the flag for UE Policy Service, see PCF UE Policy Service.

Configure

You can configure the Spending Limit Status Report feature using the CNC Console.

To configure the feature for SM, AM and UE services, perform the feature configurations under the **User** group on the respective service configurations page. For more information, see the following sections:

- PCF Session Management
- PCF Access and Mobility
- PCF UE Policy Service

Observe

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following metrics are added to PDS Service metrics:

- server_request_total
- server_response_total

For more details on these metrics, see Policy DS Metrics.

4.132 NF Scoring for a Site

The NF Scoring feature calculates the score for a site based on Network Function (NF) specific factors such as metrics, alerts, etc. The NF Scoring feature helps the operator to determine the health of a site as compared to other sites. Comparing the NF scores within or across the sites helps the customers to choose the site.

One of the use cases is the Controlled Shutdown feature that allows the operator to partially or completely isolate the site. The NF Scoring feature helps the operators to choose which site to partially or completely isolate based on NF scoring.

App-Info service queries and calculates NF Score as it has the site information.

App Info Scoring Mechanism:

App Info reads the configurations from the common config server to check if NF Scoring functionality is enabled or not. It works in the following ways:

- **Continuous NF Score Calculation:** When the NF Scoring feature is enabled, app info periodically reads the configurations to calculate the score.
- **On-Demand NF Score Calculation:** When the NF Scoring feature is enabled, app info fetches all the factors or criteria to calculate the NF Score. It is real-time fetching of factors and then the NF score is calculated on demand.

> **Note**
>
> NF score will calculate the alerts that contains namespace in the labels and expression.

Table 4-193 NF Scoring Criteria

Factors	Default Score	Formula to calculate Factor Score	Details
TPS	20	min(Current_TPS / Max_TPS * Max_TPS_Score, Max_TPS_Score)	Current_TPS = IGW + EGW + Diameter Ingress + Diameter Egress Max_TPS specifies the maximum TPS. Max_TPS_Score Specifies the maximum score of the TPS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-193 (Cont.) NF Scoring Criteria

Factors	Default Score	Formula to calculate Factor Score	Details
Service	30	A / N * Max_SVC_Score	A = Number of available services N = Number of configured services Max_SVC_Score Specifies the maximum score of the Service Health.
Connection	20	min(Conn_Current / Conn_Total * Conn_Score, Conn_Score)	Conn_current specifies the number of connections from network to Policy. Conn_Total specifies the total number of connections expected from network to Policy. Conn_Score specifies the score for the connection.
Replication_health	30	min(Site_Current / Site_Total * Site_Score, Site_Score)	Site_Total specifies the total number of possible replication links. Site_Current specifies the available active healthy links. Replication_health Score specifies the score for the replication_health.
Locality_Preference	5	NA	The value of Locality_Preference is added for NF score calculation.
Critical_Alerts	2	CrN * Configured_Score	CrN is the Number of active critical alarms. Configured_Score_Critical_Alerts specifies the score configured by the user.
Major_Alerts	1	MaN * Configured_Score	MaN is the Number of active Major alarms. Configured_Score_Major_Alerts specifies the score configured by the user.
Minor_Alerts	0	MiN * Configured_Score	MiN is the Number of active Minor alarms. Configured_Score_Minor_Alerts specifies the score configured by the user.

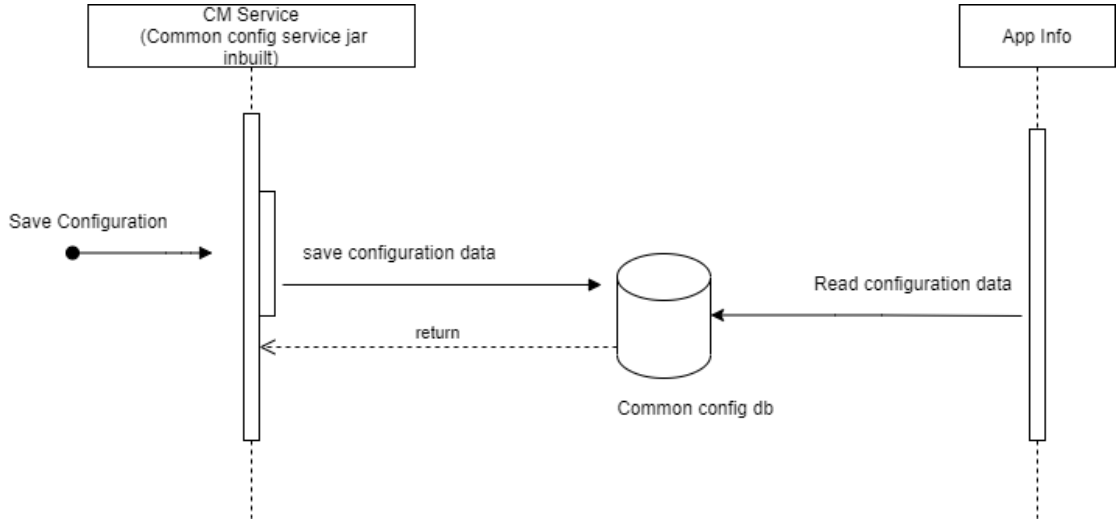
Formula for NF scoring of a site: Sum of TPS_Score, SVC_Score, Conn_Score, Replication_health, and Locality_Preference score subtracted by Alerts scores.

Call Flows

This section describes examples of the call flows for the NF Scoring feature:

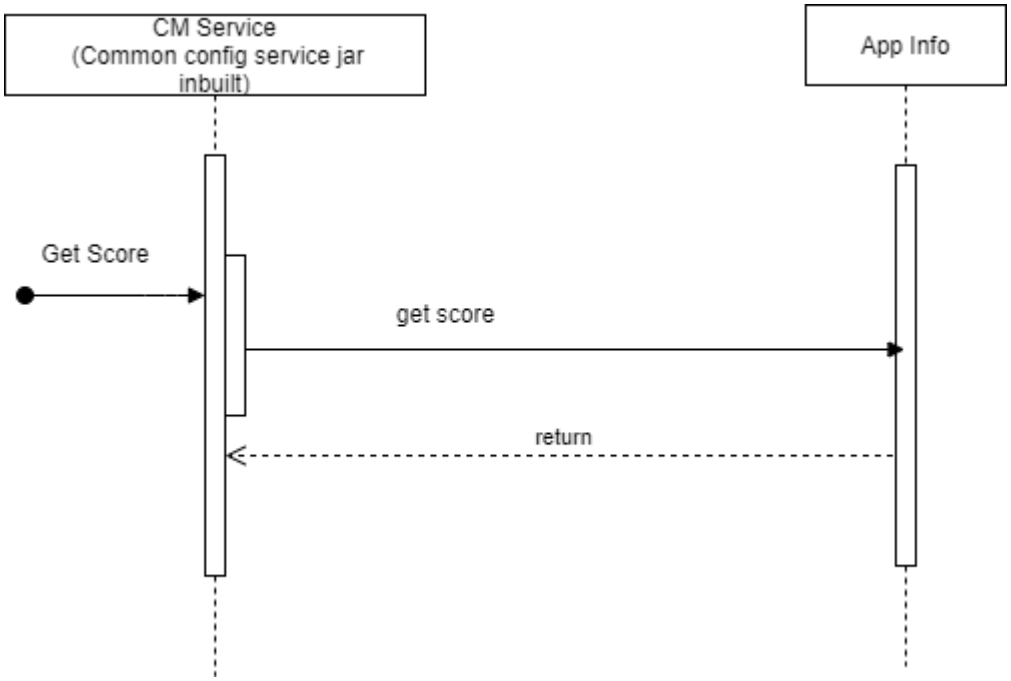
Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-278 Call flow to Save Configuration Data



The operator sends a request to save the configuration is sent to the CM service. It saves the configuration data to the common config database. App-Info reads the configuration data and returns the acknowledgment.

Figure 4-279 Call flow to Get the NF Score



The operator sends a request to CM service to get the score. CM service requests it to App-Info. App-Info queries and calculates NF Score.

Managing NF Scoring for a Site

Enable

Copyright © 2019, 2026, Oracle and/or its affiliates.

You can enable this feature by selecting the **Enable NF Scoring** field in the **Settings** page of **NF Scoring**.

> **Note**
>
> Enabling the NF Scoring feature for the first time, requires configuring `prometheusUrl` and `alertmanagerUrl` under the `appinfo` and `perfinfo` sections in the `custom-yaml`. These Urls get reflected in the config-map of AppInfo and Perf-Info services. For AppInfo and PerfInfo pods to pick up these changes, they need to be restarted.

For more information about enabling the feature through CNC Console, see NF Scoring Configurations .

Configure

Configuring using CNC Console: The NF Scoring feature can be configured through CNC Console. For more information, see NF Scoring Configurations.

> **Note**
>
> You can configure the environment variable, `NF_SCORING_INTERVAL`, in deployment of App-Info. Default value is 30 seconds (changing the environment variable results into restart of App-info pod).

Configuring using REST API: Policy provides the following REST API for configuration: `/oc-cnpolicy-configuration/v1/ nfscore.`

You can perform the GET operation to get NF score. For more information about REST API configuration, see "NF Scoring for a Site" in Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide.

Observability

Metrics

Policy provides the following metrics specific to NF Scoring feature:

- nfscore
- nfScoringFactorActualValue

For more information, see AppInfo Metrics.

4.133 Consistent UDR Updates Using ETag

When two different Policies are connected to UDR in a georedundant setup and both are updating the UsageMonData for the same subscriber simultaneously, there is the possibility of data loss as the update can overwrite each other. ETag (Entity Tag) support helps to make sure that the update is successful only when the consumer has the latest set of data. ETag represents the state of a resource. A consumer service may use conditional HTTP requests to fetch or modify the resource based on its knowledge of the state. Conditional requests are HTTP requests that include one or more header fields indicating a precondition to be tested before applying the method semantics to the target resource. ETag can be either a weak or strong validator, with strong being the default. If an origin server provides an entity-tag for a

Copyright © 2019, 2026, Oracle and/or its affiliates.

representation and the generation of that entity-tag does not satisfy all of the characteristics of a strong validator, then the origin server must mark the entity-tag as weak by prefixing its opaque value with "W/" (case-sensitive).

HTTP Headers

The following HTTP headers are implemented as part of this feature:

Header Name	Description	Example
Etag	The "ETag" header field in a response provides the current entity-tag for the selected representation, as determined at the conclusion of handling the request.	• ETag: "xyzzy" • ETag: W/"xyzzy" • ETag: ""
If-Match	The "If-Match" header field makes the request method conditional on the recipient origin server either having at least one current representation of the target resource, when the field-value is "*", or having a current representation of the target resource that has an entity-tag matching a member of the list of entity-tags provided in the field-value.	• If-Match: "xyzzy" • If-Match: W/"xyzzy" • If-Match: "xyzzy", "r2d2xxxx", "c3piozzzz" • If-Match: "*"
If-Unmodified-Since	The "If-Unmodified-Since" header field makes the request method conditional on the selected representation's last modification date being earlier than or equal to the date provided in the field-value. This field accomplishes the same purpose as If-Match for cases where the user agent does not have an entity-tag for the representation.	If-Unmodified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Last-Modified	The "Last-Modified" header field in a response provides a timestamp indicating the date and time at which the origin server believes the selected representation was last modified, as determined at the conclusion of handling the request.	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT

HTTP Status Codes

Copyright © 2019, 2026, Oracle and/or its affiliates.

HTTP Status Code	Description
412 Precondition Failed	The 412 (Precondition Failed) status code indicates that one or more conditions given in the request header fields evaluated to false when tested on the server. This response code allows the client to place preconditions on the current resource state (its current representations and metadata) and, thus, prevent the request method from being applied if the target resource is in an unexpected state.

HTTP Messages Examples

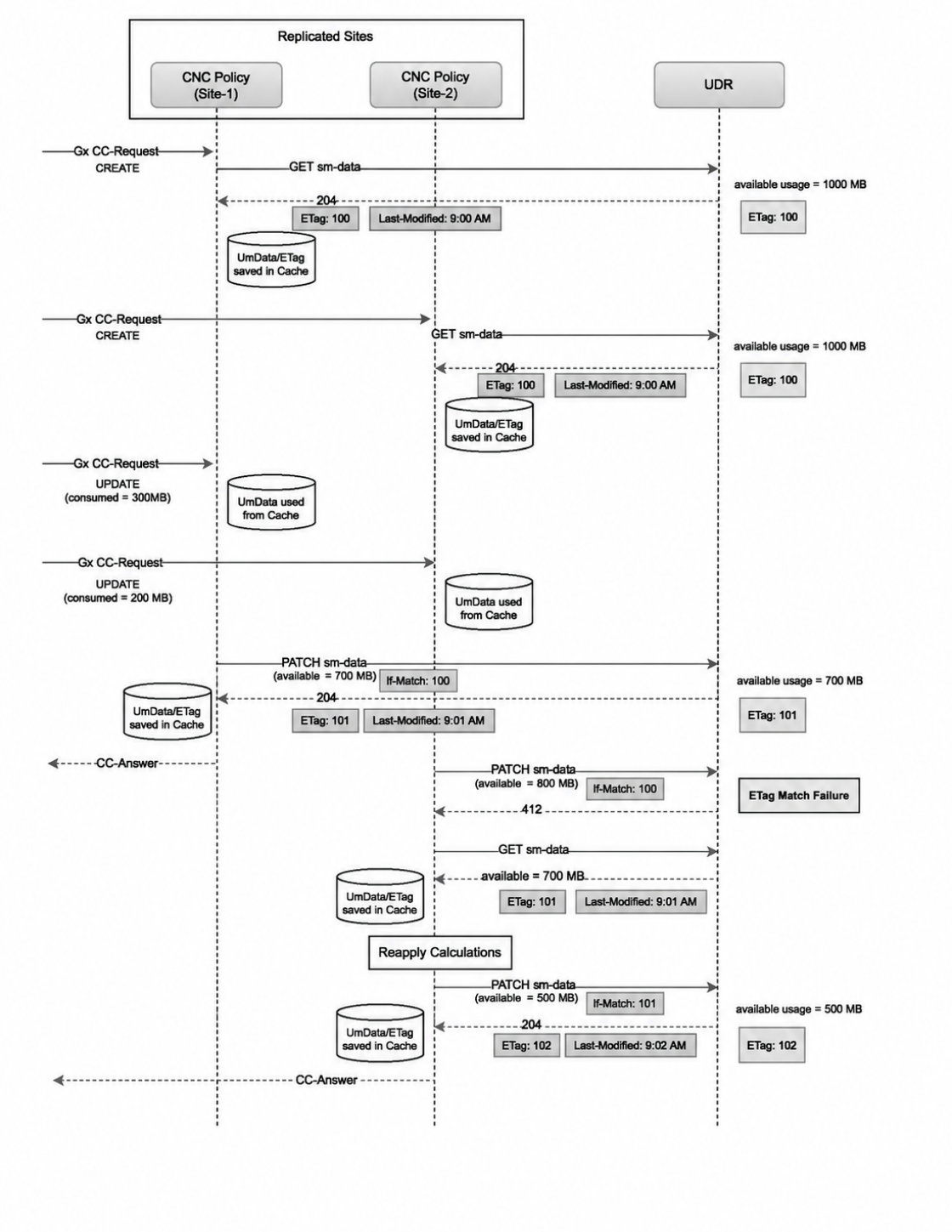
"ETag" in GET Response >> Request: GET /index HTTP/1.1 Host: www.example.com >> Response: HTTP/1.1 200 OK Date: Fri, 26 Mar 2010 00:05:00 GMT ETag: "123-a" Content-Length: 12 Content-Type: text/plain Hello World!	"Last-Modified" in GET Response >> Request: GET /index HTTP/1.1 Host: www.example.com >> Response: HTTP/1.1 200 OK Date: Fri, 26 Mar 2010 00:05:00 GMT Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT Content-Length: 70 Content-Type: text/plain Hello World!
"If-Match" Success >> Request: PATCH /resource/index HTTP/1.1 Host: www.example.com If-Match: "123-a" Content-Length: 12 Content-Type: text/plain Hello Again! >> Response: HTTP/1.1 204 No Content	"If-Match" Failure >> Request: PATCH /resource/index HTTP/1.1 Host: www.example.com If-Match: "123-aa" Content-Length: 12 Content-Type: text/plain Hello Again! >> Response: HTTP/1.1 412 Precondition Failed Date: Fri, 26 Mar 2010 00:05:00 GMT

Copyright © 2019, 2026, Oracle and/or its affiliates.

Date: Fri, 26 Mar 2010 00:05:00 GMT ETag: "123-a" Content-Length: 0	Content-Length: 0
"If-Unmodified-Since" Success >> Request: PATCH /resource/index HTTP/1.1 Host: www.example.com If-Unmodified-Since: Tue, 15 Nov 1994 12:45:26 GMT Content-Length: 12 Content-Type: text/plain Hello Again! >> Response: HTTP/1.1 204 No Content Date: Fri, 26 Mar 2010 00:05:00 GMT ETag: "123-a" Content-Length: 0	"If-Unmodified-Since" Failure >> Request: PATCH /resource/index HTTP/1.1 Host: www.example.com If-Unmodified-Since: Mon, 14 Nov 1994 12:45:26 GMT Content-Length: 12 Content-Type: text/plain Hello Again! >> Response: HTTP/1.1 204 No Content Date: Fri, 26 Mar 2010 00:05:00 GMT Content-Length: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-280 NF Level Flow



For more information on how to configure this feature using CNC Console, see the Configuring Usage Monitoring.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.134 Support for Resource Allocation for PCC Rules

When Successful Resource Allocation (SRA) is enabled, Policy provides the status of the Policy and Charging Control Rules (PCC Rules) that are successfully installed and validated by Session Management Function (SMF).

Policy writer can make the appropriate action based on the successful activation of a rule.

For example, a Policy writer can hold updating the installed PCC rule unless SRA is applied at SMF.

> **Note**
>
> This feature is applicable to the PCC Rules that are installed by Policy and not through Application Function (AF).

To apply the SRA functionality, PCC Rule must include `policyCtrlReqTriggers` and `lastReqRuleData`.

For example:

```
"policyCtrlReqTriggers":[
   "PLMN_CH",
   "UE_IP_CH",
   "DEF_QOS_CH",
   "AC_TY_CH",
   "SUCC_RES_ALLO"
],
"lastReqRuleData":[
   {
      "refPccRuleIds":[
         "0_2",
         "0_3"
      ],
      "reqData":[
         "SUCC_RES_ALLO"
      ]
   }
]
```

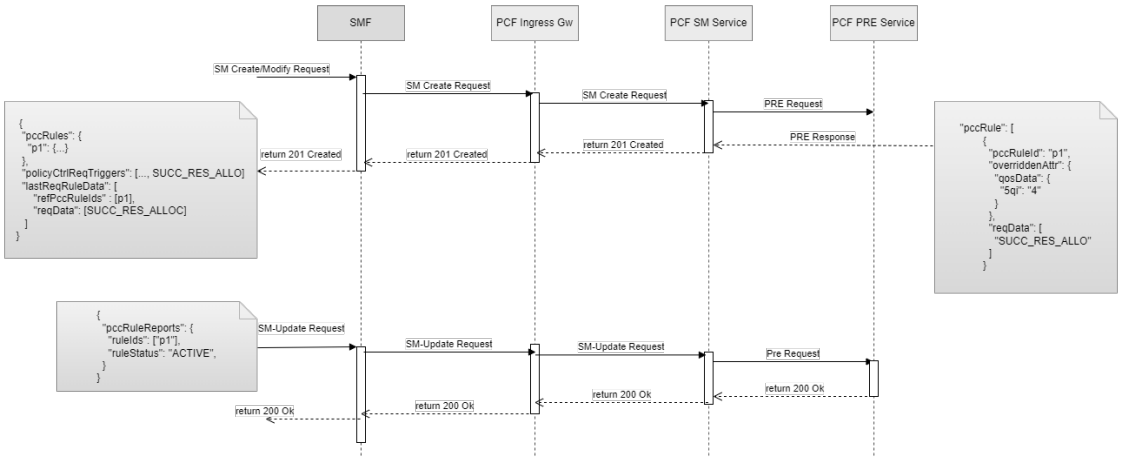
In the above example, `SUCC_RES_ALLO` under `policyCtrlReqTriggers` triggers the application of SRA. `lastReqRuleData` includes the last requested rule data and `SUCC_RES_ALLO` under `reqData` is the requested data.

> **Note**
>
> Policy does not have to send any `policyCtrlReqTriggers` to receive failed-to-install PCC rules from SMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow for SRA

Figure 4-281 PCC Rule for SM Create and SM Update requests



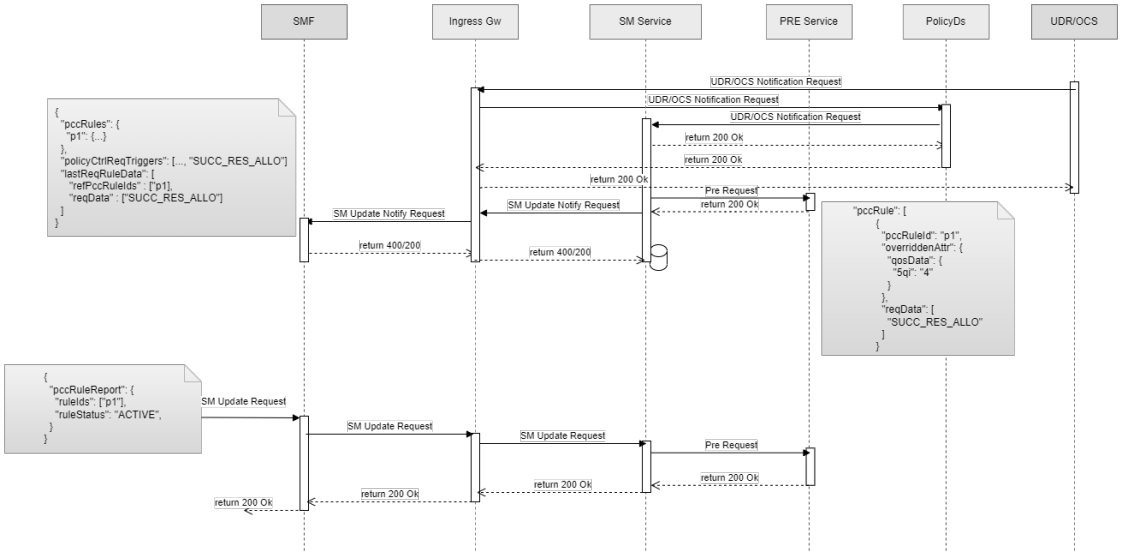
1. SMF receives an SM Create request with the PCC Rule installation information to create a new PCC Rule p1 with requested data as `SUCC_RES_ALLO` indicating SRA.
2. SMF sends the SM Create request to SM Service via Ingress Gateway.
3. SM Service forwards the SM Create request to PRE for evaluation.
4. PRE evaluates the details and responds to SM Service.
5. SM Service creates the session details in the session database, sends a 201 created message to SMF via the Ingress Gateway.

> **Note**
>
> The SM Create contains different media components. If any media component that contains a flow status set as 'removed', the notification towards SMF will not be sent.

6. SMF installs and validates PCC Rule p1. It includes `SUCC_RES_ALLO` under PolicyctrlReqTrigger indicating the application of SRA, along with the details of the last requested rule data and requested data containing `SUCC_RES_ALLO`.
7. After the session creation, SMF receives an SM Update request that includes PCC rule report for p1 with `ruleStatus` as `ACTIVE`.
8. SMF sends the SM Update request to SM Service via Ingress Gateway.
9. SM Service forwards the SM Create request to PRE for evaluation.
10. SM Service forwards the 200 ok response that it receives from PRE to SMF via the Ingress Gateway.
11. SMF validates the details and responds with a 200 ok message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-282 PCC Rule in SM-UPDATE-NOTIFY request (Re-authorization)



1. Policy receives an SM Update-Notify from one of the data sources such as UDR via the ingress gateway.
2. Policy sends the update notification request to SM Service.
3. SM Service acknowledges the update by returning a 200 ok message to Policy.
4. Policy in-turn responds to the data source with a 200 ok message via the ingress gateway.
5. SM Service shares the SM Update Notify details to PRE for evaluation. The update-notify information includes an update to the PCC Rule p1 with `overriddenAttr` containing the updates to the PCC Rule.
6. PRE evaluates the update and returns a 200 ok message to SM Service.
7. SM Service sends the SM Update Notify request to SMF via the Ingress Gateway.
8. SMF modifies and validates the PCC Rule p1 as per the given details and returns a 400/200 message to SM Service via the Ingress Gateway.
9. SM Service updates the session database accordingly.
10. After the successful processing of the SM Update-Notify request, SMF receives a SM Update request containing PCC rule report for P1 with `ruleStatus` as `ACTIVE`.
11. SMF forwards the SM Update request to SM Service via the Ingress Gateway.
12. SM Service shares the SM Update with PRE for evaluation and receives a 200 ok response.
13. SM Service sends the 200 ok response to SMF via the Ingress Gateway.

Managing Support for Successful Resource Allocation for PCC Rules

Enable

By default, the SRA support for PCC Rules is disabled. You can enable this functionality using the CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To enable this feature, under **Rule** section in **PCF Session Management** page in CNC Console, set the value of `Default PCC Rule Requested Rule Data` parameter to `SUCC_RES_ALLO`.

For more details on enabling the SRA support for PCC Rules, see Settings.

Configure

You can use blockly action to configure Install/Update/Remove PCC Rules with Override Attributes. For more information, see *PCF-SM Category* in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Observe

Added `rule_action` metric to support Successful Resource Allocation.

For more information on metrics, see SM Service Metrics.

4.135 Subscriber State Variables in Policy

State variables hold the intermediate state of the policy evaluation. The state variables are defined by the policy writer that can be set within a policy action to be used at a later time during policy rule execution (in either conditions or actions). The names of these variables are not predefined and are determined by the policy writer.

State variables have `scope` which determines how long the value is persisted after it is set.

Depending on the scope, the following state variables are defined in Policy:

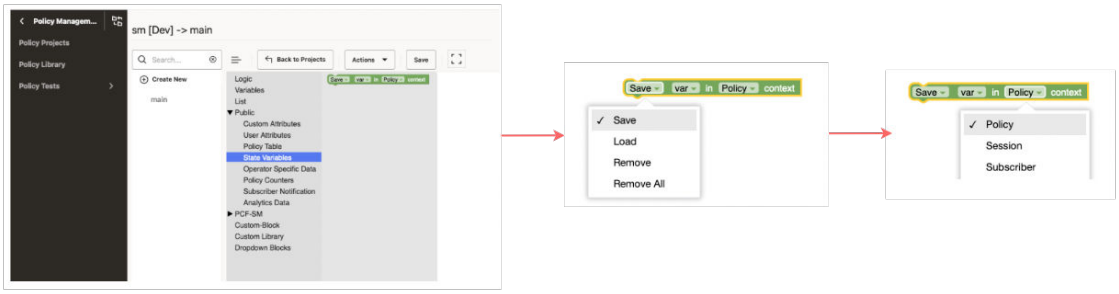
- **Policy Evaluation State Variables**: Used during Policy evaluation. These variables exist only for the lifetime of a policy evaluation cycle (the process of evaluating all the policies for a single request/context).
- **Session State Variables**: Contains a value that is saved as long as the session they are associated with is valid. These variables are stored in the session database in the respective core services (SM Service, AM Service, UE Policy Service, and PCRF Core). On the subsequent operation of the session, the values are extracted and reused. Once the session is terminated, these variables will no longer have a value and will no longer be available for use in policies.
- **Subscriber Local Policy Evaluation State Variables**: Created for a subscriber and remains until at least one session for the subscriber exists. When there are multiple sessions associated with a subscriber across services (SM Service, AM Service, UE Policy Service, or PCRF Core), these subscriber state variables are used across sessions based on the subscriber ID. The subscriber state variables are stored in subscriber database on PDS where other subscriber details are available. These variables hold a value as long as the associated subscriber has at least one active session. Once the last session for the subscriber is terminated, these variables will no longer have a value and will no longer be viable for use in policies.
- **Subscriber Remote State Variables:** Persist remotely in a Subscriber Profile Repository (SPR) as long as the subscriber exists in the SPR. Using these variables requires that an SPR/HSS be configured that is capable of storing these variables.

4.135.1 Local Subscriber State Variable

The Policy blockly for each of the services (SM Service, AM Service, UE Policy Service, and PCRF Core) includes **State Variable** section under **Public** Category.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-283 State Variables in Policy



- Save: saves a variable
- Load: load a variable
- Remove: Remove a variable
- Remove All: Applicable only for JSON type of variable. This function removes all the variables from the specified context.

You can select the required action for each context.

For example, you can select the context as **Policy** and select **Save** to save the specified state variable var and the value assigned to it.

> **Note**
>
> - The context list includes the Remote option to create Subscriber Remote State Variables only for SM Service and UE Policy Service. This option is not available for AM Service.
> - Remove SSV is not revalidated when Query on Update or Query on Delete is enabled in the core service (SM Service or UE Policy Service).

For more information on configuring state variables using blockly, see *State Variables* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Configurations

The service configurations for both SM and AM in CNC console supports, the boolean parameter `Enable Subscriber State Variables` to enable the SSV query. And also the following deployment variable are added to AM and UE services to support SSV reset context.

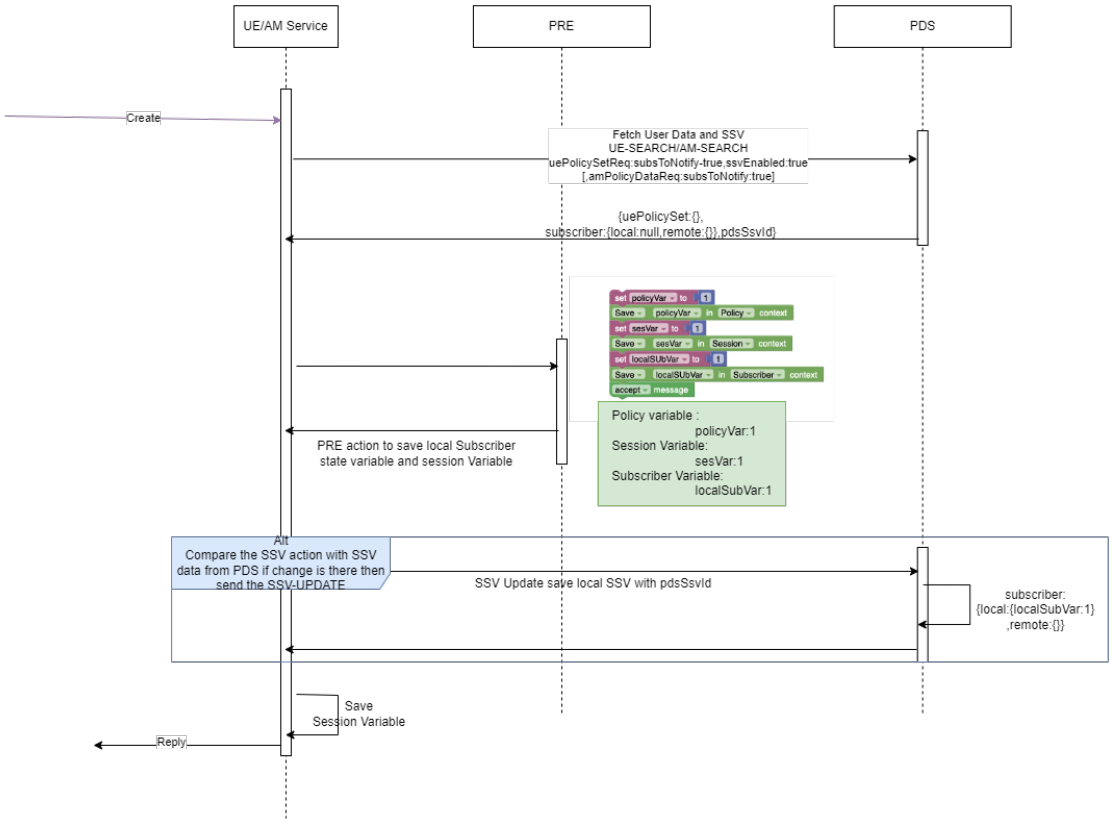
Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-194 SSV Reset Context Deployment Variable

Variable Name	Values	Description
USER.RESET_CONTEXT_SSV_ON_AM_CREATE	true/false	If this flag is true, then PDS SSV context information will be updated for AM context owner. If any AM context information associated to SSV has exceeded the guard time then those context will be deleted. **Default Value**: false
USER.RESET_CONTEXT_SSV_ON_UE_CREATE	true/false	If this flag is true, then PDS SSV context information will be updated for UE context owner. If any UE context information associated to SSV has exceeded the guard time then those context will be deleted. **Default Value**: false

Call Flow

Figure 4-284 State variables in create session call flow



1. Core service (AM Service /UE Policy Service) receives a session create request.

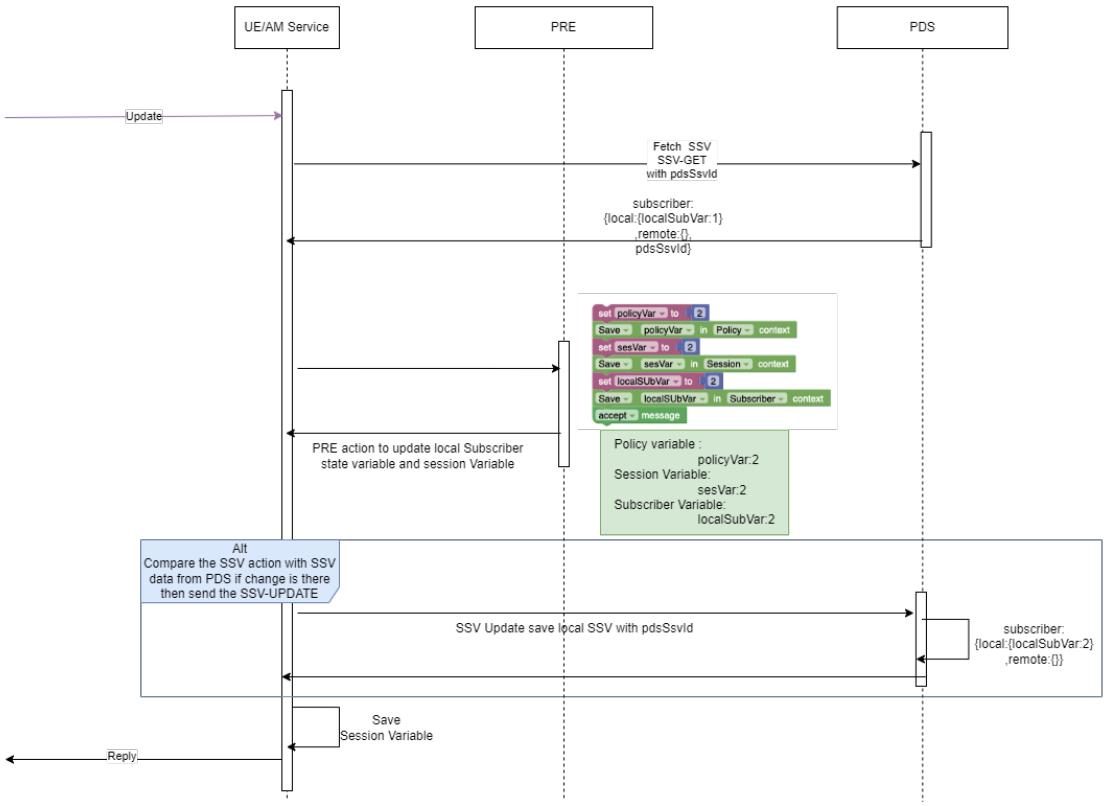
Copyright © 2019, 2026, Oracle and/or its affiliates.

2. If `ssvEnabled` is set to `true`, the core service sends a request to PDS to fetch the Subscriber State Variable (SSV) and the user data.
3. PDS creates a new entry for the SSV in its database. It searches for the user data in PolicyDS database. If it is not present in PolicyDS, it sends a request to the data source such as UDR or CHF through UDR Connector or CHF Connector to get the required details. PDS then responds to the core service with the required information.
4. Core service sends a request to PRE to evaluate the data. PRE creates the Policy state variables as required. PRE does not share these variables with the core service.
5. PRE responds to the core service along with the details of the action to be taken.
6. The core service identifies the session state variables and saves them in the respective session database. Then, it sends the subscriber state variables to PDS to save in the subscriber database.

> **Note**
>
> The core service sends the subscriber state variables to PDS only when there is an update to the variables.

7. After the core service receives a response from PDS and also the core service saves the Session State variables in session database, it replies to SMF/AMF.

Figure 4-285 State variables in update session call flow



1. Core service (AM Service /UE Policy Service) receives a session update request.

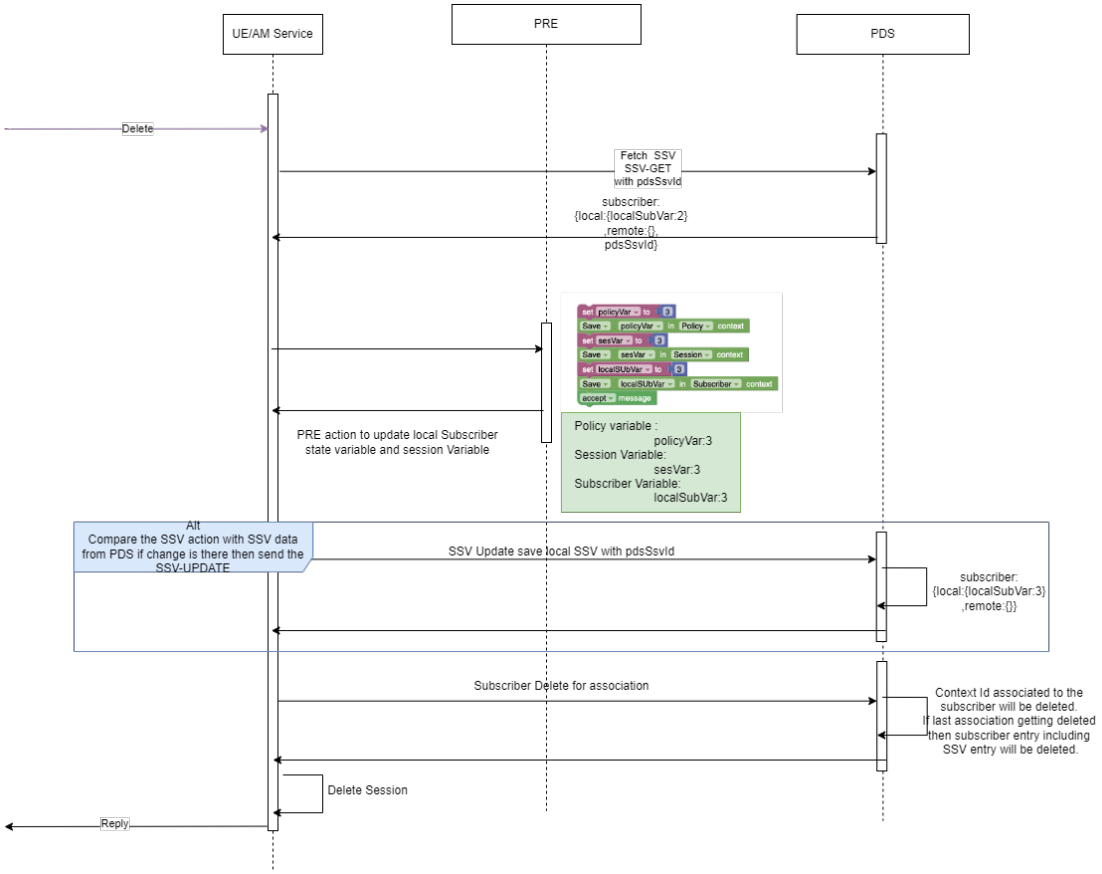
Copyright © 2019, 2026, Oracle and/or its affiliates.

2. If `ssvEnabled` is set to `true`, the core service sends a request to PDS to fetch the Subscriber state Variable (SSV).
3. PDS responds to the core service with the required information.
4. Core service sends a request to PRE to evaluate the data.
5. PRE responds to the core service along with the details of the action to be taken.
6. The core service identifies the session state variables and saves them in the respective session database. Then, it sends the subscriber state variables to PDS to save in the subscriber database.

   Note: The core service sends the subscriber state variables to PDS only when there is an update to the variables.
7. After the core service receives a response from PDS, and also saves the State Session Variables in its session database, it replies to SMF/AMF.

> **Note**
>
> In case of error, session retry is not yet supported.

Figure 4-286 State variables in delete session call flow



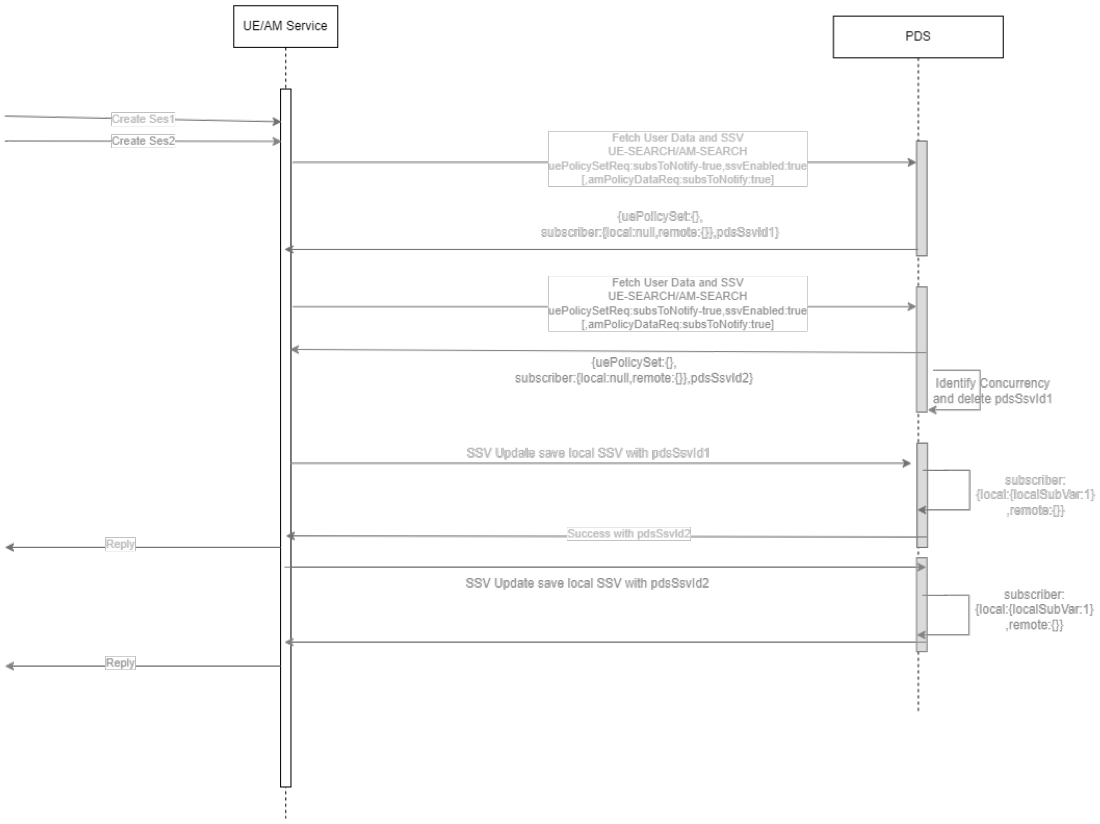
1. Core service (AM Service /UE Policy Service) receives a session delete request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. If `ssvEnabled` is set to `true`, the core service sends a request to PDS to fetch the Subscriber state Variable (SSV).
3. PDS responds to the core service with the required information.
4. Core service sends a request to PRE to evaluate the data.
5. PRE responds to the core service along with the details of the action to be taken.
6. The core service identifies the session state variables and saves them in the respective session database. Then, it sends the subscriber state variables to PDS to save in the subscriber database.

   Note: The core service sends the subscriber state variables to PDS only when there is an update to the variables.
7. After the core service receives a response from PDS, and also saves the State Session Variables in its session database
8. Core service sends the subscriber delete request to PDS to delete the subscriber delete for the association.
9. After the core service receives a response from PDS, it deletes the session details from its session database and responds to AMF/SMF.

Figure 4-287 State variables in concurrent flows



1. Core service (AM Service /UE Policy Service) receives multiple create session requests simultaneously.
2. If `ssvEnabled` is set to `true`, the core service sends two separate requests to PDS to fetch the Subscriber state Variable (SSV) for both the requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. PDS creates the entries for SSVs and profiles for both the requests and responds to the core service with the required information.
4. When PDS identifies the concurrency either during UDR subscription call flow or during the subsequent create request, PDS deletes the Subscriber State Variable for the first request and merges the rows in PDS database. When PDS receives the update session for the same SSVID as the first create request, the update request includes the SSVID of the first request along with the PDS SSVID.
5. PDS returns the update to the core service indicating that it is a new SSV ID and the previous one is deleted.
6. The core service updates the same SSVID in its database.

Managing Subscriber Variables in Policy

Enable

You can enable the Subscriber Variables for SM Service, AM Service, UE Policy Service, and PCRF Core using CNC Console.

- To enable the Subscriber Variables for SM Service, configure **Disable Subscriber Variables** parameter under **User** section in **PCF Session Management** page. For more details, see PCF Session Management.
- To enable the Subscriber Variables for AM Service, configure **Enable Subscriber State Variables** parameter under **User** section in **PCF Access and Mobility** page. For more details, see PCF Access and Mobility.
- To enable the Subscriber Variables for UE Policy Service, configure **Enable Subscriber State Variables** parameter under **User** section in **PCF UE Policy** page. For more details, see PCF UE Policy Service.
- To enable the Subscriber Variables for PCRF Core Service, configure **Enable Subscriber Variables** parameter under **User** section in **Settings** page in **PCRF Core**. For more details, see PCRF Core Service Configurations.

Configure

You can configure the updates to PDS SSV entry's context information for AM context owner and UE context owner using the following flags in `values.yaml` file.

- `resetContextSsvOnAMCreate`
- `resetContextSSVOnUECreate`
- `enableSsvIdForReqParam`

For more information, see *Enabling/Disabling Services Configurations* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

Configure using CNC Console

You can configure the state variables for Policy using CNC Console.

- For details on configuring state variables for SM Service, see PCF Session Management.
- For details on configuring state variables for AM Service, see PCF Access and Mobility.
- For details on configuring state variables for UE Policy Service, see PCF UE Policy Service.
- For details on configuring state variables for PCRF Core Service, see PCRF Core Service Configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Observe

The following PolicyDS metrics provide information about state variables:

- client_request_total
- client_response_total

For more information, see Policy DS Metrics.

4.135.2 Remote Subscriber State Variable

Policy provides UE Policies, via the AMF transparently to the UE. The UE Policy is divided into Policy sections. Such Policy sections are predefined in PCF. PCF either retrieves from UDR, or dynamically generates them. The PCF interfaces with User Data Repository (UDR) to receive subscriber-related Policies for User Equipment (UE). UDR stores the subscriber attributes. PCF communicates with UDR to receive these attributes which are used in the evaluation of Policies.

PCF support for dynamic data for UE Policies:

Subscriber State Variable (SSV) comprises of local and remote section. The remote SSV section is formed by extracting the data from UDR response as per the UEPolicySet datasource path, configured at PDS Settings in the CNC Console. SSV section is sent back to UE service as part of create request processing. UE service forwards the SSV to Policy Runtime Engine(PRE) for:

- Evaluation of Policies, and
- Update the changes in the state variable and send it to UDR.

Revalidation of dynamic data for UE Policies:

UE service supports 'ResetContext' and 'Revalidation' feature. On enabling this feature, an updated SSV remote Policy section is formed with revalidated UE data. This section is updated in the database and sent to UE service.

Write Remote Subscriber State Variable in UDR as a PATCH request:

UE service sends SSV to PRE service for evaluation of Policies. The policy evaluation results in addition or modification or deletion in the SSV. The PRE sends back the updated SSV to UE service. UE service sends the updated SSV to Policy Data Service (PDS). PDS service sends the remote SSV section toward UDR as PATCH request through UDR Connector. The PATCH request that PDS sends to UDR Connector will also include the data source information. UDR Connector uses this data source information to forward the PATCH to appropriate UDR. If the data source information is not included in the PATCH, it will be determined by the UDR-Connector.

> **Note**
>
> - PCF supports dynamic data for UE policies in independent deployment only. It does not work if SM and UE services are running in the same PCF instance with SSV enabled.
> - Verify the latest Remote Subscriber State Variable data from User Data session viewer and ignore the same from SM Policy Association session viewer result.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.135.3 Support to Write Remote Subscriber State Variables to Operator Specific Data (OSD)

This feature enables Converged Policy to write values received from Online Charging System (OCS) provided counters into Operator Specific Data (OSD) in the UDR using Remote Subscriber State Variables. The values are written directly to operator specified paths within operator specific data. Remote subscriber state variables allow operators to synchronize session or charging state between policy engines and UDR, supporting use cases like OCS spending limits and dynamic policy enforcement.

This feature has the following functionality:

- The feature supports the OSD PATCH operation as defined in 3GPP specification.
- This feature applies only to the SM-OCS-Sy-Nudr call flow when SSV is enabled.
- Based on the existing behavior, only one data source PATCH operation per deployment is supported.
- Only the REPLACE operation is supported among the operations defined in the 3GPP specification.
- Values received from OCS are written without transformation. Additional validation or modification is not performed before applying the REPLACE operation based on the configured policy.
- The policy design supports only the REPLACE and LOAD operations for OSD data.
- The feature supports synchronous and asynchronous OCS handling for success and failure scenarios during initial and intermediate requests. Depending on the `createContextOnFailure` setting in PCF-SM and the `ENABLE_OCS_ERROR_HANDLING` setting in PDS Advance Settings configuration, the response or notification can include one of the following results:
  - Valid `ocsSpendingLimitStatus` data for success scenarios.
  - No `ocsSpendingLimitStatus` data. For example, `null value`, `ocsSpendingLimitStatus` with `lastErrorCode` (on failure scenarios), or no notification or context creation, based on the `ENABLE_OCS_ERROR_HANDLING` and `createContextOnFailure` settings.
- For REQUEST-PC based OCS requests, set the `ENABLE_OCS_ERROR_HANDLING` parameter to true in the PDS advanced settings to send notifications to SM. Notifications are generated only when a valid subscription or context exists. To configure a policy for SSV updates when an SLR Initial request fails, use the `createContextOnFailure` feature in PCF-SM settings. For details about the createContextOnFailure flag, see Sy SLR Enhancements for Signaling Updates and UDR Notification.
- PATCH retry is handled only at UDR-C through an alternate route.
- The `Enable End Session SSV Remote to UDR` field is not applicable for Operator Specific Data.
- Concurrency handling for multiple site writes to the same UE is not supported.

For more information on policy configurations, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> - If Converged Policy cannot connect to all configured UDRs, or if PATCH retry attempts fail, the PATCH update may not be applied to the affected UDR. In such cases, Converged Policy and UDR data may become out of sync. Subsequent PATCH updates are not triggered if there is no change in the UDR remote SSV values within the Converged Policy session context. Resynchronization occurs after the existing Protocol Data Unit (PDU) session terminates and a new session is established.

Managing Support to Write Remote Subscriber State Variables to OSD

Configure

This feature can be configured using CNC Console and REST API.

Configure using CNC Console

This feature can be configured using **Operator Specific Data** field under **Settings** section in CNC Console. For more information, see PDS Settings.

Configure using REST API

This feature can be configured using `operatorSpecificData` parameter under `remoteSSVRootPath` in PDS Settings API: `{apiRoot}/oc-cnpolicy-configuration/v1/services/pds/pdsSettings`.

For more information, see *PDS Settings* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

Observability

- **Metrics**

  The following metrics are updated to support this feature:

  - `server_request_total`
  - `server_response_total`
    Updated the dimension value with `method = "JSON_PATCH"`. This method value applies only to OSD updates. Other data sources continue to use `method="PATCH"`. For more information, see Policy DS Metrics.
  - `ocpm_udr_tracking_request_total`
  - `ocpm_udr_tracking_response_total`
    The following dimensions are used to track this feature:
    * `operation_type="patch", service_subresource="operator-specific-data"`

    For more information, see UDR Metrics.
- There are no new KPIs or alerts available for this feature.

4.136 AMF Selection for Namf-comm Subscription

Policy supports discovering AMF as a producer based on AMF SetID and AMF Region ID, which are extracted from Globally Unique AMF Identifier (GUAMI). This aids in transferring the UE Policy to UE through AMF and sending initial subscription request to AMF during UE Policy Transfer request. For more details, see UE Policy Enhancements.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.137 Support for MCPTT Features

Oracle Communications Cloud Native Core, Policy (Policy) supports Mission Critical Push-to-Talk (MCPTT) and other mission-critical data and video over cellular networks. There are many MCPTT applications that are available through cellular Long Term Evolution (LTE), with mobile broadband meeting many emergency responders' needs for reliable coverage, secure communication and real-time video sharing.

This feature enables PCRF support for MCPTT related QoS Class Identifier (QCI)s, and MCPTT specific features such as Priority sharing and Preemption.

PCRF enables MCPTT for a session based on the supported features exchanged between the Policy and Charging Enforcement Function (PCEF)/Application Function (AF) and PCRF (dynamic discovery of supported features).

Policy supports the following MCPTT features:

- **Allocation Retentions Priority (ARP) Selection**: ARPs determine the priority level, the pre-emption capability and the pre-emption vulnerability of each QoS flow according to the operators' policy. PCRF uses ARPs to determine the relative importance of a resource request and decides whether a new QoS Flow can be accepted or rejected in the case of resource limitations.
- **QoS Class Identifier (QCI) selection**: QCIs are used to ensure carrier traffic is allocated appropriate Quality of Service (QoS). Different carrier traffic requires different QoS and therefore different QCI values.

  The following are the MCPTT related QCIs:

  - QCI-65 - MCPTT Audio service flow.
  - QCI-66 - Non-MCPTT Audio service flow.
  - QCI-67 (for MC Video)
  - QCI-69 - MCPTT signaling flow.
  - QCI-70 - MCPTT Data service flow.
  - QCI-7 - Voice, video (live streaming)
  - QCI_128-254 - Operator specific
- **Priority Sharing**: For all the Policy and Charging Control Rules (PCC rules) with the same QCI assigned and having an associated priority sharing indicator, PCRF assigns the same Allocation and Retention Priority (ARP) settings. Having the same setting for the ARP enables the usage of the same bearer.

  PCRF decides the ARP for the PCC rules (same QCI and Priority Sharing indicated by AF) as follows:

  - ARP Priority is set as highest of the priority among all the PCC rules
  - ARP pre-emption capability is set if any of the original PCC rules have the ARP pre-emption capability set
  - ARP pre-emption vulnerability is set if all the original PCC rules have the ARP pre-emption vulnerability set
- **Preemption control**: If PCEF informs the PCRF that a PCC rule provisioning or modification failed (due to resource reservation failure), PCRF can apply pre-emption and remove the active PCC rules from PCEF and retry the PCC rule provisioning or modification procedure.

Copyright © 2019, 2026, Oracle and/or its affiliates.

If PCRF does not apply pre-emption, AF is notified that the resource reservation for the new media flow failed.

Feature enablement is controlled by the supported feature negotiation done between the PCRF and the PCEF/AF. By default, all MCPTT related feature bits are enabled and applied to session (when supported by PCEF and AF).

Table 4-195 MCPTT related features in Gx

Feature Name	Feature bit	M/O	Feature list Id	Vendor Id
MissionCriticalQCIs	25	O	1	10415
MCVideoQCI	9	O	2	10415
MCVideo	22	O	1	10415

Table 4-196 MCPTT related features in Rx

Feature Name	Feature bit	M/O	Feature list Id	Vendor Id
MCPTT	17	O	1	10415
PrioritySharing	18	O	1	10415
MCPTT-Preemption	21	O	1	10415

You must mention the supported features separated by comma as values in these keys.

This is not limited to MCPTT feature bits. You can disable any of the existing optional features using this option.

Mandatory features such as Rel8, Rel9 and Rel10 are enabled by default for negotiation.

Selecting QCIs

You can select the required QCIs using the existing Policy actions.

You must assign these QCIs to the PCC rules using Policy and PCC rule configurations. When there is no decision received from Policy suggesting QCI for MCPTT session, QCIs are chosen based on the media type.

For example:

Table 4-197 QCI based on Media Type

Media Type	QCI
Audio	QCI_65
Data	QCI_70
*Anything else	QCI_69

Selecting ARPs

You can configure the ARP parameters such as priority, Preemption capability and preemption vulnerability for default EPS bearer and PCC rules generated for the AF flows.

When there is no ARP set from Policy, the ARP settings for MCPTT session is created under PCRF core service configuration.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> ARP assigned based on Policy is considered as final. This can be overridden by priority sharing feature (when enabled). But the original ARP decision is stored for future use.

Priority Sharing

When priority sharing feature is enabled, the ARP assigned by policy or configuration can be overridden (when conditions are met). The original ARP assigned for the PCC Rule is stored along with the overridden ARP as part of the session data stored in the database. The original ARP information is required when there is a need to apply the priority sharing again on these PCC rules in the future.

Table 4-198 Sample priority sharing scenario

PCC Rule 1 original ARP			PCC Rule 2 original ARP	Shared ARP				
Priority	**Preemption Capability**	**Preemption Vulnerability**	**Priority**	**Preemption Capability**	**Preemption Vulnerability**	**Priority**	**Preemption Capability**	**Preemption Vulnerability**
1	Disabled	Disabled	2	Enabled	Enabled	1 PCC Rule 1 - unchanged PCC Rule 2 - changed	Enabled PCC Rule 1 - changed PCC Rule 2 - unchanged	Disabled PCC Rule 1 - unchanged PCC Rule 2 - changed

In this case, both the PCC rules belong to the same IPCAN session, same QCI and having priority sharing indicator.

Following are the scenarios when Priority sharing rederive ARP is triggered:

- At least one of the PCC Rules (sharing same ARP) is removed
- A new PCC Rule (with same QCI, Priority sharing indicator) is created
- The original derived ARP of at least one of the PCC rule changes

Whenever the ARP of an already installed PCC rule changes, that rule will also be added as part of the Charging-Rule-Install AVP. For the rules to be modified, the charging-Rule-Definition will have the new ARP values.

Since priority sharing is applied at different scenarios, the original ARP and the priority sharing indication (received from AF) becomes necessary, These are mentioned as values of *PCRFDiameterEnfAppFlow* parameter stored in the Gx Session (in the database).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Preemption

Whenever a PCC rule (with priority sharing enabled) installation or modification fails due to resource reservation issue, any other preemptable PCC Rule(s) is removed and the failed PCC Rule will be retried.

Preemption is triggered only when the following conditions are met

- When PCC rules (with priority sharing) provisioning or modification fails (Charging-Rule-Report with rule failure code `RESOURCE_ALLOCATION_FAILURE`)
- Failed PCC Rule(s) preemption capability (original - before Priority sharing) is `ENABLED`
- At least one PCC rule with priority equal or lower (than the failed PCC rule) and having preemption vulnerability `ENABLED`
- MCPTT-Preemption is enabled (supported features)

Preemption is not triggered if any of the above mentioned conditions are not met. Instead, a Re-Authorization Request (RAR) is triggered towards AF (if requested by AF) with the Specific-Action AVP set to `INDICATION_OF_FAILED_RESOURCES_ALLOCATION` to report the resource allocation failure.

When there are more than one potential PCC rule candidate for preemption, the PCC rule to be preempted is selected based on the Pre-emption-Control-Info AVP received from Authorization Authentication Request (AAR) or the local configuration (in PCRF-core service configuration).

The control information has the following three options.

- Most recent added flow - Newest flow among the potential preemptable rules to be preempted
- Least recent added flow - Oldest flow among the potential preemptable rules to be preempted
- Highest bandwidth flow - Having highest bandwidth among the potential preemptable rules

The rule to be preempted is selected based on the information received from AF or local configuration.

The rule creation time stored in the PCC rule information (part of session object) is used to compare the oldest and the newest rule,

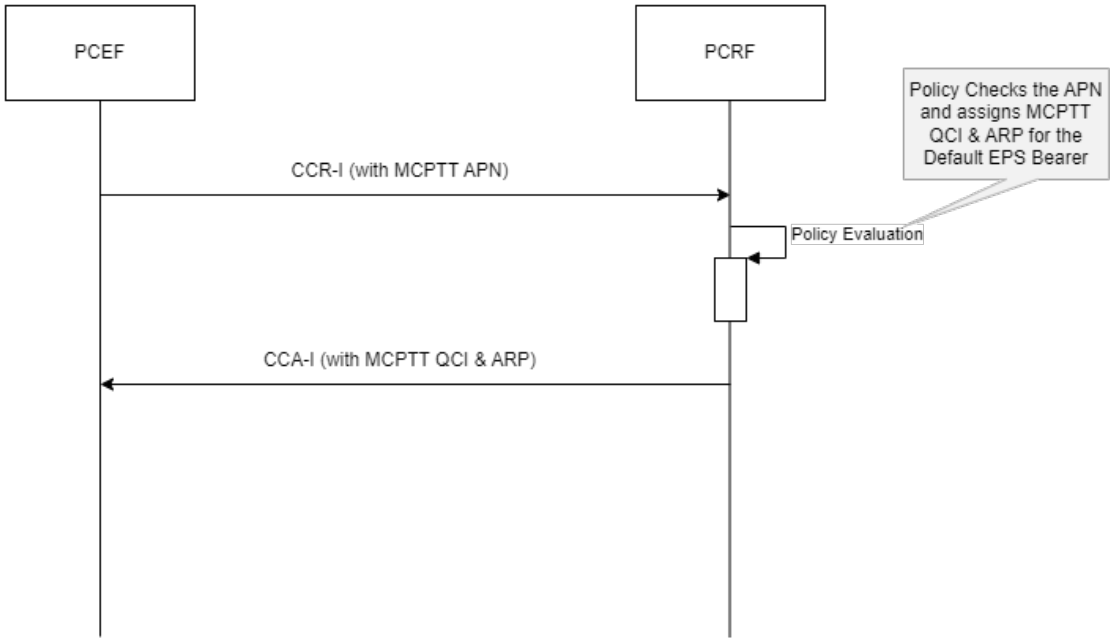
After the Preemption, Priority sharing is triggered again to rederive the ARP for the affected PCC Rules (sharing the same QCI of the preempted PCC Rule).

> **Note**
>
> Currently, Policy does not support preemption using Policy. Preemption is performed as per the procedure defined by 3GPP only.
>
> For the preempted PCC rules a Rx-RAR will be sent to AF to notify about pre-emption of the flow (with specific action set to `INDICATION_OF_RELEASE_OF_BEARER`)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Call Flow

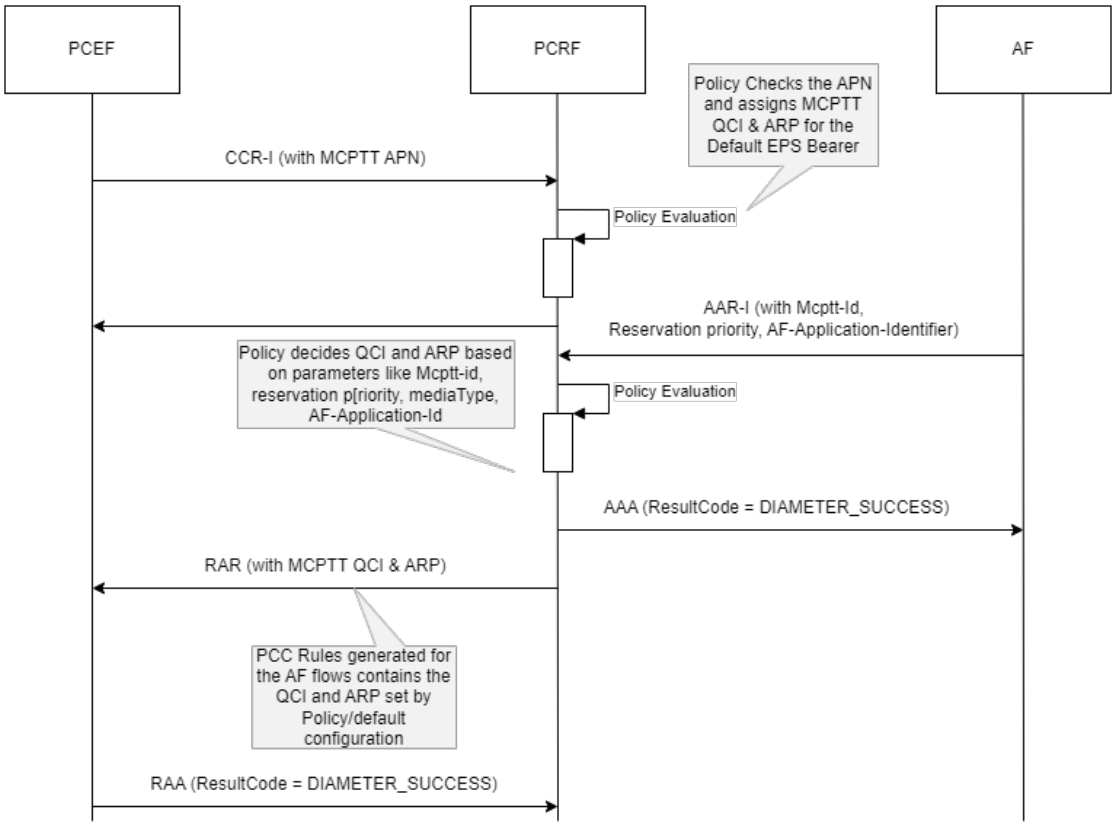
Figure 4-288 MCPTT APN Handling



1. The PCEF sends a Credit Control Request-Initial (CCR-I) message to the PCRF with MCPTT APN details.
2. PCRF checks the Access Point Name (APN) and assigns the MCPTT QCI and ARP for the default Evolved Packet System (EPS) Bearer.
3. PCRF sends a Credit Control Answer-initial (CCA-I) message to PCEF and provisions the MCPTT QCI and the ARP settings.

Copyright © 2019, 2026, Oracle and/or its affiliates.

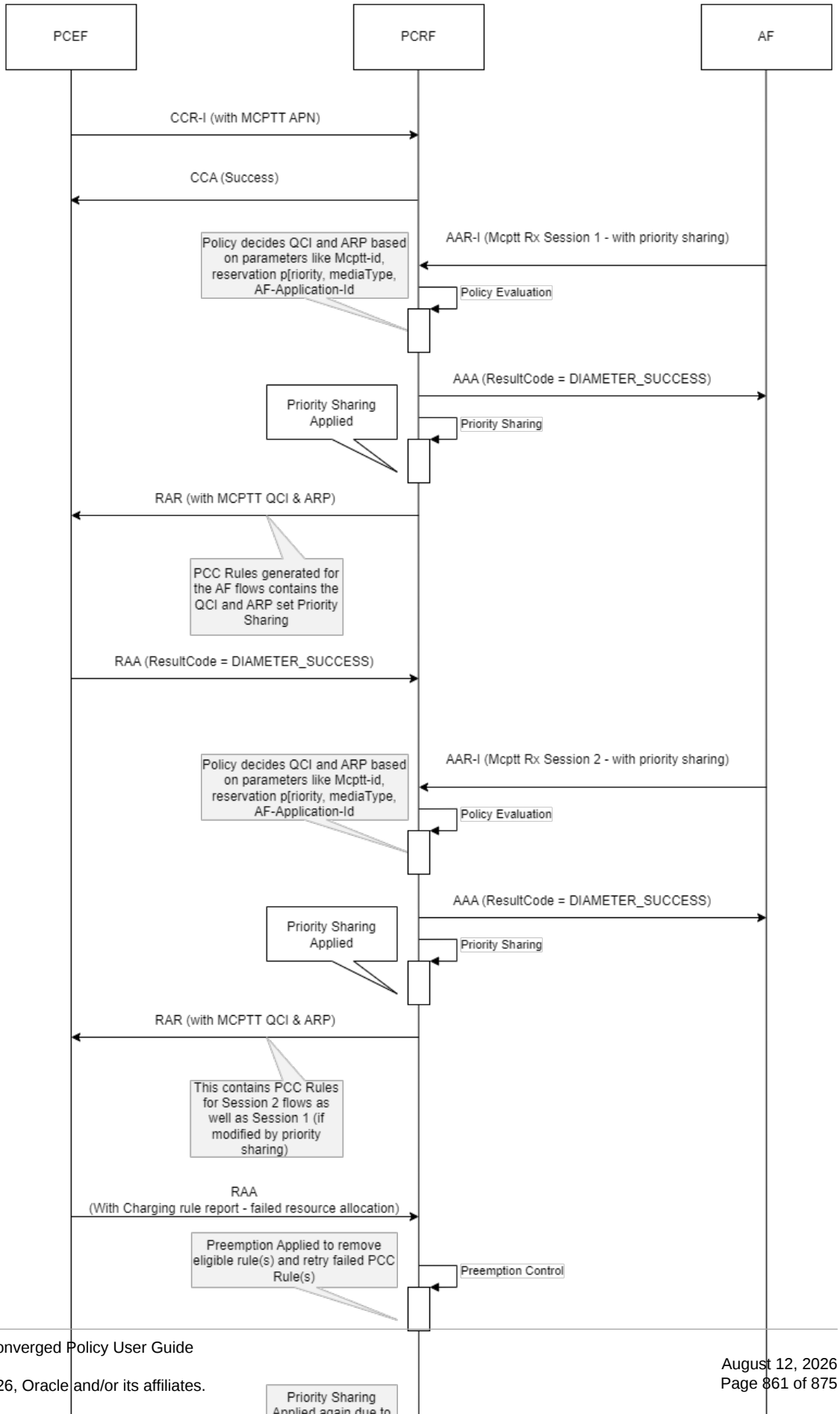
Figure 4-289 MCPTT QCI & ARP settings for MCPTT AF flows



1. The PCEF sends a Credit Control \Request initial (CCR-I) message to the PCRF with MCPTT APN details.
2. PCRF checks the APN and assigns the MCPTT QCI and ARP for the default EPS Bearer.
3. PCRF sends a credit Control Answer initial (CCA-I) message to PCEF and provisions the MCPTT QCI and the ARP settings.
4. PCRF receives an AAR message from AF with the session information, which includes MCPTT-ID, Reservation Priority, and the AF-Application-identifier associated with the session.
5. PCRF decides the QCI and the ARP based on the parameters received from AF.
6. The PCRF sends a Diameter Authentication, Authorization, and Accounting (AAA) to the AF with `ResultCode=DIAMETER_SUCCESS`.
7. PCRF sends a Reauthorization Request (RAR) message to PCEF to provision the QCI and the ARP. The PCC Rules generated for the AF flows contains the QCI and ARP set by Policy/default configuration.
8. PCEF responds to PCRF with a Reauthorization answer (RAA) message with `ResultCode=DIAMETER_SUCCESS`).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-290 Priority Sharing

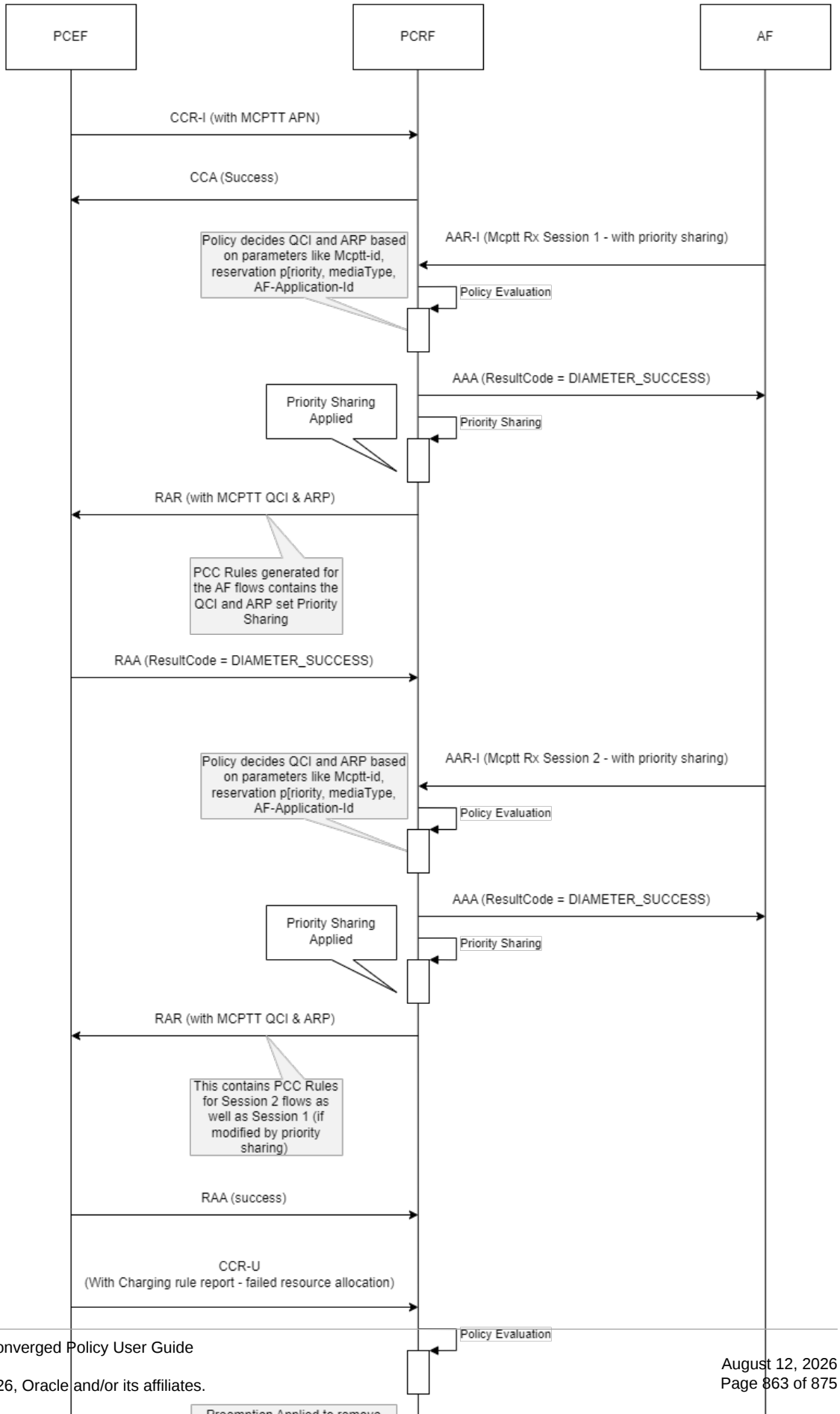


Copyright © 2019, 2026, Oracle and/or its affiliates.

1. The PCEF sends a credit control request initial (CCR-I) message to the PCRF with MCPTT APN details.
2. PCRF sends a credit control answer initial (CCA-I) success message to PCEF.
3. PCRF receives an AA-Request Initial (AAR-I) messages from AF for Rx Session 1 with priority sharing enabled.
4. PCRF decides the QCI and the ARP based on the parameters received from AF.
5. The PCRF sends a Diameter AAA to the AF with `ResultCode=DIAMETER_SUCCESS`.
6. PCRF applies Priority sharing.
7. PCRF sends a Reauthorization Request (RAR) message to PCEF to provision the QCI and the ARP. The PCC Rules for session 1 generated for the AF flows contains the QCI and ARP set by Policy/default configuration.
8. PCEF responds to PCRF with a Reauthorization answer (RAA) message with `ResultCode=DIAMETER_SUCCESS`).
9. PCRF receives an AA-Request (AAR) messages from AF for Rx Session 2 with priority sharing enabled.
10. PCRF decides the QCI and the ARP based on the parameters received from AF.
11. The PCRF sends a Diameter AAA to the AF with `ResultCode=DIAMETER_SUCCESS`.
12. PCRF applies priority sharing.
13. PCRF sends a Reauthorization Request (RAR) message to PCEF to provision the QCI and the ARP. The PCC Rules for session 2 as well as session 1 generated for the AF flows contains the QCI and ARP set by Policy/default configuration.
14. PCEF responds to PCRF with a Reauthorization answer (RAA) message with `ResultCode=DIAMETER_SUCCESS`).
15. PCRF receives a Session-Termination-Request (STR) from AF.
16. AF responds to PCRF with a Session-Termination-Answer (STA).
17. PCRF applies priority sharing.
18. PCRF sends an RAR to remove and update the PCC rules. The RAR message contains the PCC rules removed for Session 2 flows as well as session 1 (if modified by priority sharing).
19. PCEF responds to PCRF with a Reauthorization answer (RAA) message with `ResultCode=DIAMETER_SUCCESS`).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-291 Preemption Control - CCRU- ChargingRuleReport scenario

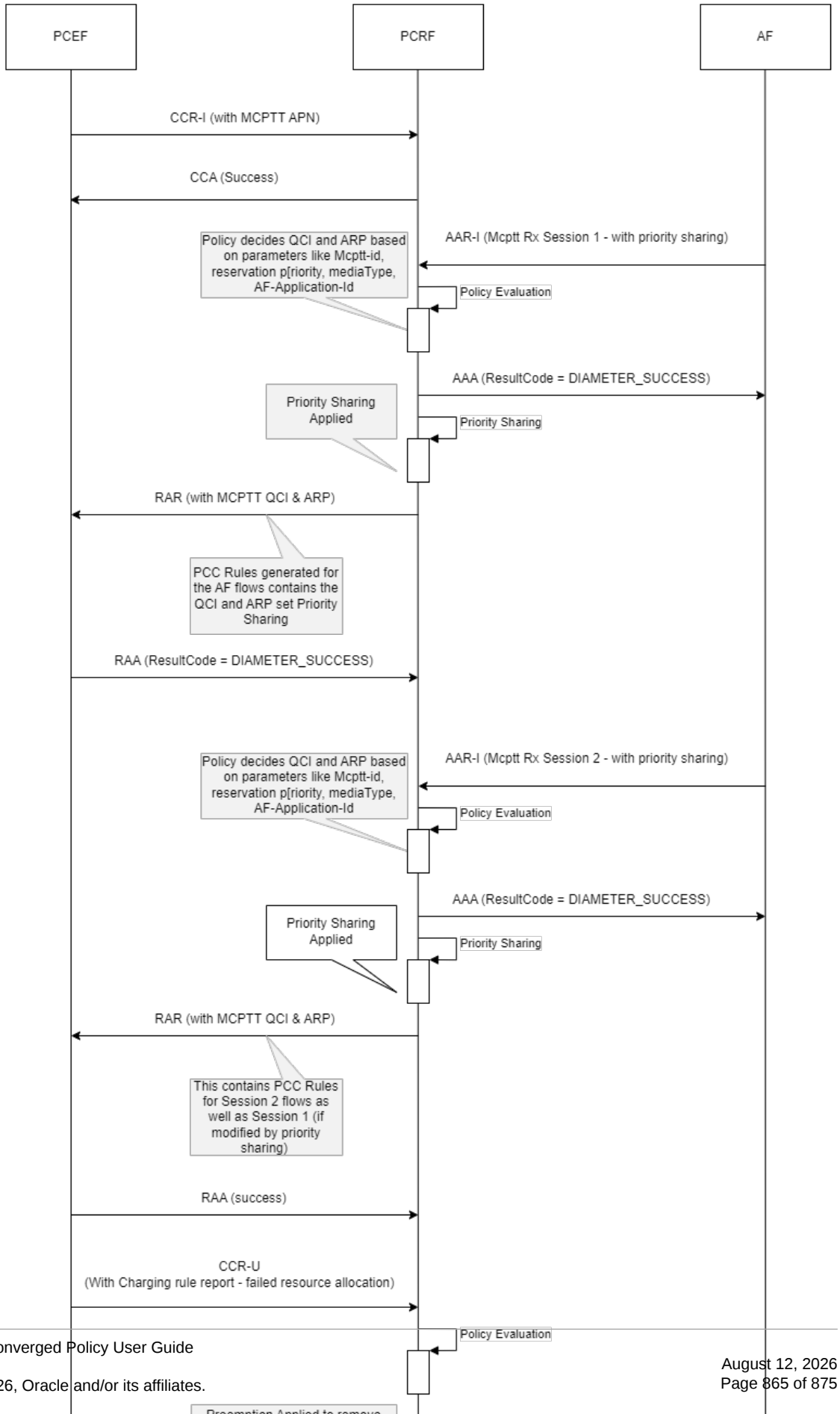


Copyright © 2019, 2026, Oracle and/or its affiliates.

1. The PCEF sends a credit control request initial (CCR-I) message to the PCRF with MCPTT APN details.
2. PCRF sends a credit control answer initial (CCA-I) success message to PCEF.
3. PCRF receives an AA-Request initial (AAR-I) messages from AF for Rx Session 1 with priority sharing and preemption enabled.
4. PCRF decides the QCI and the ARP based on the parameters received from AF.
5. The PCRF sends a Authentication, Authorization, Accounting (AAA) message to the AF with `ResultCode=DIAMETER_SUCCESS`.
6. PCRF applies Priority sharing.
7. PCRF sends a Reauthorization Request (RAR) message to PCEF to provision the QCI and the ARP. The PCC Rules for session 1 generated for the AF flows contains the QCI and ARP set by Policy/default configuration.
8. PCEF responds to PCRF with a Reauthorization answer (RAA) message with ResultCode=DIAMETER_SUCCESS).
9. PCRF receives an AA-Request (AAR) messages from AF for Rx Session 2 with priority sharing and preemption enabled.
10. PCRF decides the QCI and the ARP based on the parameters received from AF.
11. The PCRF sends a Diameter AAA to the AF with `ResultCode=DIAMETER_SUCCESS`.
12. PCRF applies priority sharing.
13. PCRF sends a Reauthorization Request (RAR) message to PCEF to provision the QCI and the ARP. The PCC Rules for session 2 as well as session 1 generated for the AF flows contains the QCI and ARP set by Policy/default configuration.
14. PCEF responds to PCRF with a Reauthorization answer (RAA) message with Charging rule report - failed resource allocation.
15. Also, PCEF sends a Credit Control Request - Update (CCR-U) with charging rule report indicating failed resource allocation.
16. PCRF evaluates the details, and applies priority control and tries the preemption once again to remove eligible rules and retry failed PCC rules.
17. PCRF applies priority sharing again due to removed PCC rules.
18. PCRF sends a Credit Control Answer-Update (CCA-U) to PCEF to remove and update the PCC Rules.
19. PCRF sends an RAR or ASR to AF informing the failed resource allocation for the preempted flow.
20. AF responds to PCRF with a Reauthorization answer (RAA) message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 4-292 Preemption - No Preemptable Rule found



Copyright © 2019, 2026, Oracle and/or its affiliates.

1. The PCEF sends a credit control request initial (CCR-I) message to the PCRF with MCPTT APN details.
2. PCRF sends a credit control answer initial (CCA-I) success message to PCEF.
3. PCRF receives an AA-Request initial (AAR-I) messages from AF for Rx Session 1 with priority sharing enabled.
4. PCRF decides the QCI and the ARP based on the parameters received from AF.
5. The PCRF sends a Authentication, Authorization, Accounting (AAA) message to the AF with `ResultCode=DIAMETER_SUCCESS`.
6. PCRF applies Priority sharing.
7. PCRF sends a Reauthorization Request (RAR) message to PCEF to provision the QCI and the ARP. The PCC Rules for session 1 generated for the AF flows contains the QCI and ARP set by Policy/default configuration.
8. PCEF responds to PCRF with a Reauthorization answer (RAA) message with `ResultCode=DIAMETER_SUCCESS`).
9. PCRF receives an AA-Request (AAR) messages from AF for Rx Session 2 with priority sharing enabled.
10. PCRF decides the QCI and the ARP based on the parameters received from AF.
11. The PCRF sends a Diameter AAA to the AF with `ResultCode=DIAMETER_SUCCESS`.
12. PCRF applies priority sharing.
13. PCRF sends a Reauthorization Request (RAR) message to PCEF to provision the QCI and the ARP. The PCC Rules for session 2 as well as session 1 generated for the AF flows contains the QCI and ARP set by Policy/default configuration.
14. PCEF responds to PCRF with a Reauthorization answer (RAA) success message.
15. Also, PCEF sends a Credit Control Request - Update (CCR-U) with charging rule report indicating failed resource allocation.
16. PCRF evaluates the details, and applies priority control and tries the preemption once again to remove eligible rules and retry failed PCC rules.
17. PCRF sends a RAR message to AF informing the failed resource allocation for the preempted flow.
18. PCRF sends a Credit Control Answer-Update (CCA-U) to PCEF indicating no change in the PCC Rules.
19. AF responds to PCRF with a Reauthorization answer (RAA) message.

Managing Support for MCPTT features

Enable

By default, the MCPTT features are enabled.

You can disable the required MCPTT related feature bits using the following two keys under **Advance Settings** in **Settings** page for **PCRF Core** on Oracle Communications Cloud Native Core, Cloud Native Configuration Console (CNC Console):

- Gx.DisableSupportedFeatures (for Gx)
- Rx.DisableSupportedFeatures (for Rx)

For more details on enabling/disabling the MCPTT features using CNC Console, see Settings.

Configure

Copyright © 2019, 2026, Oracle and/or its affiliates.

You can configure the support for MCPTT features using CNC Console and REST API.

Configure using CNC Console

- You can configure the default ARP and default preemption control by applying the configurations under **MCPTT** section in **Settings** page for **PCRF Core** on Oracle Communications Cloud Native Core, Cloud Native Configuration Console (CNC Console). For more details, see Settings.
- To assign the QCIs, apply the configurations for **Use Custom QoS Class Identifier** and **QoS Class Identifier** parameters while creating the PCC rule on **Create PCC Rule** page. For more information, see PCC Rule.
- To configure PCC profile, apply the configurations for **Use Custom QoS Class Identifier** and **QoS Class Identifier** parameters while creating the PCC rule profile on **Create PCC Rule Profile** page. For more information, see PCC Rule.
- You can use the blockly conditions and actions to set QCI and ARP default EPS bearer. For more information, see *Priority/Emergency* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

Configure using REST API

You can configure PCC Rule, PCC Profile, PCRF-core using the following REST APIs:

- `Core Service`
- `Traffic for PCC Rule`
- `Traffic for PCC Rule Profile`

For more information on configuring using REST API, see *Policy REST Specifications* section in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

4.138 Support for Listing and Comparing UPSIs Received from UDR

Converged Policy provides blocks, conditions and actions to support finding the delta between the UPSI's id list:

- currently configured in PCF
- UPSI's that are send on UE Policy Registration
- UPSIs that are on UDR

It allows the user to install/remove this delta or a subset of delta.

Also, it allows to access the attributes of the UPSI object (UPSC, MCC and MNC) and can be able to check the URSPs that are configured to be installed under a specific UPSI.

For details on the UE Policy blocks, actions, and conditions used for this functionality, see *UE Policy Blocks* section in *Oracle Communications Cloud Native Core, Converged Policy Design Guide.*

4.139 Roaming Support in Policy

PCRF supports S8 Home Routing scenario for LTE and VoLTE networks in 4G deployment.

Copyright © 2019, 2026, Oracle and/or its affiliates.

S8 Home Routing allows the home operator to control the services and policies applied to the roaming subscriber. S8 interface connects the visited network's Serving Gateway (SGW) to the home network's PGW.

Since the data is routed through the home network's PGW, the home network's PCRF applies the subscriber's policy and charging rules such as QoS and PCC Rules.

The PCRF at home network interfaces the home network PGW and applies the policies on Gx interface, such as identifying a roaming subscriber from 3GPP-SGSN-MCC-MNC AVP and applying differentiated QoS parameters for the roaming subscribers.

For details on how to write a policy based on MCC and MNC, see *Creating Policies* section in *Cloud Native Core, Converged Policy Design Guide*.

> **Note**
>
> Currently, Policy do not support:
>
> - Roaming in 5G deployment (using PCF).
> - Local Breakout (LBO)

4.140 Wi-Fi Support using RAT-Type AVPs

To support Wi-Fi (WLAN) and voice over Wi-Fi, RAT-type Attribute-Value Pair (AVP)s are included in Credit-Control-Request (CCR) messages to inform the CnPCRF about the access technology through which the UE is connected. RAT-Type is usually included as an enumerated AVP, where each type of RAT is represented by a predefined integer value.

The following are some of the values allowed for RAT-Type AVPs:

- EUTRAN (LTE)
- WLAN (Wi-Fi)
- UTRAN (3G)

Based on the RAT-Type, the CnPCRF can apply different Policy rules.

For example, different quality of service (QoS) and charging rules can be applied for a user connected using Wi-Fi (WLAN) compared to a user connected through LTE (EUTRAN).

When a UE moves from one RAT to another (for example, from LTE to Wi-Fi), the network triggers a CCR-U message with the updated RAT-Type AVP. This allows the PCRF to dynamically adjust policies in real-time.

RAT type in conjunction with other parameters in the CCR, such as user location information, subscriber profile from data sources enables operators to create dynamic, and user-centric policies in CnPCRF.

Enable

This feature is enabled automatically at the time of Policy installation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.141 Support for Database Slicing

Whenever Policy services (SM service, PCRF Core, or Usage Monitoring service) receives a Create, Retrieve, Update, or Delete request from any of the microservices, the request is processed by the main database (SMPolicyAssociation database, UMContext, GxSession).

With the use of MySQL NDB software, there is a limitation on having a single replication channel for a given database. When the commit rate for a database is very high, the replication of the database impacts the replication performance depending upon the number of commits as well as the commit (record) size.

In order to overcome the replication limitations of the database, especially in a multisite environment, the database can be sliced based on a particular slicing criteria. The database tables are divided into different slices based on the Helm configuration (such as SM_POLICY_ASSOCIATION_TABLE_SLICING_COUNT for SMPolicyAssociation, UM_CONTEXT_TABLE_SLICING_COUNT for UMContext and GX_SESSION_TABLE_SLICING_COUNT for GxSession). After the slices are created, the database records are distributed across all the slices.

With this database slicing, instead of the main database processing all the requests, some of the database operations are processed using sliced tables.

The number of slices can be configured depending upon the replication requirements.

For example, if a single slice is able to replicate up to ~40K TPS and the immediate TPS need is ~75K, two slices can support the immediate required load. If the estimated projected growth YoY is 25%, the TPS need after 5 years reaches around ~200K TPS. Thus a table slice count of 8 can be used to manage the database load for the next 5 years.

> **Note**
>
> This calculation takes into consideration only replication channel and not any other challenges that may come up for 200K TPS.

By default, there is no separate replication channel for each of these slices. Replication channels can be configured. For example, two replication channels can be configured, each replicating 4 slices. This configuration can change depending on the increase in TPS and available bandwidth across the replicating sites.

Managing the Support for Database Slicing

Slicing SMPolicyAssociation for SM service

While upgrading from an older version of Policy to a later version, you can configure the Database Slicing feature for SM service database (SMPolicyAssociation table) as follows:

1. In CNC Console, under **Service Configurations** on **PCF Session Management** page, set the value of ENABLE_SM_POLICY_ASSOCIATION_TABLE_SLICING advanced settings key to `true`. This will enable the database slicing on SMPolicyAssociation. By default, the value of this key is set to `false`. Once the database slicing is enabled, the database operations are processed on the sliced tables.

   When ENABLE_SM_POLICY_ASSOCIATION_TABLE_SLICING is enabled, the Audit Service audits the SmPolicyAssociation sliced tables as well.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Configure the number of slices using SM_POLICY_ASSOCIATION_TABLE_SLICING_COUNT Helm parameter.

   By default, the slicing count is set to 1.

   During the upgrade, add the Helm configuration in custom.yaml file to configure SM_POLICY_ASSOCIATION_TABLE_SLICING_COUNT parameter.

   The slicing table feature is backward compatible, so that the older Create, Retrieve, Update, and Delete operations work as expected. Data is populated in new tables after a successful upgrade and when ENABLE_SM_POLICY_ASSOCIATION_TABLE_SLICING is set `true` using CNC Console.

   > **Note**
   >
   > After enabling the feature, make sure that it is not disabled again because data can not be fetched from sliced tables.

Slicing for UMContext database for Usage Monitoring service

While upgrading from an older version of Policy to a later version, you can use the following Helm parameters to configure the table slicing feature for Usage Monitoring database (umContext table):

- `ENABLE_TABLE_SLICING`: to enable the database slicing feature. By default, this parameter is disabled.
- `UM_CONTEXT_TABLE_SLICING_COUNT`: to configure the number of slices created. By default, the slicing count is set to 1.

The `ENABLE_UM_CONTEXT_TABLE_SLICING` key under **Advanced Settings** in **Usage Monitoring** page for **Service Configurations** in CNC Console is used to enable/disable the database operations on sliced tables. That is, whenever `ENABLE_UM_CONTEXT_TABLE_SLICING` key is set to `true`, the create/retrieve/update/delete operations are performed on the database slices instead of the main database.

By default, `ENABLE_UM_CONTEXT_TABLE_SLICING` key is disabled.

For example, when PCRF Core sends a create request to Usage Monitoring service and `ENABLE_UM_CONTEXT_TABLE_SLICING` flag is enabled, the Usage Monitoring service responds to PCRF Core with **x-oc-slicing-info**, which contains the slicing information of Usage Monitoring database (UmContext table). PCRF Core stores this information in its Gx session database. In subsequent update or terminate requests, PCRF Core uses this in the header.

In case of any change in `UM_CONTEXT_TABLE_SLICING_COUNT` parameter, existing sessions in the UmContext table will not be impacted. Data can still be retrieved from the older slices.

> **Note**
>
> After enabling the `ENABLE_UM_CONTEXT_TABLE_SLICING` flag, make sure not to disable it again. Otherwise, data cannot be fetched from sliced tables.
>
> Also, in case of rollback, data saved on sliced tables cannot accessed. Data saved on the sliced tables must be manually ported to the main database.

In case of a change in `UM_CONTEXT_TABLE_SLICING_COUNT` parameter:

Copyright © 2019, 2026, Oracle and/or its affiliates.

The PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT key under **Advanced Settings** in **Usage Monitoring** page for **Service Configurations** in CNC Console is used to store the previous slicing count.

If UM_CONTEXT_TABLE_SLICING_COUNT is changed and the service cannot find the data with the current slicing count, it uses PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT to search for the data.

If there are multiple values for PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT, the Usage Monitoring service uses the latest previous count and if the data is still not found, it uses the next previous count. That is, if PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT contains two values such as 0 and 5, the Usage Monitoring service first uses the previous count as 5 to search for the data. If it is still not found, the service uses the previous count as 0 to search for the data.

To reduce latency, you can alter the number of slices one at a time. After migrating from the previous table count to the newly completed one, switch to the new count.

After all the data from the previous slicing count is moved to the new slicing count, make sure to remove the previous count from PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT.

If PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT does not contain 0, and ENABLE TABLE SLICING parameter is set to true, the data cannot be searched on the primary table.

Slicing in GxSession database for PCRF Core service
While upgrading from an older version of Policy to a later version, you can configure the Database Slicing feature for GxSession database as follows:

1. Enable the table slicing for GxSession database using GX_SESSION_TABLE_SLICING_ENABLED Helm parameter. This enables the database slicing on GxSession database. By default, the value of this key is set to false. Once the database slicing is enabled, the database operations are processed on the sliced tables.
2. When DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING advanced settings key is enabled, the Audit Service audits the GxSession sliced tables as well.
3. Configure the number of slices using GX_SESSION_TABLE_SLICING_COUNT Helm parameter. By default, the value of this parameter is set to 1.
4. In CNC Console, under **PCRF Core Settings** page in **Service Configurations**, set the value of DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING advanced settings key to true. By default, the value of this key is set to false. When this key is enabled and if the new slices for Gx are created, traffic for GxSessions are distributed across all the new tables. PCRF Core service will register the new tables with Audit service and also distributes the new sessions to the new slices.

> **Note**
>
> DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING advanced setting key must be enabled after upgrade or install with table slicing processes are done.

GxSession table slicing requires two separate configuration steps.

- The Helm parameters GX_SESSION_TABLE_SLICING_ENABLED and GX_SESSION_TABLE_SLICING_COUNT are used only by the installation and upgrade hooks. When GX_SESSION_TABLE_SLICING_ENABLED is set to true, the hook creates additional GxSession slice tables based on GX_SESSION_TABLE_SLICING_COUNT. For example, if GX_SESSION_TABLE_SLICING_COUNT is set to 3, the expected tables are

Copyright © 2019, 2026, Oracle and/or its affiliates.

gxsession, gxsession_1, and gxsession_2. These parameters prepare the database schema but do not enable runtime traffic distribution.

- The DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING advanced setting controls runtime behavior. When this setting is set to true, PCRF Core uses the Session-Id and the table-slicing function to select the target GxSession table for create, update, delete, and primary-key lookup operations. PCRF Core also registers the sliced GxSession tables with Audit Service when this setting is enabled.

Because these configurations are separate, enable DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING only after the installation or upgrade process is complete and the configured GxSession slice tables exist in the database. If you enable the advanced setting before the slice tables are created, PCRF Core might attempt to distribute traffic to tables that do not exist.

Identifying the slice for database operation:

- When PCRF Core service receives a CCR-I message, the primary key is hashed to find the slice. To save the GxSession in the database, use the primary key in the slicing function. The slicing function provides the slice number where the association can be saved.
- When PCRF Core service receives a CCR-U message, the slice number is obtained using the slicing function. Note that the Session-Id must never be changed. To update the database, the Session-Id is used with the slicing function to obtain the slice number where the association is saved.
- When PCRF Core service receives a CCR-T message, the slice number is calculated using the slicing function. The Session-Id is passed to the slicing function to obtain the slice number where the association to be deleted can be found.

Note

- You can start with a fixed number of slices that is estimated to cater to the replication needs of the near future (for example, next 5 years).
- All table slices may not have their own replication channels to start with. For example, to enable 75K TPS, only 2 replications channels can be configured, each replicating 4 slices. This configuration can change depending on the increase in TPS and available bandwidth across the replicating sites.
- Records are distributed across all the slices. This helps in reconfiguring the slice to replication channel mapping. No migration is required as long as the table slice count does not change.
- The hashing function selected is `Consistent Hash`.
- The hashed slice number is provided to the consumer service accessing the database as part of the resource-id to avoid the requirement of migration if and when the table slices need to be increased.
- For secondary key lookup, a parallel search is performed across all the table slices.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

Mixed-version deployments are not supported in multisite configurations for PCRF Core GxSession table slicing. When Policy is upgraded and the source and target versions are the same, the upgrade procedure does not create the database slice tables. Enable and configure slice creation using Helm. For more information, see *Preupgrade Tasks* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

The following are some of the scenarios of database slicing during a Policy software upgrade in a geo-redundant setup:

- All sites are running an older software version, and the first site is upgraded to a release that supports table slicing. Runtime distribution remains disabled. In this case, there is no runtime impact. Activating runtime distribution across the new slice tables requires enabling the DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING Advanced Setting.
- All sites are upgraded to a software version that supports table slicing. The required slice tables are created using Helm, but runtime distribution is enabled only on Site 1. In this case, GX_SESSION_TABLE_SLICING_ENABLED and GX_SESSION_TABLE_SLICING_COUNT were used during installation or upgrade to create the GxSession slice tables, but DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING is enabled only on Site 1. Gx sessions are distributed across the configured slice tables only on Site 1. Sites where DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING remains disabled continue to use only the primary gxsession table for new runtime operations.

  This scenario does not represent a software version mismatch because all sites are running a version that supports GxSession table slicing.
- A new site is added to an existing cluster where runtime distribution is disabled, while other sites have runtime distribution enabled with four slices. Sites where runtime distribution is enabled distribute Gxsessions across the configured slice tables. If runtime distribution remains disabled on the new site, the site continues to use only the primary Gxsession table for new runtime operations.
- A new site is added to an existing cluster with runtime distribution enabled with four slices, while runtime distribution remains disabled on the existing sites. The new site distributes Gx sessions across the configured slice tables. Existing sites where runtime distribution remains disabled continue to use only the primary Gxsession table for runtime operations.

Observability

Metrics

Slicing SMPolicyAssociation for SM service

occnp_db_overall_processing_time. getBySecondaryKeyV4 metric is used to calculate total response time for secondary key serial search when table slicing on SMPolicyAssociation database is enabled.

Slicing UMContext for Usage Monitoring service

usage_mon_context_found metric is used to count the session lookup on the main table or the sliced tables for old sessions of the subscribers when table slicing is enabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4.142 Support for Interworking Between Evolved Packet Core (EPC) and CNC

This section describes how Converged Policy supports interworking between Evolved Packet Core (EPC) and 5G Cloud Native Core (CNC).

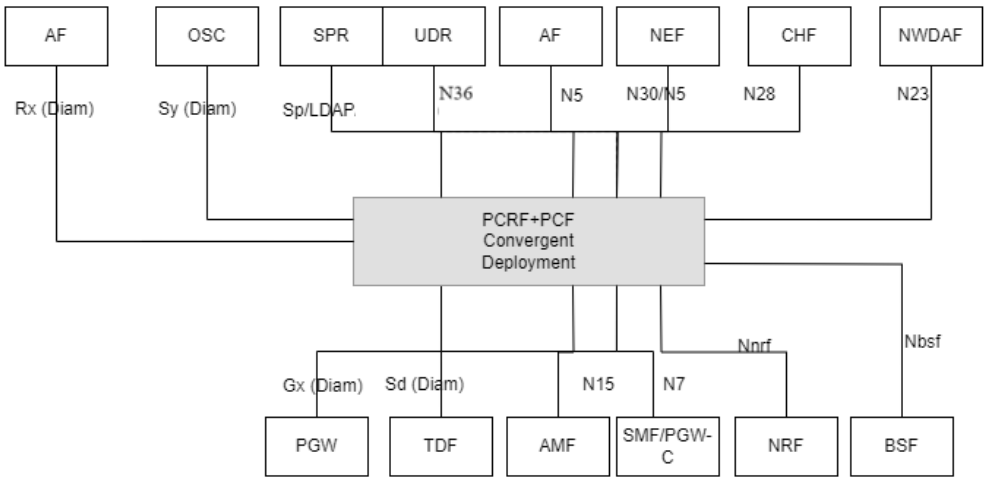
EPC provides converged voice and data services on a 4G LTE network to enable advanced services, such as VoIP.

EPC comprises:

- Serving Gateway (SGW)
- PDN Gateway (PGW)
- Mobility Management Entity (MME)
- Home Subscriber Server (HSS)

Converged Policy deployment to support both EPC/5G Core network element

Figure 4-293 Converged Policy Architecture to Support EPC and 5GC



3GPP recommends the following deployment Options with both LTE,NR and EPC,5GC co-exist. The Interfaces on which the UE attach lands for each of these options is shown.

Table 4-199 Deployment Options

3GPP Deployment Options	CnPolicy (PCRF+PCF)
Option 1: Standalone LTE under EPC	UE attaches to CnPolicy over Diameter Gx Interface.
Option 2: Standalone NR under 5GC	UE attaches to CnPolicy over Nsmf/N7 Interface.
Option 3: NonStandalone LTE and NR under EPC	UE attaches to CnPolicy over Diameter Gx Interface.
Option 4: NonStandalone NR and LTE under 5GC	UE attaches to CnPolicy over Diameter Gx Interface.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 4-199 (Cont.) Deployment Options

3GPP Deployment Options	CnPolicy (PCRF+PCF)
Option 7: Non Standalone LTE and NR under 5GC	UE attaches to CnPolicy over Nsmf/N7 Interface.

Typical Migration strategy from 4G LTE to 5GC SA is as follows:

4G LTE -> NSA Option 3 -> NSA Option 7: NSA Option 4 -> SA Option 2

Copyright © 2019, 2026, Oracle and/or its affiliates.

5

Integrating Policy with Different Network Functions

You can integrate Oracle Communications Cloud Native Core, Converged Policy with different Network Functions (NFs), such as Oracle Communications Cloud Native Core, Network Repository Function (NRF), Oracle Communications Cloud Native Core, Unified Data Repository (UDR), and Charging Function (CHF).

NRF Integration

NRF Management (Client) service enables policy solution to integrate with NRF server for service registration, discovery, and service status/ load related information.

Management Service support includes the following functions:

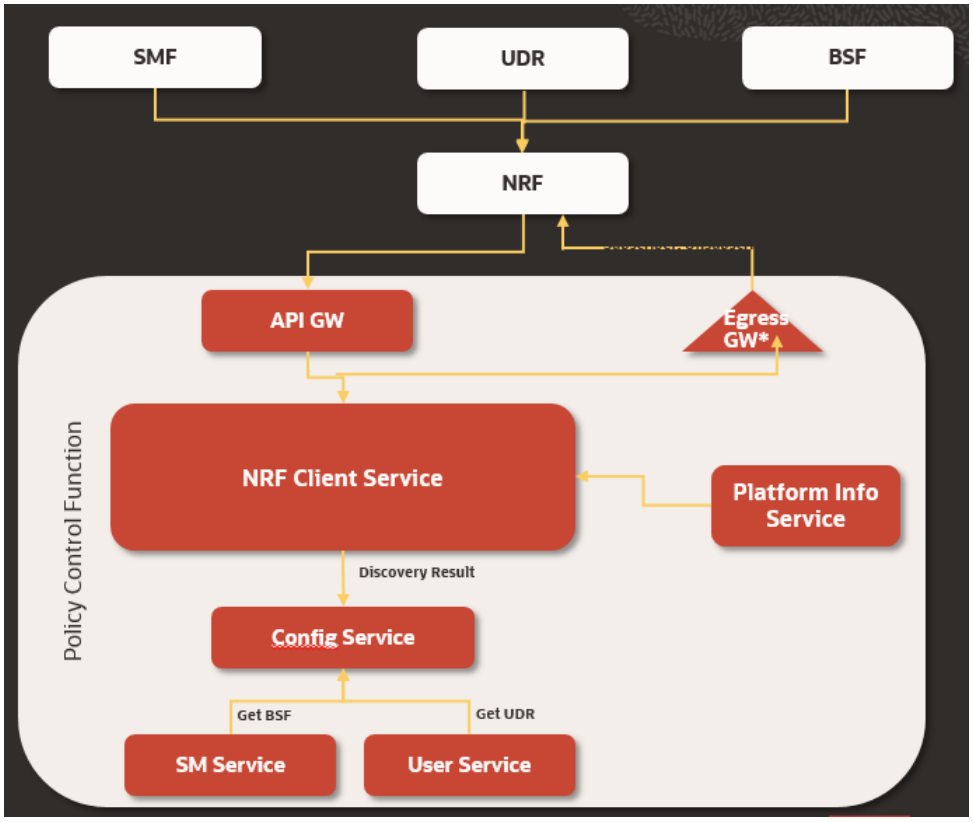
- Register Service
- Deregister Service
- PCF heartbeat to NRF that includes load, priority, and capacity information
- Knowledge to NRF of scaling change
- Subscribe or Unsubscribe

Discovery Service

- Used to discover UDR, BSF, and CHF services
- Compliant with 29.510

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 5-1 NRF Integration



Editing Kubernetes Configuration Map

A Kubernetes Configuration Map is provided to save the NRF address and the NF Profile information. You can edit the Kubernetes Configuration Map to register Policy Control Function (PCF) with the NRF.

To edit the Kubernetes Configuration Map:

Open a console to the master node of the Kubernetes deployment and edit the config map named "*pcf-name*-application-config" where *pcf-name* is the HELM chart release name used at the time of installation, see *Oracle Communications Cloud Native Core Policy Installation, Upgrade and Fault Recovery Guide*.

1. Get a list of all the config maps in the PCF deployment namespace by running the following command:

   ```
   kubectl get cm -n pcf-namespace
   ```

   where, *pcf-namespace* is the PCF deployment namespace used by the helm command.
2. Edit the application configuration map by running the following command:

   ```
   kubectl edit cm pcf-name-application-config -n pcf-namespace
   ```

   where, *pcf-name* is the release name used by the helm command.
   A standard unix vi editor is opened with the config map contents pre-filled. Use vi commands to edit the application configuration map.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Verify the NRF address (fqdn/IP) and the port number. NRF address is contained in the custom value yaml file. See the `configmapApplicationConfig` attribute in the custom yaml file.
4. Check and add necessary NFs to "nrfClientSubscribeTypes". This is required when PCF needs to autonomously discover and subscribe to certain NF Types. The discovery and subscription is performed each time the primary nrf-client-management pod comes up after a fresh installation or upgrade and/or pod maintenance cycles. Using this procedure, PCF creates and maintains a subscription at the NRF so it can be notified when NF instances change (e.g., new NF registered, deregistered, profile updated) based on NF Type.
   PCF may need to discover and subscribe to UDR, CHF and BSF NF Types.
5. Check and edit the PCF Profile to be registered with the NRF. For example, if required enter the IP details of the PCF Services.
   PCF needs to register with NRF to make itself discoverable to consumer NFs like SMF and AMF. A template of the NF profile is provided that can be edited as required. The important attributes that need to be edited are listed below:
   - NF FQDN
   - Service FQDN and Port
   - Service IP End Points
   - Service API versions and schemes (http/s)

   > **Note**
   >
   > PCF may need to register the following services as per the operator deployment scenarios:
   > - Npcf_AMPolicyControl
   > - Npcf_SMPolicyControl
   > - Npcf_UEPolicyControl
6. Save and exit the editor.

Configuring Capacity of NFProfile and NFService using Policy CNC Console

The PCF heartbeat to NRF includes load, priority, and capacity information. The `capacity` is a static capacity information in the range of 0-65535, expressed as a weight relative to other services of the same type.

PCF provides the capability to change the `capacity` of a PCF instance in its NF Profile or NF Service and update the same to NRF. The Policy operator can use CNC Console to make changes to this parameter for a profile, this field was previously fetched from **perf-info** service only. These changes are committed to common configuration database which allow handling of upgrade and rollback scenarios. The import and export of updated profile is supported as done for other configuration parameters.

To configure, the "Capacity" field manually on the Policy CNC Console, navigate to "Policy -> Status and Query -> NF Data -> NF Registration Profile" section. For more information on the NF registration profile, see PCF Registration Profile menu in CNC Console.

You can now configure or update the NfProfile or NfService parameters through REST or CNC Console. These parameters can not be configured using Helm. **NfProfileConfigMode** in HELM mode is not a valid scenario for this feature. The **dynamicLoadAndCapacity** values coming from common configuration database are considered only when the **NfProfileConfigMode** parameter is set to REST.

Copyright © 2019, 2026, Oracle and/or its affiliates.

NRF-Client has different validations based on the **dynamicLoadAndCapacity**. For example, if the **nfProfile/ServiceLoad(or dynamicLoad)** is set to false and **nfProfile/ ServiceCapacity(or dynamicCapacity)** is set to true, then perf-info will be called and the response will be used for NF Profile load and the capacity set in the profile coming from common configuration database will be used for NF Profile capacity only. So, even that the CNC Console is allowing to change capacity and load for nfprofiles and nfservices, the dynamicLoadAndCapacity flags mentioned in the following code snippet control from which source the value will be taken. For example:

```
dynamicLoadAndCapacity.nfProfileLoad = false
dynamicLoadAndCapacity.nfServiceLoad = false
dynamicLoadAndCapacity.nfProfileCapacity = true
dynamicLoadAndCapacity.nfServiceCapacity = true
NfProfileConfigMode = REST
```

> **Note**
>
> There exists a specific limitation during the upgrade process due to the **dynamicLoadAndCapacity** parameter being unavailable in releases prior to 25.1.200. For instance, when performing an upgrade from version 24.2.x to 25.1.200, the NRF Client exhibits varying validations dependent upon the **dynamicLoadAndCapacity** parameter. In scenarios where the CNC Console facilitates the modification of capacity and load for nfprofiles and nfservices, the **dynamicLoadAndCapacity** parameter governs the source from which the value is obtained.

UDR and CHF Integration

Policy solution supports integration with external policy data sources using user service encapsulates all the DB integration complexity from other micro-services. The feature helps the dynamic discovery of UDR and CHF from NRF and Nudr/Nchf interfaces.

Support for CHF to access counter information

- This is an evolution of the Sy interface, where the PCF consumes the Nchf_SpendingLimitControl service provided by the CHF.
- The service enables the PCF to retrieve policy counter status information per UE from the CHF by subscribing to spending limit reporting, such as notifications of policy counter status changes.
  - Dynamic discovery of CHF from NRF
  - Support for policy counter retrieval and subscription for changes and notification handling
  - Compliant with 29.594 v15.2.0

Support for UDR
This is an evolution of the 4G UDR/SPR where the PCF is able to retrieve, update, subscribe, and get notified to changes for:

- Session Management Policy Data
- Access And Mobility Policy Data
- UE policy data

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Usage Monitoring Data
- Policy Data Subscriptions
- Individual Policy Data Subscription
- Compliant with 29.519 V15.2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

6
Configuring Policy

This section provides the information for configuring Oracle Communications Cloud Native Core, Converged Policy for various services.

Policy offers the following interfaces to configure the solution:

- A web-browser based Graphical User Interface (GUI)
  For more information on configurations using GUI, see Configuring Policy Using CNC Console.
- A REST API based Machine-to-Machine interface
  For more information about Policy REST APIs, see *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.
- Custom Value files to customize the Policy deployment.
  The Policy deployment can be customized by overriding the default values of various configurable parameters in the custom value files. For more information about downloading and customizing the custom value files, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.
- Kubernetes Configuration Maps. This configuration map is used to register PCF with NRF.
  For more information, see Integrating Policy with Different Network Functions.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7
Configuring Policy Using CNC Console

This chapter describes how to configure different global and service parameters in Oracle Communications Cloud Native Core, Converged Policy using Oracle Communications Cloud Native Core, Cloud Native Configurations Console (CNC Console).

Oracle Communications Cloud Native Core, Cloud Native Configuration Console Interface

This section provides an overview of the CNC Console, which includes an interface to help in creating global and service parameters in Policy.

You can use Policy integration with CNC Console only after logging successfully in to the CNC Console application. To log in to the CNC Console, make the following updates to the hosts file available at the `C:\Windows\System32\drivers\etc` location.

1. In Windows system, open the **hosts** file in a notepad as an Administrator and append the following set of lines at the end:

   ```
   <IP Address> cncc-iam-ingress-gateway.cncc.svc.cluster.local
   ```

   ```
   <IP Address> cncc-core-ingress-gateway.cncc.svc.cluster.local
   ```

   where:

   <IP Address> is the host address of the deployment cluster. It depends on the deployment cluster.

   Example:

   ```
   10.75.225.189 cncc-iam-ingress-gateway.cncc.svc.cluster.local
   ```

   ```
   10.75.225.189 cncc-core-ingress-gateway.cncc.svc.cluster.local
   ```

   > **Note**
   >
   > The IP Address can change when deployment cluster changes.

2. Save and close the hosts file.

> **Note**
>
> Before logging into CNC Console, create a CNC user and password. Using these user details, you can log in to the CNC Console application. For more information about creating a CNC Console user and password, see *Oracle Communications Cloud Native Core, Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

To log in to CNC Console:

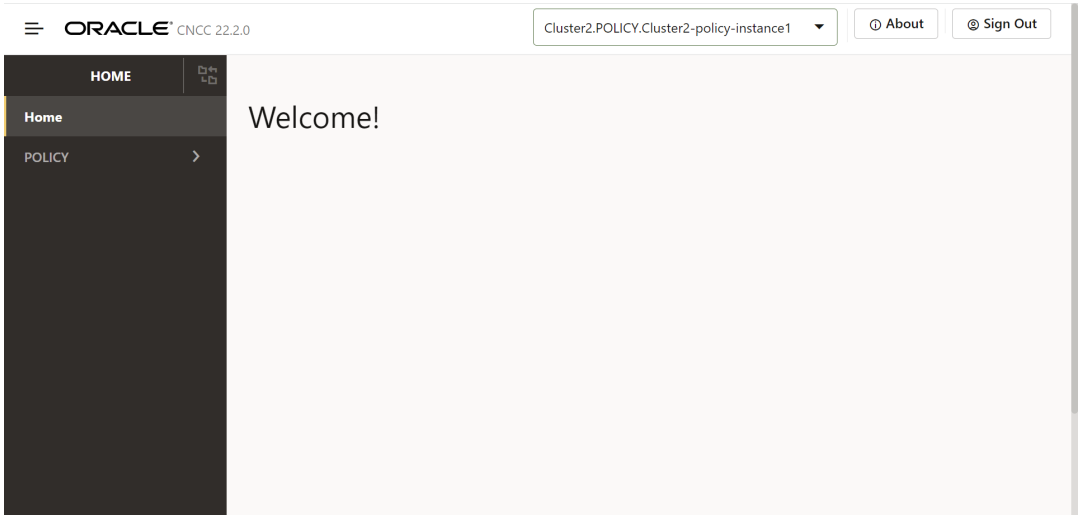
1. Open a web browser and enter the URL: http://*<host name>*:*<port number>* and press Enter.
   Where, *<host name>* is cncc-iam-ingress-ip and *<port number>* is cncc-iam-ingressport.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The log in page opens.

2. Enter the **Username** and **Password**.
3. Click **Log In**.
4. On the Welcome page, select the required NF instance from the **Please Select Instance** drop-down field.
   This opens the CNC Console home page for the selected NF instance:

Figure 7-1 CNC Console for Policy



5. To use Policy services integrated with CNC Console, click **Policy** in the left navigation pane.

> **Note**
>
> For all the request timeout configurations using CNC Console if the default request timeout value is modified, then the value being set has to be higher than downstream services request timeout value.

7.1 General Configurations

This section describes how to customize the general settings in a Policy deployment using the **General Configuration** pages. The configurations include general settings, such as log levels settings, enabling or disabling metrics, subscriber activity logging settings, and so on.

7.1.1 General Settings

The **General Settings** page displays the General Settings related to the Policy setup. The page allows you to edit the configurations.

To edit the General Settings:

1. From the navigation menu, under **Policy**, navigate to **General Configurations**, and select **General Settings**.
   This opens the **General Settings** page. The page displays the existing configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Click Edit.
   This opens the **Edit General Settings** page.
3. Enter the following information:

Table 7-1 Edit General Settings

Field Name	Description
API Gateway Host	Specifies the name for the API gateway host .
API Gateway Port	Specifies the port number of the API gateway .
Enable Tracing	Specifies whether to enable/disable tracing. The default value is `true`.
Enable Metrics	Specifies whether to enable/disable system metrics. The default value is `true`.
Enable TLS	Specifies whether to enable/disable TLS. The default value is `false`.
Enable Subscriber Activity Logging	Specifies whether to enable/disable subscriber activity logging. The default value is `false`.
Enable Policy Event Record	Specifies whether to enable/disable Policy Event Record (PER) feature. The default value is `false`.
Policy Event Record Host	Specifies the valid URL of PER host to receive the PER record. The format of the URL is: http://*per-host*:*per-port*, where *per-host* specifies the PER host and *per-port* specifies the PER port. For example, `http://localhost:8101/v1/echo`
Enable SBI Correlation	This specifies whether to enable/disable correlation-info header in PCF. The default value is false.

Table 7-2 Enhanced Logging Configuration

Field Name	Description
Enable Enhanced Logging	Determines whether the service logs the enhanced error response or not. This enabled the LoggingUtils logger. **Default value**: `false`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-2 (Cont.) Enhanced Logging Configuration

Field Name	Description
Enable UE Identifier Information	Determines whether the UE identifier information (SUPI/GPSI) is logged as part of enhanced logging or not. When multiple identifiers are present, the hierarchy follows: a. SUPI b. GPSI **Default value**: `false` **Note** For the subscriberId or subscriptionId, choose only between GPSI/MSISDN and SUPI/IMSI. If both are present, SUPI/IMSI is taken first.

Table 7-3 Truncate Stack Trace Configurations

Field Name	Description
Enable Truncate Stack Trace	Specifies whether to enable or disable the Stack Trace Truncation feature. This will limit the number of lines displayed in the StackTraceUtil logger. **Default value**: `true`
Stack Trace Num of Lines	This field is configured to limit the number of lines shown on the stack trace. **Default value**: 5 **Range**: 0 to 65535

Note

- The enhanced WARN logging is globally applied to all interfaces and call flows (Create, Update, Delete, Notify) involved in SM/Rx operations. You do not require additional configuration.
- The `StackTraceUtil` is always printed; the flag in the configuration only limits the truncation. If it is set to false, the entire stack-trace available in the exception will be printed.
- `MaxJavaStackTraceDepth` JAVA_OPTION configuration takes effect first, and then the number of lines in the stack trace is applied as a limit to the resulting output. See **Support for enhanced StackTrace** in the Logging Support for Error Response section.

4. Click **Save**.
   The page saves the General Settings.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.1.2 Logging Configuration

This section describes how to customize the log level and subscriber logging activity settings in Policy using the **Logging Configuration** pages.

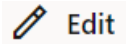
7.1.2.1 Logging Level

This procedure describes how to configure log level for different Policy services through CNC Console.

> **Note**
>
> Default log level for each service is Warn.

The **Logging Level** page displays the log level configured for different Policy services. The page allows you to edit the log level configurations.

To configure the log level:

1. From the navigation menu, under **Policy**, navigate to **Logging Configuration**, and select **Logging Level**.
   This opens the **Logging Level Configuration** page. You can add, edit, or delete the log level and package log level for each service type from this page.
2. Click 

   .
   This opens the **Edit Log Level** page.
3. From the **Service Type** drop-down list, select the service for which you need to view, edit, or delete the logs.

   Policy supports configuring log level for the following service types:

   - PCRF Core
   - PCF Session Management
   - PCF Access and Mobility
   - PCF UE Policy
   - PCF User Connector
   - NRF Discovery Client
   - NRF Management Client
   - Policy DS
   - Bulwark
   - CM Service
   - Config-Server
   - Diameter Gateway
   - Diameter Connector
   - LDAP Gateway
   - Soap-Connector

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Ingress Gateway
- Egress Gateway
- Alternate Route
- Query Service
- Binding Service
- PRE/PRE-Test Service
- Audit Service
- App_info
- Perf-info
- Notifier
- Usage Monitoring
- NWDAF Agent

4. From the **Application Log Level** drop-down list, select the root log level of the application for the selected service type. Possible values are:
   - **TRACE**
   - **DEBUG**
   - **INFO**
   - **WARN**
   - **ERROR**

   > **Note**
   >
   > The value for the **Application Log Level** field is the mandatory value, and the package log level is the optional value.

5. Expand the **Package Log Level** group to enter the package log level information:

   > **Note**
   >
   > This section is only applicable when Oracle Engineering is trying to isolate an issue and requests one or more package names be added and logs collected after the reproduction of an issue.

   a. Click Add .
   The **Add Package log Level** dialog box opens.

   b. Enter the value in the **Package** field.
   The value of **Package** field is dependent on the name of the package in each application. Before you set value of the **Package** field, you must know which package is available in that application.

   c. From the **Log Level** drop-down list, select the log level for the package. Possible values are:
      - **TRACE**

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **DEBUG**
- **INFO**
- **WARN**
- **ERROR**

d. Click **Save**.
The Package log level information for the selected service is saved.

> **Note**
>
> Use the Edit or Delete icons available in the next column to update or delete the package log level information.

6. Click **Save**.
The page saves the log level information for the selected service type.

7.1.2.2 Subscriber Activity Logging

Subscriber Activity Logging allows you to define a list of the subscribers (identifier) that you may require to troubleshoot the NFs and trace all the logs related to the subscribers separately to view. This functionality can be used to troubleshoot problematic subscribers without enabling logs or traces that can impact all subscribers. You can capture and monitor subscriber logs for UDR or CHF notifications, and associated call flow in Session Management (SM), Access and Mobility (AM), User Equipment (UE), PCRF Core, and Egress Gateway.

The Diameter Connector and Diameter Gateway codes have a Java limitation that prevents creating AVP variables starting with a numeric value. As a result, the AVPs generated by these components adhere to the following naming convention:

- 3GPP Specification AVP name: 3gpp-User-Location-Info
- Diam-Connector AVP logging name: User-Location-Info-3GPP

Consequently, Subscriber Activity Logging prints AVP names according to this limitation.

To enable the subscriber activity logging functionality, set value of the **Enable Subscriber Activity Logging** parameter to **true** on the **General Configurations** page. By default, this functionality remains disabled. For more information about enabling the functionality, see General Settings.

This procedure provides information about how to configure and manage subscriber logging.

The **Subscriber Activity Logging** page allows you to create new and manage existing subscribers. The page displays the list of defined subscribers and provides the options to import, export, or add lists.

You can configure the list of subscribers using the **Subscriber Activity Logging** page.

To configure a list of subscribers for logging:

To configure Subscriber Activity Logging:

1. From the navigation menu under **Policy**, navigate to **General Configurations**, click **Logging Configuration**, and then select **Subscriber Activity Logging**.
This opens the **Subscriber Activity Logging** page. The page lists the existing configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Click Add .
This opens the **Create Subscriber Activity Logging** page.
3. On the **Create Subscriber Activity Logging** page, enter the following information:

> **Note**
>
> The number of entries in the **Subscriber Activity logging** page should be less than equal to 20. If the entries are more than 20, the import fails. If you add the 21st entry manually using GUI, the error is displayed.

Table 7-4 Create Subscriber Activity Logging

Field Name	Description
Identifier Type	Select the subscriber identifier type. Supported subscriber identifier type are: • GPSI • SUPI • IPV4 • IPV6 **Note** Subscriber Activity is supported for 64/128 prefix. Following values are allowed in GPSI and SUPI: • GPSI- `extid-123456789@domain.com`, `msisdn-11111` • SUPI- `imsi-311480754396811`, `nai-tmsi06666666.pt12.set001.region48` **Note**: AM and UE services do not support IPV4 or IPV6 identifiers. **Note:** The value which are allowed in SUPI are imsi-311480754396811, nai-tmsi06666666.pt12.set001.region48GSPI are extid-123456789@domain.com, msisdn-11111
Identifier Value	The identifier value for the selected identifier type.
Enable	Use this switch to enable or disable the subscriber logging functionality for the selected subscriber.

4. Click **Save**.
The configuration gets listed on the **Subscriber Activity Logging** page. The page defines the Subscriber Activity Logging configuration in the Policy database and it is available to be used in a Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the configuration.

For details on exporting or importing Subscriber Activity Logging, see Export & Import.

Subscriber Identifiers

SUPI

In the 5G system, a globally unique Subscription Permanent Identifier (SUPI), known as IMSI (International Mobile Subscriber Identity) till 4G, is assigned for each subscription. The SUPIs are assigned in such a manner that it helps in identifying subscriptions and is independent of the user equipment.

For 4G systems, the value of IMSI is structured as:

imsi: <value>

For 5G systems, the value of SUPI is structured as:

supi: imsi-<value>

GPSI

General Public Subscription Identifier (GPSI), known as MSISDN (Mobile Station International Subscriber Directory Number) till 4G, is a 3GPP defined subscriber public identifier that can be used both inside and outside of the 3GPP system. The association between GPSI and its related SUPI are stored in the subscription data in a 5G system.

For 4G systems, the value of MSISDN is structured as:

msisdn/e164:<value>

For 5G systems, the value of GPSI is structured as:

gpsi: msisdn-<value>

Limiting size of the Subscriber Activity Logging Mapping Table

Users can specify the number of sessions in the subscriber activity mapping table. By default, the number of sessions per subscriber is defined as 20 in the mapping table.

However, the users can modify the number of sessions by changing the value on the `SUBS_ACT_MAPPINGTABLE_ENTRY_SIZE` through CM service, Ingress Gateway deployment, or Diameter Gateway.

Limiting size of the mapping table helps in maintaining the network latency and size of the mapping table.

7.1.3 SBI Ingress Error Code Profiles Collection

This procedure provides information about how to use the SBI Ingress Error Code Profiles Collection page to create and manage SBI Ingress error code profiles collection in General Configurations.

To configure Error Code profiles collection, perform the following steps:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the navigation menu, under **Policy**, click **General Configurations**, and then select **SBI Ingress Error Code Profiles Collection**.
   This opens the SBI Ingress Error Code Profiles Collection page.
2. Click Edit.
   This opens the Edit SBI Ingress Error Code Profiles Collection page.
3. Click Add .

   This opens the Add SBI Ingress Error Code Profiles Collection page.
4. Enter values for the available input fields as described in the following table:

Table 7-5 Error Code Profiles Configurations

Field Name	Description
Name	Specifies a unique name to identify the error profile.
Error Code	Specifies the HTTP Code that is populated in the error response when a message request is rejected due to overload control.
Error Cause	Specifies the error cause that is populated in the error response when a message request is rejected due to overload control.
Error Title	Specifies the error title that is populated in the error response when a message request is rejected due to overload control.
Error Description	Specifies the error description that is populated in the error response when a message request is rejected due to overload control.

5. Click **Save** to save the error code profile.
   To discard the changes, click **Cancel**

   The value gets listed on the SBI Ingress Error Code Profiles Collection page. Use or available under the **Actions** column to update or delete the profile.

7.1.4 Policy Mated Region

This procedure provides information about how to create and manage the sites for takeovers in case of failure scenarios.

The **Policy Mated Region** page allows you to create new and manage existing sites for takeover. The page displays the list of defined sites with the options to import, export, or add profiles.

To configure site:

1. From the navigation menu under **Policy**, navigate to **General Configurations**, and then select **Policy Mated Region**.
   This opens the **Policy Mated Region** page. The page lists the existing sites. You can add or import new profiles using this page.
2. Click Add .
   This opens the **Create Policy Mated Region** page.
3. On the **Create Policy Mated Region** page, enter the following information:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-6 Create Policy Mated Region

Field Name	Description
Name	The unique name for the site. This name is used to refer to the site in Site Fallback configuration as explained in Site Fallback. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Site ID	The UUID of the site.

4. Click **Save**. The site details gets listed on the **Policy Mated Region** table.

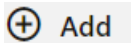
> **Note**
>
> As the config-server database table is site specific and not Geo-replicated across sites, the configurations for Site Fallback and the associated Policy Mated Region on each individual site must be manually added.

7.1.5 Site Fallback

This procedure provides information about how to create and manage the sites for takeovers in case of failure scenarios.

The **Site Fallback** page allows you to create new and manage existing sites for takeover. The page displays the list of defined sites with the options to import, export, or add profiles.

To configure site:

1. From the navigation menu under **Policy**, navigate to **General Configurations**, and then select **Site Fallback**.
   This opens the **Site Fallback** page. The page lists the existing sites. You can add or import new profiles using this page.
2. Click 

   .
   This opens the **Create Site Fallback** page.
3. On the **Create Site Fallback** page, enter the following information:

Table 7-7 Create Site Fallback

Field Name	Description
Site Name	Name of the site for which the fallback sites must be configured. The fallback site can be selected from the drop-down list of sites that are created on **Policy Mated Region** page. For details on **Policy Mated Region**, see Policy Mated Region. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Fallback List	Click Add to configure **Fallback List**, this opens the **Add Site Fallback List** pop-up window. In the **Add Site Fallback List** window configure the following fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-7 (Cont.) Create Site Fallback

Field Name	Description
Fallback Site Name	The drop down list of fallback site names. This list is populated from **Policy Mated Region** Configurations. Select the sites that must be considered for fallback. Timer adoption for Audit service is considered based on the configured fallback priority.
Preference Order:	The preference order of the selected sites. Site with highest priority is considered for timer adoption. If the site with higher priority is unavailable, site with next priority takes over the timer adoption.

4. Click **Save**. The site details gets listed on the **Fallback List** table.

> **Note**
>
> If the Audit service of the configured site becomes unavailable, and all the audit pods are unable to manage the timers created at that site, Audit service at the configured fallback site takes over the timer adoption and processes the timers.
>
> For example, if the **Fallback List** includes three sites configured as follows:
>
> ```
> [{"name":"site1","fallbackList":
> [{"fallbackSiteName":"site2","preferenceOrder":"1"},
> {"fallbackSiteName":"site3","preferenceOrder":"2"}]}]
> ```
>
> In this case, site1 is considered for timer adoption for Audit service. If the Audit service at site1 is unavailable, the Audit service at site2 will process the timers of site1. If Audit service is unavailable at both site1 and site2, the Audit service at site3 will process the timers.

7.2 Error Handling

This section describes how to manage and view the error configurations in Policy, using the **Error Handling** Configurations page.

7.2.1 Error Configurations

The error handling framework allows the users to configure an error state and an action for it. The action contains two parts, an error rule and an error context. On the Console UI, the operator configures the error state specific to the PCF services and the list of actions for it.

The **Error Configurations** page displays the error configurations related to different Policy services.

To add error handler template for a Policy service:

Error Configurations for Diameter Gateway Service

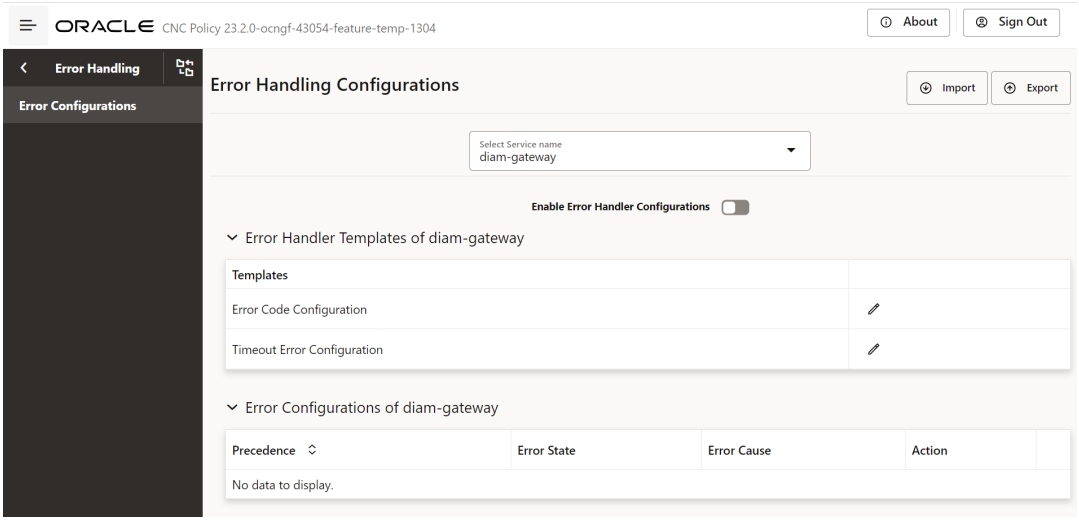
1. From the navigation menu, under **Policy**, click **Error Handling**, and select **Error Configurations** page. This opens the **Error Handling Configurations** page.
2. From the `Select Service Name` drop-down list select the value `diam-gateway`. The page allows you to add and edit configurations for diameter message retry for Rx RAA or Rx

Copyright © 2019, 2026, Oracle and/or its affiliates.

ASR. On the page **Error Handler Templates of diam-gateway** and **Error Configurations of diam-gateway** subsections are displayed.

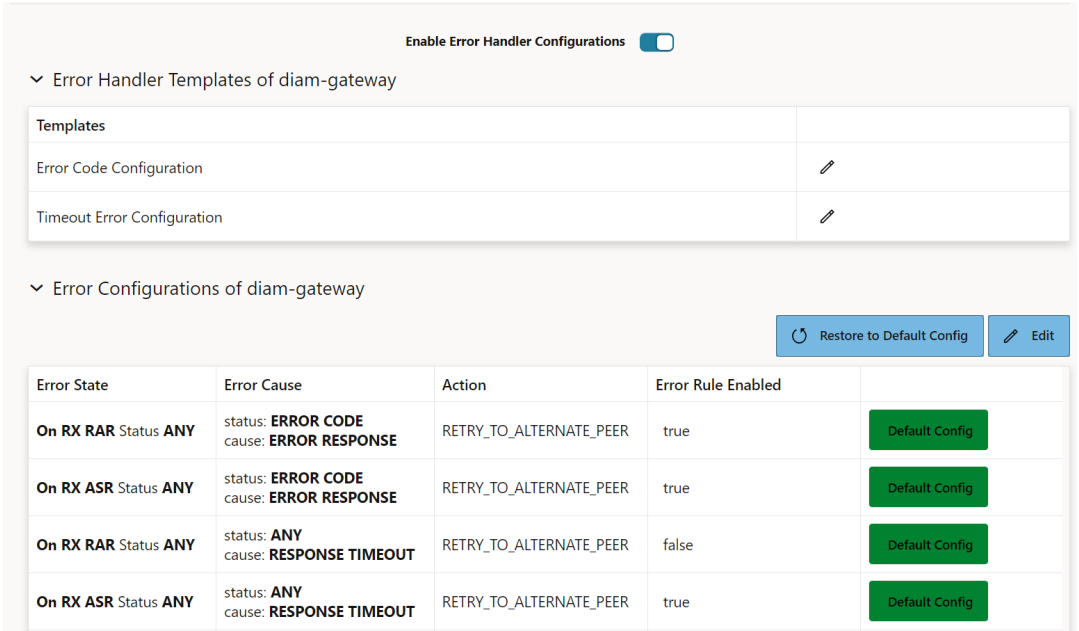
3. Enable the error handler configurations using the **Enable Error Handler Configurations** toggle button.
4. The **Error Handler Templates of diam-gateway** provides two options:
   - **Error Code Configuration**
   - **Timeout Error Configuration**

Figure 7-2 Error Handling Configuration UI



5. The **Error Configurations of diam-gateway** provides default error handling configurations to retry on all error codes (except diameter result code 2xxx) and timeout for Rx RAA and Rx ASA failed diameter messages.

Figure 7-3 Default Configurations



Copyright © 2019, 2026, Oracle and/or its affiliates.

6. To configure the **Error Code Configuration** in **Error Handler Templates of diam-gateway** , Click 

.
This opens the **Error Handler Template** editing page.
7. Enter values for the available input fields. The following table describes the fields:

Table 7-8 Create Error Code Configuration - Edit

Field Name	Description
On Rx	Specifies the list of diameter interfaces. The values are: • RAR • ASR Default value: RAR
Status	Specifies the error status to be provided by the user.

Table 7-9 Error Cause Configure

Field Name	Description
Error Cause Field	Specifies to search for which error causing field in the diameter answer message. Default value: ALL
Match Operator	Specifies the match operator to search error section in the diameter answer message. Default value: ANY
Message	Specifies the error message to search in the error section of diameter answer message. Default value: ANY
Status	Specifies the error status code to search in the error section in the diameter answer message. Default value: ANY
Cause	Specifies the field that matches the cause during error ends with 'not found'. User can choose from the following options: • ANY • RESPONSE_TIMEOUT Default value: ANY

Table 7-10 Action

Field Name	Description
Action	The action to be performed in the event of failed diameter message on Rx interface. User can choose from the following options: • RETRY TO ALTERNATE PEER • ONE RETRY TO ALTERNATE PEER
Error Originator	The peer from which the error origination occurs. User can choose from the following options: • ANY • INTERMEDIATE_PEER • DESTINATION PEER

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-4 Edit Error Code Configuration:

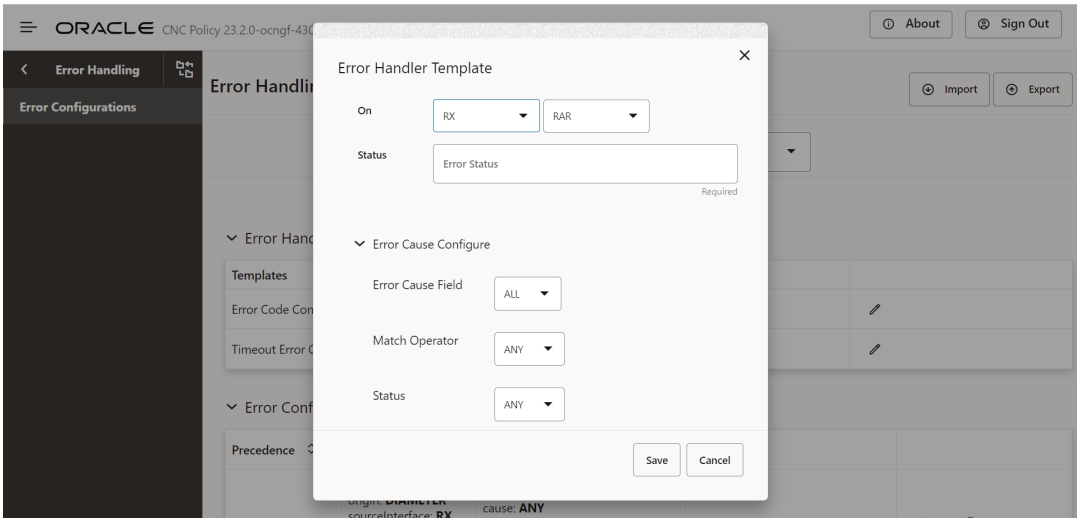
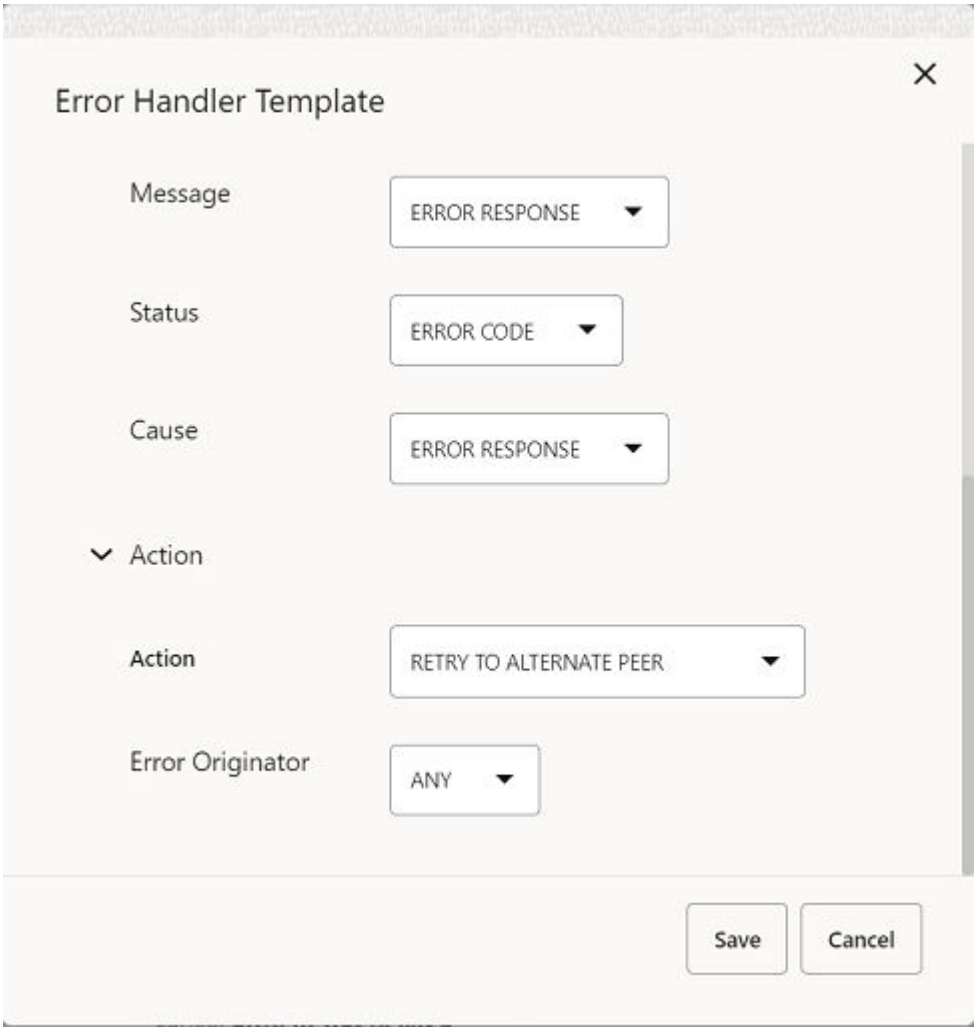


Figure 7-5 Edit Error Code Configuration continuation..



8. Click **Save** to save the changes or Click **Cancel** to discard the changes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

9. To configure **Timeout Error Configuration** in **Error Handler Templates of diam-gateway** , Click 

.
This opens the **Error Handler Template** editing page
10. Enter values for the available input fields. The following table describes the fields:

Table 7-11 Create Timeout Error Configuration

Field	Description
On RX	Specifies the list of diameter interfaces. Default value: RAR
Status	Specifies the error status to be provided by the user. Default value: ANY

Table 7-12 Error Cause Configure

Field	Description
Error Cause Field	Specifies to search for which error causing field in the diameter answer message. Default value: MESSAGE
Match Operator	Specifies the match operator to search error section in the diameter answer message. Default value: EQUALS
Message	Specifies the error message to search in the error section of diameter answer message. Default value: TIMEOUT_EXCEPTION
Status	Specifies the error status code to search in the error section in the diameter answer message. Default value: ANY
Cause	Specifies the field that matches the cause during error ends with 'not found'. Default value: ANY
Instance	Specifies the field that matches the instance during error contains the term 'Illegal'. Default value: ANY
resource	Specifies the resource to search in the error section of diameter answer message. Default value: ANY

Table 7-13 Action

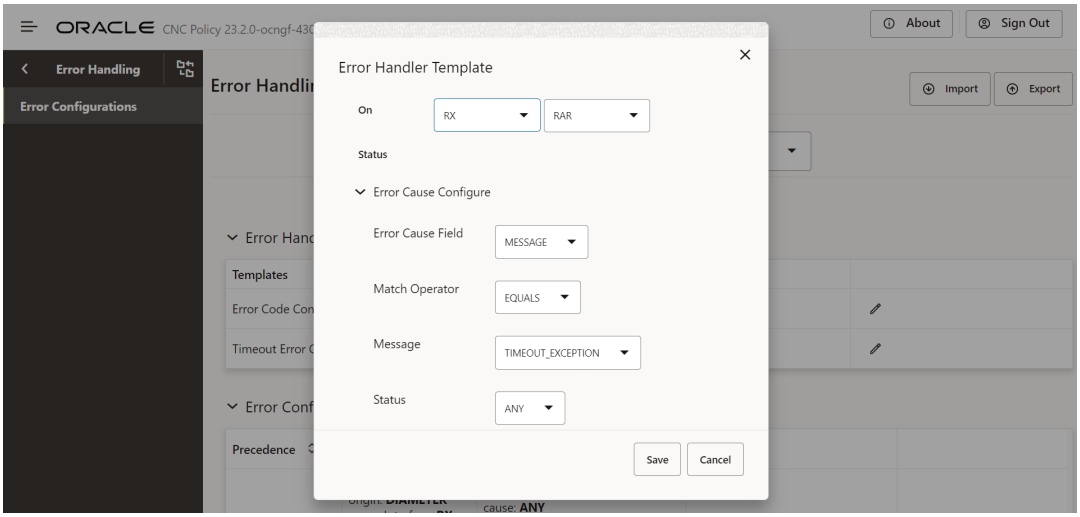
Field	Description
Action	The action to be performed in the event of response timeout on Rx interface. User can choose from the following options: • RETRY TO ALTERNATE PEER • ONE RETRY TO ALTERNATE PEER

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-13 (Cont.) Action

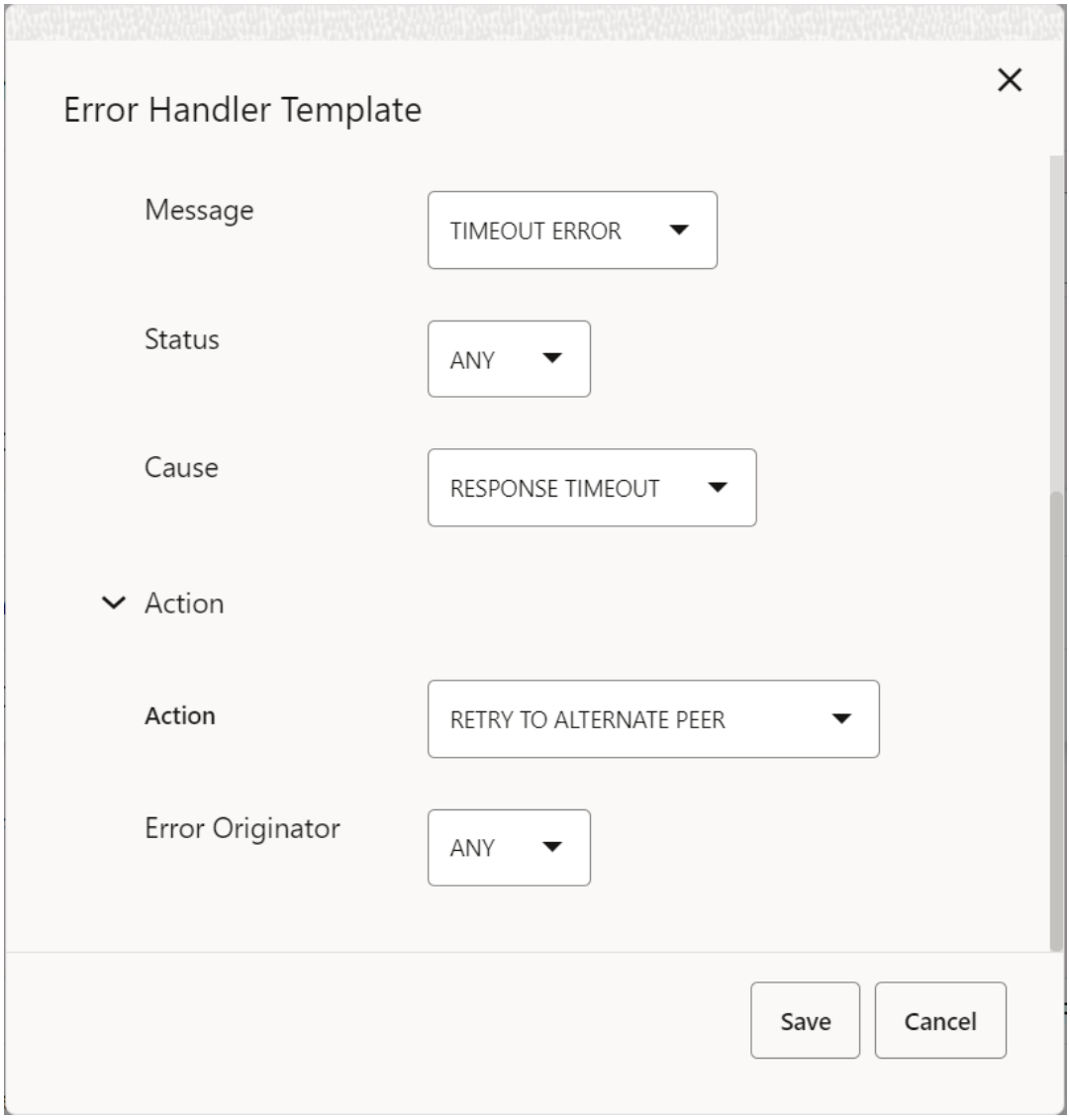
Field	Description
Error Originator	The peer from which the error origination occurs. User can choose from the following options: • ANY • INTERMEDIATE_PEER • DESTINATION PEER

Figure 7-6 Edit Timeout Error Configuration:



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-7 Edit Timeout Error Configuration Continuation:



11. Click **Save** to save the changes or Click **Cancel** to discard the changes.
Using the edit error handling configuration option, you can enable or disable the configurations.

The priority for each error handling configuration can be set using the

↑

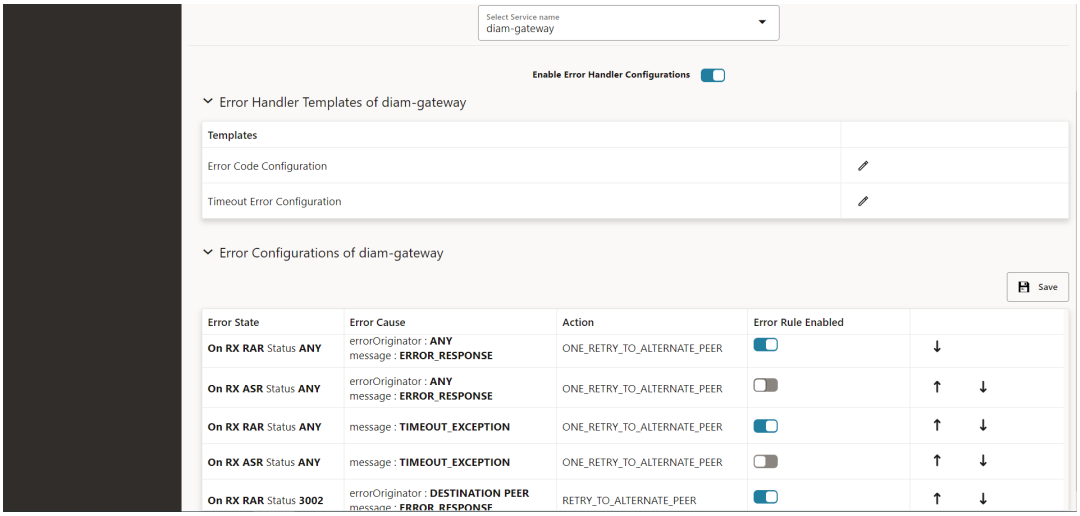
and

↓

arrow buttons.

Copyright © 2019, 2026, Oracle and/or its affiliates.

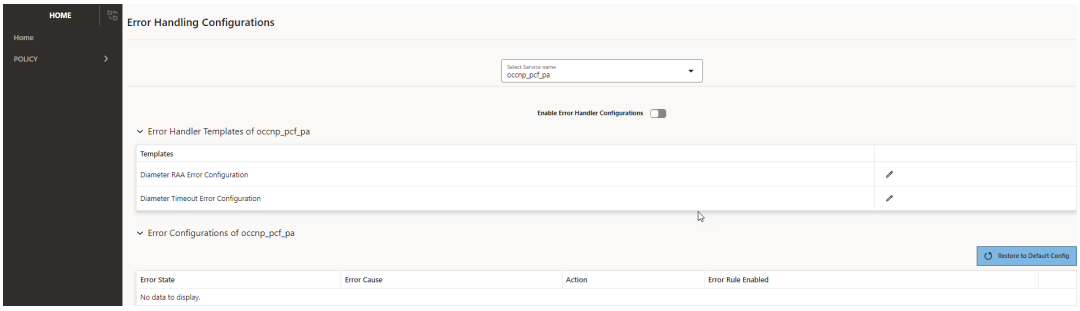
Figure 7-8 Error Handling User Saved Configuration with Priority:

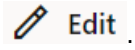


Error Configurations for PA Service

1. From the navigation menu, under **Policy**, click **Error Handling** and select **Error Configurations** page.
   This opens the **Error Handling Configurations** page.
2. From the `Select Service Name` drop-down list, select the value `occnp_pcf_pa`.
3. Enable the error handler configurations using the **Enable Error Handler Configurations** toggle button.
4. The **Error Handler Templates of occnp_pcf_pa** provide two options:
   - Diameter RAA Error Configuration
   - Diameter Timeout Error Configuration

Figure 7-9 Error Handling Configuration



5. To configure the **Diameter RAA Error**, Click 

   .
   This opens the **Error Handler Template** editing page for Diameter RAA Error.
   a. Enter values for the available input fields. The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-14 Diameter RAA Error Configuration

Field Name	Description
On Rx	Specifies the list of diameter interfaces. **Default Value**: RAR
Status	Specifies the diameter error result code to be provided by the user.

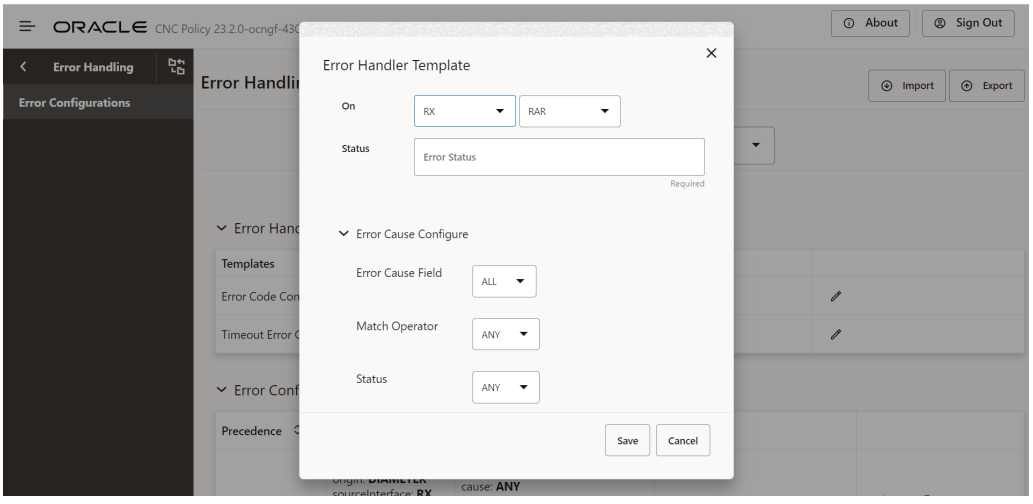
Table 7-15 Error Cause Configure

Field Name	Description
Error Cause Field	Specifies the error causing field in the diameter answer message. **Default Value**: Error Response Originator
Match Operator	Specifies the match operator to search error section in the diameter answer message. **Default Value**: EQUALS
Error Response Originator	Specifies the originator of the error response. **Default Value**: ANY

Table 7-16 Action

Field Name	Description
Action	Either terminate the ongoing transaction related to RAA or cleanup the Rx/N5 session. **Default Value**: Terminate Transaction

Figure 7-10 Diameter RAA Error Configuration:



b. Click **Save** to save the changes or Click **Cancel** to discard the changes.

6. To configure **Diameter Timeout Error Configuration**, Click Edit.
This opens the **Error Handler Template** page for Diameter Timeout Error Configuration.

a. Enter values for the available input fields. The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-17 Diameter Timeout Error Configuration

Field	Description
On RX	Specifies the list of diameter interfaces. **Default Value**: RAR
Status	Specifies the error status to be provided by the user. **Default Value**: NA

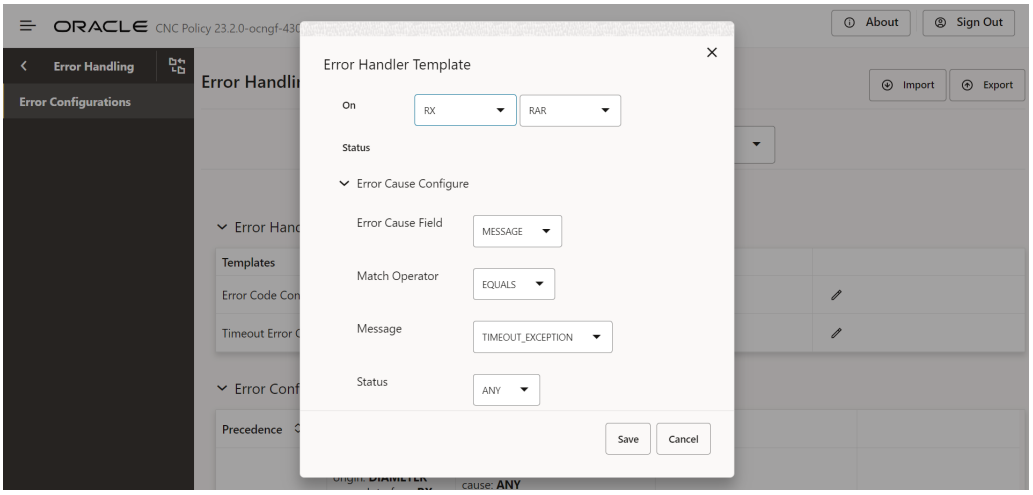
Table 7-18 Error Cause Configure

Field	Description
Error Cause Field	Specifies the error causing field in the diameter answer message. **Default Value**: MESSAGE
Match Operator	Specifies the match operator to search for error section in the diameter answer message. **Default value**: EQUALS
Message	Specifies the error message to search in the error section of diameter answer message. **Default value**: TIMEOUT_EXCEPTION

Table 7-19 Action

Field	Description
Action	Either terminate the ongoing transaction related to RAA or cleanup the Rx/N5 session. **Default value**: Terminate Transaction

Figure 7-11 Diameter Timeout Error Configuration:



b. Click **Save** to save the changes or Click **Cancel** to discard the changes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Error Configurations for AM, SM, UE, CHF Connector, UDR Connector, and Binding Services

1. From the navigation menu, under **Policy**, click **Error Handling**, and select **Error Configurations** page. This opens the **Error Handling Configurations** page.
2. From the **Select Service Name** drop-down list, select the required service.
3. Enable the error handler configurations using the **Enable Error Handler Configurations** toggle button.
4. The error handler template provides *Error Enhancement Configurations*.
5. To configure the *Error Enhancement Configurations* in Error Handler Templates of the required service, Click 

. This opens the **Error Handler Template** editing page.
6. Enter values for the available input fields. The following table describes the fields:

Table 7-20 Error Handler Template

Field	Description
On	Specifies the Application Error. Default value: Application Error

Table 7-21 Action

Field	Description
Action	Specifies the action to be performed in the event of failed message. Default value: Reject with Enhanced Detail
Exclude from error message	Specifies exclusion of the provided components from detail error message. By default, "Error State and "Problem Cause" are excluded.

7. Click **Save** to save the changes.

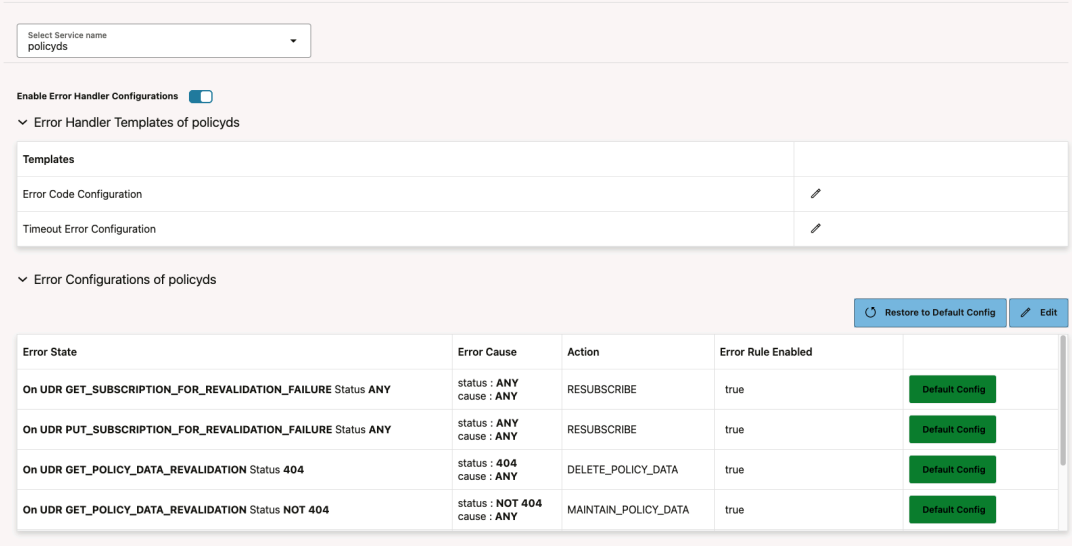
> **Note**
>
> Click **Cancel** to discard the changes.

Error Configurations for PDS Service

1. From the navigation menu, under **Policy**, click **Error Handling**, and select **Error Configurations** page. This opens the **Error Handling Configurations** page.
2. From the **Select Service Name** drop-down list select the value `policyds`. The page allows to add and edit error handling configurations for PDS.
3. Enable the error handler configurations using the **Enable Error Handler Configurations** toggle button.
4. When the **Enable Error Handler Configurations** button is enabled, it displays **Error Handler Templates of policyds** and **Error Configurations of policyds** subsections are displayed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

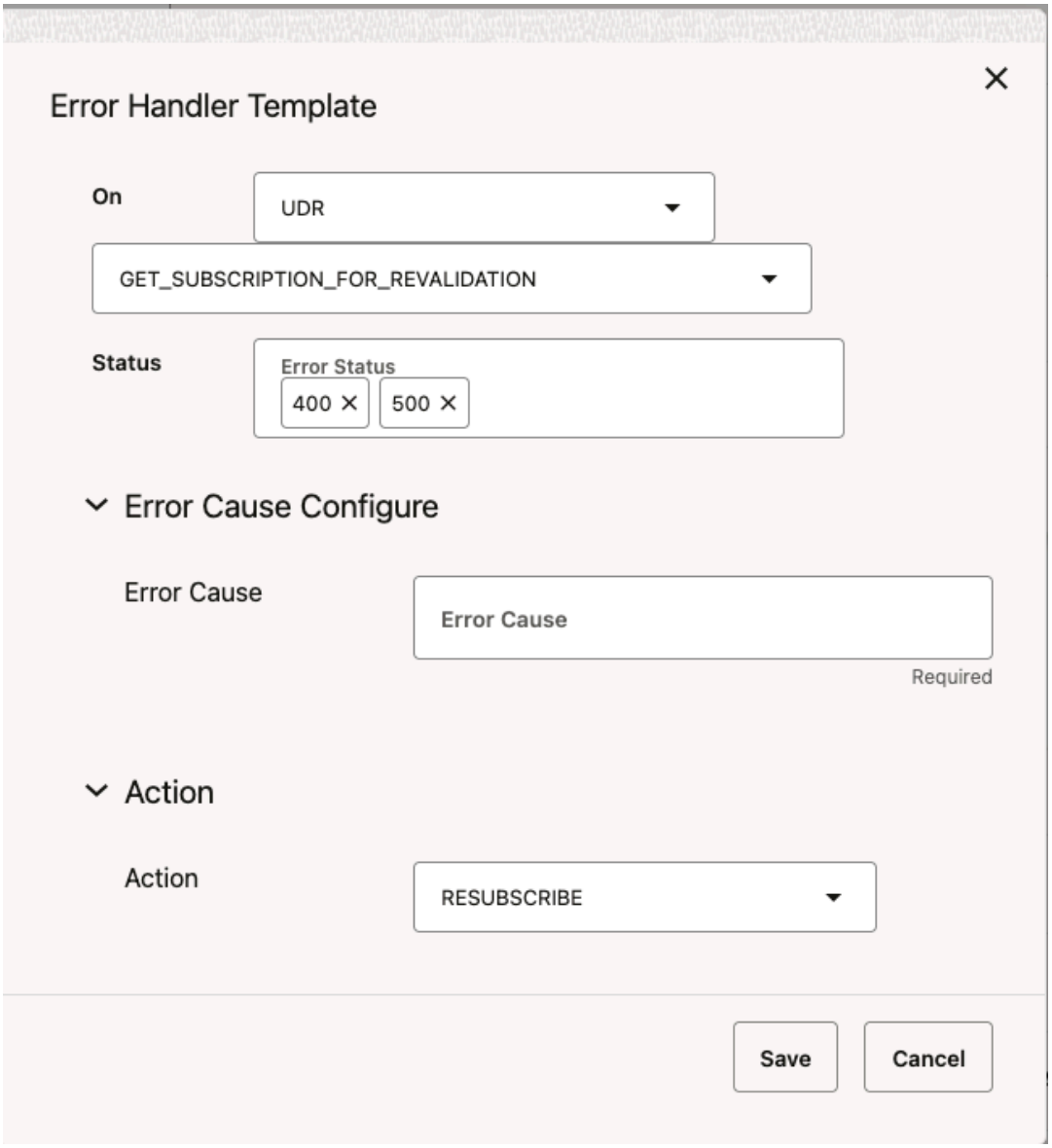
Figure 7-12 Error Handling Configuration



5. The **Error Handler Templates of policyds** provides two options:
   - **Error Code Configuration**
   - **Timeout Error Configuration**
6. The **Error Code Configuration** provides default error handling configurations to handle all the error codes for call flows when PDS interacts with UDR through UDR Connector using GET operation to revalidate the subscription. By default, the Error Code Configurations are enabled.
7. To configure the **Error Code Configuration** in **Error Handler Templates of policyds**, click Edit.
   This opens the **Error Handler Template** editing page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-13 Error Code Configuration Template



8. Enter values for the available input fields. The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-22 Error Code Configuration

Field Name	Description
On UDR	Lists the UDR subscription revalidation status for GET request from PDS. Possible values is: `GET_SUBSCRIPTION_FOR_REVALIDATION` **Note** Currently GET_SUBSCRIPTION_FOR_REVALIDATION is the only one supported to be configurable for PDS in Error Configuration with a Error Code / Cause / TimeOut.
Status	Specifies the error status code to search in the error section in the UDR subscription revalidation failure message. Possible value can be `ANY` or any error code between 400 and 599. Default value: ANY

Table 7-23 Error Cause Configure

Field Name	Description
Error Cause	Specifies the field that matches the cause during error ends with 'not found'. Possible value can be `ANY` or any other cause such as `NOT_FOUND` or `UNKNOWN_USER`. Default value: ANY

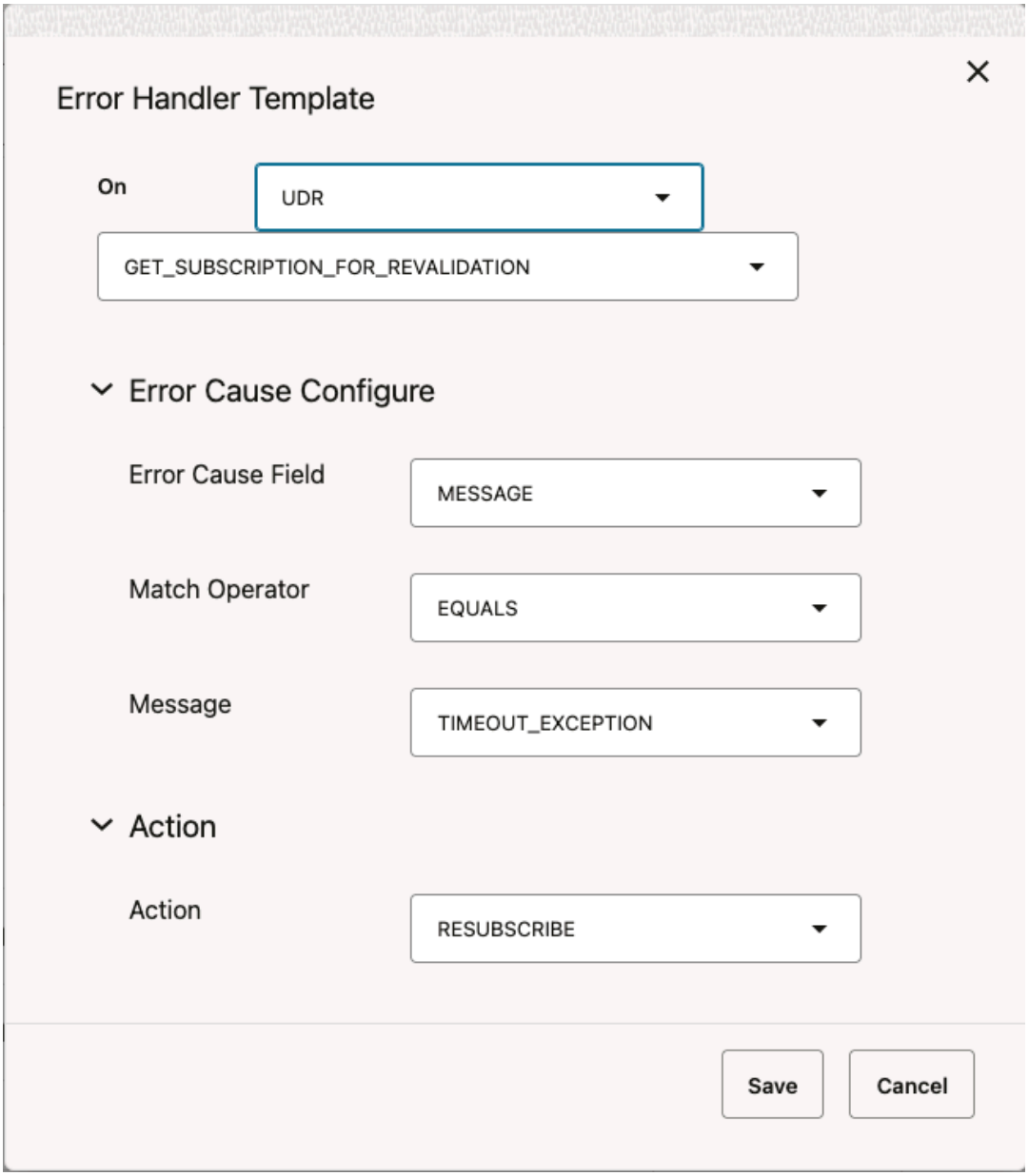
Table 7-24 Action

Field Name	Description
Action	The action to be performed in the event of failed UDR subscription revalidation failure message. Possible values are: RESUBSCRIBE: This action describes a subsequent POST operation when the previous operation (PUT / GET Subscription) failed to create a new resource in UDR, by removing the subscription information from the POST request towards UDR Connector to ensure a POST to create a new resource is sent to UDR.

9. Click **Save** to save the changes or Click **Cancel** to discard the changes.
10. To configure **Timeout Error Configuration** in **Error Handler Templates of policyds**, click Edit.
    This opens the **Error Handler Template** editing page

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-14 Configuration Error Handler Template for UDR - Subscription



11. Enter values for the available input fields. The following table describes the fields:

Table 7-25 Create Timeout Error Configuration

Field	Description
On UDR	Specifies the list of UDR subscription revalidation failure message. Default value: GET_SUBSCRIPTION_FOR_REVALIDATION

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-26 Error Cause Configure

Field Name	Description
Error Cause Field	Specifies to search for which error causing field the UDR subscription revalidation failure message. Default value: MESSAGE
Match Operator	Specifies the match operator to search error section in the UDR subscription revalidation failure message. Default value: EQUALS
Message	Specifies the error message to search in the error section of UDR subscription revalidation failure message. Default value: TIMEOUT_EXCEPTION

Table 7-27 Action

Field Name	Description
Action	The action to be performed in the event of failed UDR subscription revalidation failure message. Possible values are: • RESUBSCRIBE: This action describes a subsequent POST operation when the previous operation (PUT / GET Subscription) failed to create a new resource in UDR, by removing the subscription information from the POST request towards UDR Connector to ensure a POST to create a new resource is sent to UDR.

12. Click **Save** to save the changes or click **Cancel** to discard the changes.

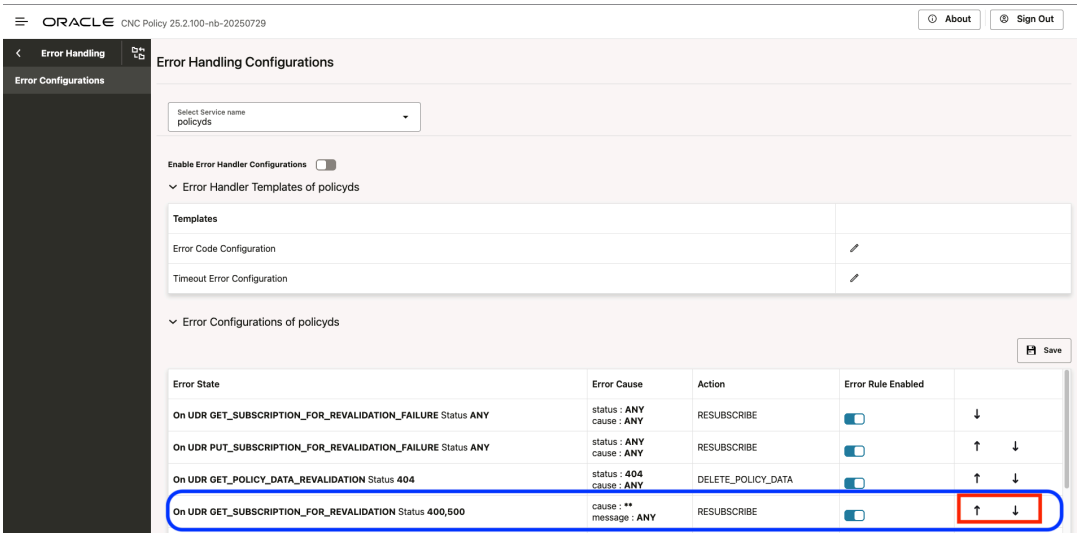
Editing the Default or Custom Rules - Priority

1. Click the 

button in **Error Configurations of policyds** section.
2. The **Error configurations of policyds** section displays a set of arrows that allow to change the priority of the rule.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-15 Changing priority of the rule



3. The top rules have higher priority than the ones from the bottom. That is, the top rules or the higher priority ones are evaluated before the ones with lower priority. The priority rules come into picture only when there are more than one rules of the same Error State. Priority is applied to rules with **GET_SUBSCRIPTION_FOR_REVALIDATION_FAILURE** and the rest of the rules are not affected.

> **Note**
>
> In order to be more precise with the rule, it is recommended to disable the default rule for **On UDR GET_SUBSCRIPTION_FOR_REVALIDATION_FAILURE** with Status **ANY**, so that those errors that do not need resubscription can complete the transaction there.

7.3 Service Configurations

This section describes how to customize the Policy services according to the network requirements using the **Service Configuration** pages. The configurations include setting up end point addresses, setting up log levels, log level tracing, customizing and optimizing NF interactions, such as with UDR and so on.

> **Note**
>
> The advanced settings keys should have a unique value without any duplicates. For example, CONCURRENCY.BULWARK_ENABLED_FOR_CHF_NOTIFICATION settings for PDS should have a single key with value either true or false. There should not be two keys for CONCURRENCY.BULWARK_ENABLED_FOR_CHF_NOTIFICATION, each of them holding different values.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.1 Common Data

This section includes the common data configurations for Policy services.

To access Common Data functionality from the CNC Console home page, expand **Policy**, navigate to **Service Configurations** and select **Common Data**.

On clicking **Common Data**, you can perform the following operations:

- Reattempts Profile
- Retry Profiles
- Timer Profiles
- Site Takeover
- NF Communication Profiles
- Attribute Forwarding Profiles
- Rx Reauth Profiles
- Message Profiles
- Default Processing Profiles
- Service Profiles
- Message Attributes

7.3.1.1 Reattempts Profile

This procedure provides information about how to create and manage the reattempts profiles for the binding registration, UE NAS operations along with AMF Discovery.

The **Reattempts Profile** page allows you to create new and manage existing reattempt profiles. The page displays the list of defined reattempt profiles with the options to import, export, or add profiles.

To configure reattempt profile:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **Common Data**, and then select **Reattempts Profile**.
   This opens the **Reattempts Profile** page. The page lists the existing reattempt profiles. You can add or import new profiles using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Reattempts Profile** page.
3. On the **Create Reattempts Profile** page, enter the following information:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-28 Create Reattempts Profile

Field Name	Description
Name	The unique name for the reattempt profile. This name is used to refer to the reattempt profile in other service configuration screen, such as SM Service. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Interface Type	The interface type for which a reattempt profile is being created. You can choose from: • BSF • AMF • NRF Select **BSF** to reattempt PCF binding request. Select **NRF** to reattempt AMF discovery request. Select **AMF** to reattempt N1N2 Subscribe, N1N2 Transfer, N1N2 Failure Notification requests. **Default value**: BSF
Re-attempt Settings	Provide the Re-attempt settings details:
Maximum Number of Attempts	To configure maximum number of reattempts that are allowed for a service operation. On selecting **BSF** interface type, it is the number of reattempts that must be run when PCF Binding request fails. It takes a range between 0 - 50. On selecting **NRF** interface type, it is the number of reattempts that must be run when AMF discovery request fails. It takes a range between 0 - 100. On selecting **AMF** interface type, it is the number of reattempt that must be run when N1N2 Subscribe, N1N2 Transfer, N1N2 Failure Notification requests fails. It takes a range between 0 - 100.
Back-off timer configurations	The amount of time that represents each back-off timer. Click Add to configure **Back-off timer configurations** in the table and configure the following parameters: • **Index:** Represents the number of back-off timer • **Back-Off Timer (Seconds):** Configure back-off timer for every reattempt request in seconds. This is a numerical value in the range of 20 to 2678400 seconds. **Note**: Recommendation for `UE Policy` delivery back-off timer creation is to use a value greater than or equal to 60. • **Max Random Number (Millisecond):** Configure any random number in milliseconds that is added to the back-off timer. This is a numerical value, which can be in the range of 1-5000 milliseconds. If this is not configured then the back-off timer is considered without an random value. **Note:** In case the number of configured attempts in the Back-off timer configurations table is less than the set value for **Maximum Number of Attempts**, the remaining attempts uses the back off timer and max random number of the last configured attempt. **Note:** Policy supports a maximum of 20 back-off timer configurations and if more of it is added then an error will be displayed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-28 (Cont.) Create Reattempts Profile

Field Name	Description
Threshold Limit Level	**BSF** - Configure the threshold limit for the Pending Operations. Once this value is reached, no pending operations are added to the table. This is a numerical value in the range of 0 - 1000. For information about pending operation configurations, see PCF Session Management. **Default Value:** 1000 for BSF interface type. **AMF/NRF** - To configure the threshold limit for timers that can be backed off for reattempt. Once threshold limit is reached, PCF shall not allow to add more requests in the queue for reattempt. This is confined to maximum of 360K combined for all NF operations. This is a numerical value in the range of 0 - 360000. **Default Value:** 200000 for NRF/AMF interface type.
Re-attempt Error Code Settings	Provide Re-attempt Error Code settings details:

Enable Reattempt On Internal Failure	This flag determines whether to perform reattempt in occurrence of internal failures.
	If flag is **true**, then
	• Reattempts are allowed for any internal failure, and not just service timeouts.
	• The internal failure signifies timeout exceptions, and also exceptions which results in no response from AMF.
	• The decision is based on the *current* error result, not from the last one.
	• If session retry is enabled and multiple routes are available, even a timeout on the last route will be considered for a reattempt.
	If flag is **false**, then
	• Reattempts depend on the *previous* route error if the last route timed out.
	• Timeout on the last route alone will not trigger a reattempt.
	Default value: true

Re-attempt for Following Error Codes	Configure the list of combination of HTTP error code and cause for reattempt with back off. A maximum of 32 combinations of error code and cause can be provided. Click Add to configure **Re-attempt for Following Error Codes** table and configure the following parameters • **Error Code**: Provide the HTTP error code for which the reattempt is applicable. It is a number and can range from 100-999. • **Error Cause**: Provide the cause for an error code so that reattempt is made only for the matching causes of the error code. The **Error Cause** value should be in upper case. Use only underscore '_' between words, and do not use space. **Note**: • If the error code or error cause is not configured then reattempts is not applicable for any errors. • If the error code is configured without error cause, then reattempt is applicable for any cause of the configured error code. • If both the error code, and its cause is configured, but error cause is not received, then PCF reattempts based on configured error code
Rate Limiting Settings	Provide Rate Limiting settings details:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-28 (Cont.) Create Reattempts Profile

Field Name	Description
Rate Limit (per second)	Configure the rate limit threshold per second for NF service operation(s). This value can be in the range between 0 - 700. Default value: 100 **Note**: It is recommended to keep this value above or equal to 100 requests per second. The timer expiry notification rate should be more than the allowed timer creation time so as to prevent the creation of backlogs which will cause a delay in timer expiry notification reaching the UE service.

4. Click **Save**.
   The reattempt profile gets listed on the **Reattempt Profile** page. The page defines the reattempt profile in the Policy database and it is available to be used in a Policy.

> **Note**
>
> Use or available under the **Actions** column to update or delete the reattempt profile.

Importing Reattempt Profiles

To import Reattempt Profile:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.1.2 Retry Profiles

This procedure provides information about how to create and manage retry profiles.

The **Retry Profile** page allows you to create new and manage existing retry profiles. The page displays the list of defined retry profiles with the options to import, export, or add profiles.

To configure retry profile:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **Common Data**, and then select **Retry Profiles**.
   This opens the **Retry Profiles** page. The page lists the existing retry profiles. You can add or import new retry profile using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Retry Profile** page.
3. On the **Create Retry Profile** page, enter the following information:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 Create Retry Profile

Field Name	Description
Name	The unique name for the retry profile. This name is used to refer to the retry profile in other service configuration screen, such as SM Service, User Connector and so on. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Retry on Internal Send Failure	Specifies whether to enable or disable retry for failed messages between core microservices of Policy. On enabling this switch, ensure that you configure the parameters under **Retry Settings** group. However, if the switch is disabled, the configurations in the Retry Settings group are not taken into consideration. When enabled, retries are attempted when PCF encounters internal send failures for egress messages. A failure to send egress messages internally indicates an exception in the core service, such as SM service, UDR or CHF connector, and so on. The exception can occur while connecting to the next microservice or a failure on the microservice itself. For example, egress message did not reach the egress gateway. This also includes the connection errors and timeouts on the core microservice. **Note**: Since the failure is internal, the external NF and SCP (if applicable) remain the same during retry attempt.
Enable Alternate Routing	Specifies whether to enable or disable alternate routing. On enabling this switch, ensure that you configure the parameters under the Alternate Routing Settings group. When enabled, alternate routing is attempted when the Policy messages are not delivered successfully to an external NF destination. It may happen because of an exception on the Egress Gateway, such as connection error, timeout, or a failure returned by the external NF or an intermediate router.
Server Header Support	Specifies whether to enable or disable server header. The value configured in this parameter is used when PCF acts as a consumer and receives server header in error response messages. Depending on the requirements, you can select any of the following values from the drop-down list: • Disabled (**default**) - Select this option to disable server header. On disabling server header, Policy as a consumer searches for alternate producer without considering the value of server header. • Single Instance - Select this option to accept only one value in the server header. When the value is configured as Single Instance and server header contains multiple values, Policy rejects the header. • Multi Instance - Select this option to accept multiple values in the server header.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 (Cont.) Create Retry Profile

Field Name	Description
Pattern To Ignore Server Header Value	Specifies the pattern to ignore server header values. **Note** This field appears only when *single Instance* or *Multi Instance* is selected from the drop-down of the *Server Header Support* field.
Ignore Custom server header value	This field appears on selection of either "Single Instance" or "Multi Instance" value for the field **Server Header Support**. In this field you can specify the string pattern that can be ignored in the server header value. This is provided in the form of regular expression. The regular expression evaluates the server header content to ignore the strings that match the pattern specified the regular expression.
Retry Settings	Provide Retry Settings details:
Maximum Number Of Retries	Specifies the number of retries that PCF attempts on encountering failure while sending egress messages from Policy core microservices. **Note**: The value configured for this parameter does not include the initial attempt. For instance, if you set the value as 3, Policy performs the retry cycle three times after the initial attempt.
Alternate Routing Settings	Provide Alternate Routing Settings details:
Maximum Number Of Alternate Routing Attempts	Specifies the number of retries that PCF attempts on receiving error response from Egress Gateway. The number of retry attempts can be in the range of 1 to 10. **Note**: The value configured for this parameter does not include the initial attempt. For instance, if you set the value as 3, Policy performs the retry cycle three times after the initial attempt. If the retry attempts are exhausted, CNC Policy fails the transaction with an exception. In certain cases, the number of retry attempts can be greater than the available alternate destinations to be tried. If such a situation arises, Policy fails the transaction when no alternate destination is available even if retry attempts are still available.
Attempt Alternate Route for Following Error Codes	Allows to configure the HTTP error codes for which Policy reattempts the requests after the ARR request failures. **Note**: In Policy 22.1.0, Error Causes does not work for Notify Flows. Users are recommended to leave it blank. To add a value, click **Add** and enter values for the following fields: • **Error Code** - Specifies the HTTP error code. For example, 504 • **Error Causes** - Specifies the error cause. For example, GATEWAY_TIMEOUT, NF_TIMEOUT. You can configure up to 32 error codes with each error code supporting up to five causes. **Note**: The Error Causes and Error Code are unique. In case you import them from earlier version containing duplicate values, it will pick only one value.
Priority Pool	Specifies whether to enable or disable the load sharing between different NFs.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 (Cont.) Create Retry Profile

Field Name	Description
Use Alternate SCP for Alternate Routing	Specifies whether to enable or disable choosing alternate SCP to reach the alternate destination. If you set the value for this parameter as true, Egress Gateway uses an alternate SCP for routing to an alternate NF destination. If there are fewer SCPs than alternate NF destinations, Egress Gateway tries sending the request through one of the previously used SCPs. **Note**: Additional SCP configuration is required for egress gateway. For more information, see Oracle Communications Cloud Native Core Policy Installation and Upgrade Guide.
Use Binding Information from Binding Header	Specifies whether to enable or disable the use of information received in 3gpp-sbi-binding header. When Policy receives the unique NF Instance ID in the error response, it retrieves the 3gpp-sbi-binding header for that particular NF instance. It extracts the `SetId` to choose the alternate producer. This parameter is considered only for subsequent retry requests. By default, this switch is disabled. **Note**: When this switch is enabled, the value of NFSet Preference is not taken into consideration.
Use Binding Information from NF Profile	Specifies whether to enable or disable the use of information from the set NF Profile. When Policy receives the unique NF Instance ID in the error response, and it does not receive information from the 3gpp-sbi-binding header for that particular NF instance, it extracts the `SetId` to choose the alternate producer. This parameter is considered only for subsequent retry requests. By default, this switch is disabled. **Note**: For subsequent requests, this field takes precedence only if the **Use Binding Information from Binding Header** flag is disabled or no NF binding is received in the initial request.
NF Set Resolution	Specifies whether to enable the on demand discovery of subsequent messages based on the NFSet ID, in case of failure response. The possible values are: • **NRF Discovery:** If this value is selected, then PCF sends a request to NRF to get the list of NFs based on the `SetId` value from the *3gpp-Sbi-Binding header* of the NF with a successful Initial Request. • **Cached NF Profiles:** If this value is selected, then PCF selects the list of NFs from the already discovered NF list. By default **Cached NF Profiles** remains selected. **Note**: CHF or BSF doesn't support on-demand NRF discovery, only UDR supports on-demand NRF discovery. So, while creating retry profile for CHF or BSF, you should select **Cached NF Profiles** option. **Note**: NRF discovery is applicable for subsequent messages functionality only. For the other retry requests, the NF list is provided through the cached NF profiles. If the **Cached NF Profiles** option is selected for the subsequent messages, then it uses the DNS-SRV configuration for session retry.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 (Cont.) Create Retry Profile

Field Name	Description
NF Set Preference	Specifies the NF set preference when choosing the alternate producer for an initial request. Policy excludes the producer (received in the failed request) and selects an alternate producer based on the value you choose from the drop-down menu: • Same: Choose the next producer from the same NFSet as the previous request. • Different: Choose the next producer from a different NFSet. • None **(default)**: NFSets filter does not apply. **Note**: This parameter applies only to initial requests. For subsequent requests, the default behavior is to choose the same NFSet provided by Sbi-Binding Info (if enabled). Otherwise, it goes to the same NFSet as the current NF. In case the current NF does not belong to any NFSet or NFSet is missing, it falls back to DNS-SRV.
Locality Preference	Specifies the locality preference when choosing the alternate producer for a failed request. Policy excludes the producer (received in the failed request) and selects an alternate producer based on the value you choose from the drop-down menu: • Same: Choose the next producer from the same locality as the previous request. • Different: Choose the next producer from a different locality. • None **(default)**: Locality filter does not apply.
Re-attempt to Same NF	Specifies whether Policy shall send the request to the same NF that failed in the first attempt. If you enable this switch, Policy allows re-attempting to the same NF based on the following conditions: • If the server header in error-response has SCP host alone, Policy does not consider error code and error cause, and retries to the same NF. • If the server header in error-response has instances with or without SCP or envoy, Policy checks error code and error cause to find out if retry to same NF is allowed. By default, this switch is disabled. **Note**: Make sure to configure the value for **Re-attempt same NF for following Error Codes** field.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 (Cont.) Create Retry Profile

Field Name	Description
Re-attempt Same NF for following Error Codes	Specifies the HTTP error codes for which Policy does not look for alternate producer and retries the request to the same NF or SCP that failed in the first attempt. To add a value, click **Add** and enter values for the following fields: • **Error Code** - Specifies the HTTP error code. For example, 504 • **Error Causes** - Specifies the error cause. For example, GATEWAY_TIMEOUT, NF_TIMEOUT. You can configure up to 10 error codes with each error code supporting up to five causes. When the field is left empty (default), Policy does not send the request to the NF that failed in the first attempt. **NOTE:** Policy considers this parameter only when **Re-attempt to same NF** switch is enabled. **Note:** It is mandatory for all error codes and their corresponding causes listed under the **Re-attempt Same NF for Following Error Codes** field to also appear in the **Attempt Alternate Route for Following Error Codes** section. As an alternative, you can leave the 'Error Cause' field blank in the **Attempt Alternate Route for Following Error Codes** section, indicating that all error causes associated with a specific error code in the **Re-attempt to Same NF** section will be applicable.
Enable DNS Resolution	Specifies whether to enable or disable falling back to DNS resolution. When this flag is enabled, during subsequent requests, after the application of filters and flags if no alternate NFs are found, Policy falls back to DNS resolution (DNS SRV). By default, this flag is disabled. **Note**: **Enable FallBack to Higher Priority Destination** and **Retry After Interval** fields are considered only if **Enable DNS Resolution** field is enabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 (Cont.) Create Retry Profile

Field Name	Description

Enable Fallback to Higher Priority Destination	Specifies whether to enable or disable falling back to the higher priority destination that failed earlier (after the retry interval). Policy attempts fallback even if the current destination is available.
	When you enable this switch, Policy attempts to fallback to a higher priority NF destination. The priority of NF destination is determined by Alternate Route service (either via DNS-SRV resolution or by static configuration).
	Default Value: False
	The following example illustrates a scenario when Fallback is enabled and **Retry After Interval** is set to 900 seconds:
	`NRF returned profiles - UDR1 (priority-1), UDR2 (priority-2), UDR3 (priority-3),`
	`Alternate Route configuration for UDR1 - UDR1 (priority-1), UDR1.2 (priority-2), UDR1.3 (priority-3),`
	`Retry After Interval - 900 seconds, Fallback is enabled`
	`9:00 AM PCF receives an SM Create request and establishes a session with UDR1`
	`9:05 AM PCF receives an SM Modify request and routes to UDR1, UDR1 fails, PCF reroutes to UDR1.2`
	`9:10 AM PCF receives an SM Modify request and routes to UDR1.2`
	`9:20 AM PCF receives an SM Modify request and routes to UDR1 (fallback)`
	Note: This configuration applies to subsequent message routing only.
	Priority pool must be enabled to use **Enable FallBack to Higher Priority Destination**.
	For multi-pod deployments where subsequent requests for a subscriber can be distributed across different pods, the fallback to higher priority destination will be effective only when there is sufficient traffic. The messages are distributed to all the pods such that they build up respective cache with failed destination info along with failed time stamp. If this cache is not present on a particular pod, the fallback to higher priority will not happen.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 (Cont.) Create Retry Profile

Field Name	Description

Retry After Interval (in seconds)	Specifies the time in seconds after which Policy re-attempts a request to a higher priority destination.
	In case of fallback, when a route is being determined while the current destination has not failed, PCF attempts to fallback to a higher priority NF destination. Priority of NF destination is determined by Alternate Route service, either through DNS-SRV resolution or static configuration.
	You can set the value for retry after interval from 0 to 86,400 seconds.
	By default, the value is set to 0, which means that a high priority destination is blocklisted.
	Note:
	• This configuration applies to subsequent message routing only.
	• Blacklisting may still be done by Egress Gateway
	• An NF destination (FQDN) is not re-attempted within the context of a single operation, such as SM Modification request
	
	`NRF returned profiles - UDR1 (priority-1), UDR2 (priority-2), UDR3 (priority-3),`
	`Alternate Route configuration for UDR1 - UDR1 (priority-1), UDR1.2 (priority-2), UDR1.3 (priority-3), UDR1.4 (priority-4)`
	`Retry After Interval - 900 seconds, Fallback is disabled`
	
	`9:00 AM PCF receives an SM Create request and establishes a session with UDR1`
	`9:05 AM PCF receives an SM Modify request and routes to UDR1, UDR1 fails, PCF reroutes to UDR1.2`
	`9:10 AM PCF receives an SM Modify request and routes to UDR1.2`
	`9:12 AM PCF receives an SM Modify request and routes to UDR1.2, UDR1.2 fails, PCF reroutes to UDR1.3`
	`9:16 AM PCF receives an SM Modify request and routes to UDR1.3 (no fallback)`
	`9:20 AM PCF receives an SM Modify request and routes to UDR1.3, UDR1.3 fails, PCF alternate routes to UDR1 (not UDR1.4)`

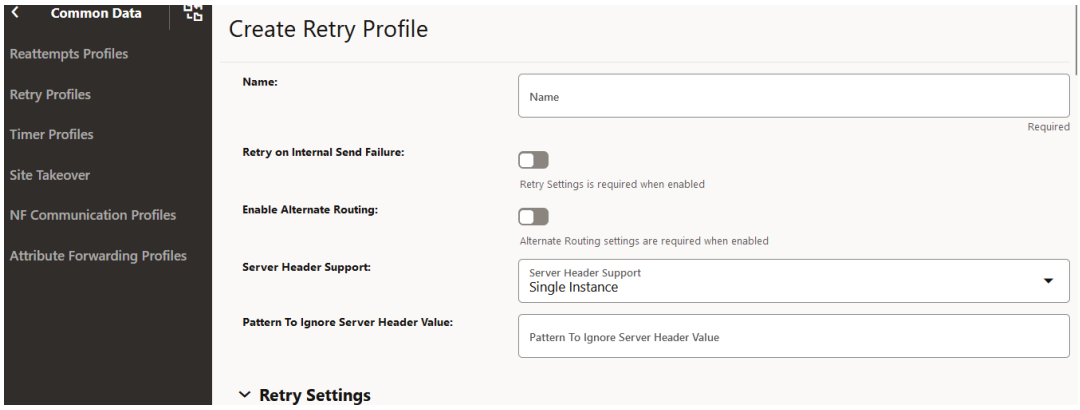
Retry again at end of alternate NF options	When you set the value for this parameter to true, Policy initiates the retry cycle and sends request to the selected NF when the following conditions are true: • Retry attempts made to all available NF instances • Maximum Number of Alternate Routing Attempt is not exhausted
Retry After Settings	

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-29 (Cont.) Create Retry Profile

Field Name	Description
Enable Retry-After IE:	This parameter enables or disables deferring an N1N2Transfer message for the retryAfter IE value received from AMF. The supported retryAfter IE range is 1 to 600 seconds. **Note**:This parameter applies only to the retryAfter IE received from AMF over the N1N2 interface; it does not apply to the HTTP Retry-After header or other service interfaces.

Figure 7-16 Create Retry Profile



4. Click **Save**.
   The retry profile gets listed on the **Retry Profile** page. The page defines the retry profile in the Policy database and it is available to be used in a Policy.

> **Note**
>
> Use or available under the **Actions** column to update or delete the retry profile.

Importing Retry Profiles

To import Retry Profile:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.1.3 Timer Profiles

This procedure provides information about how to create and manage timer profiles.

The **Timer Profile** page allows you to create new and manage existing timer profiles. The page displays the list of defined timer profiles with the options to import, export, or add profiles.

To configure timer profile:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **Common Data**, and then select **Timer Profiles**.
   This opens the **Timer Profiles** page. The page lists the existing timer profiles. You can add or import new profiles using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Timer Profile** page.
3. Select any of the following services from the **Service Type** drop-down list and perform the required configurations.
   - **PCF User Connector**
     To configure the timer profile for PCF User Connector:
     a. Enter the timeout value for **UDR**:
        Timeout Per Service.nudr-dr (in milliseconds): Specifies the maximum time for the response from the nudr-dr service. The messages can be of the following types:
        - Query
        - Subscribe
        - Unsubscribe
        - Update
        - Subscribe with Immediate Report

        > **Note**
        >
        > You can enter timeout for specific messages.

     b. Enter the timeout values for **CHF**:
        Timeout Per Service.nchf-spendinglimitcontrol (in milliseconds): Specifies the maximum time for the response from the nchf-spendinglimitcontrol service.
   - **PCF Session Management**
     To configure the timer profile for PCF Session Management:
     a. Enter the timeout values for **SMF**:
        Timeout Per Service.notification (in milliseconds): Specifies the maximum time for the response from the notification service.
     b. Enter the timeout values for **AF**:
        Timeout Per Service.notification (in milliseconds): Specifies the maximum time for the response from the notification service.
   - **PCF Access and Mobility**
     To configure the timer profile for AMF:
     a. Enter the timeout values for **AMF**:
        Timeout Per Service.notification (in milliseconds): Specifies the maximum time for the response from the notification service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **PCF UE Policy**
  To configure the timer profile for PCF UE Policy:
  a. Enter the timeout values for **AMF**:
     Timeout Per Service.namf-comm (in milliseconds): Specifies the maximum time for the response from the namf-comm service.

     Timeout Per Service.notification (Non N1N2 messages. In milliseconds): Specifies the maximum time for the response from the notification service. This will be used only if its value is less than the 3gpp-max-response-time header value.
- **PCF Binding Service**
  To configure the timer profile for Binding Service
  a. Enter the timeout values for **BSF**:
     Timeout Per Service.nbsf-management (in milliseconds): Specifies the maximum time for the response from the BSF service.

4. Click **Save**.
   The timer profile gets listed on the **Timer Profile** page. The page defines the timer profile in the Policy database and it is available to be used in a Policy.

> **Note**
>
> Use or available under the **Actions** column to update or delete the timer profile.

Importing Timer Profiles

To import Timer Profile:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.1.4 Site Takeover

This procedure provides information about how to create and manage the sites for takeovers in case of failure scenarios.

The **Site Takeover** page allows you to create new and manage existing sites for takeover. The page displays the list of defined sites with the options to import, export, or add profiles.

To configure site:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **Common Data**, and then select **Site Takeover**.
   This opens the **Site Takeover** page. The page lists the existing sites. You can add or import new profiles using this page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Site Takeover** page.
3. On the **Create Site Takeover** page, enter the following information:

Table 7-30 Create Site Takeover

Field Name	Description
Name	The unique name for the site. This name is used to refer to the site in other service configuration screen, such as SM Service. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Site ID	The site ID for which the current site takes control of the pending binding records in case of binding registration failures.

4. Click **Save**.
   The site gets listed on the **Site Takeover** page. The page defines the site in the Policy database and it is available to be used in a Policy.

> **Note**
>
> Use or available under the **Actions** column to update or delete the site.

Importing Site Takeover

To import site:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.1.5 NF Communication Profiles

The **NF Communication Profiles** page allows you to create new and manage existing NF communication profiles. The page displays the list of defined profiles with the options to import, export, or add profiles.

To configure NF communications profile, perform the following steps:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **Common Data**, and then select **NF Communication Profiles**.
   This opens the **NF Communication Profiles** page. The page lists the existing profiles. You can add or import new profiles using this page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create NF Communication Profile** page.
3. On the **Create NF Communication Profile** page, enter the following information:

Table 7-31 Create NF Communication Profile

Field Name	Description
NF Communication Profile Name	The unique name for the NF communication profile. This name is used to refer to the profile in other service configuration screen, such as SM Service, User Connector, and so on. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Policy NF Communication Model	Indicates the communication model as defined in 3GPP Technical Specification 23.501 Annexure E, in which the Policy NF is deployed. Select any of the following values from the drop down menu: • **Custom**: Select this option to create a customized communication profile. • **Model B**: Direct communication with NRF interaction. In this model, consumers perform discovery by querying the NRF. Based on the discovery result, the consumer does the selection and sends request to the selected producer. Selecting this option configures the communication profile according to Model B and populates data for the respective input fields. • **Model C**: Indirect communication without delegated discovery. In this model, consumers perform discovery by querying the NRF. Based on the discovery result, the consumer does the selection of an NF set or a specific NF instance of the NF set. The consumer sends the request to the SCP containing the address of the selected service producer pointing to a NF service instance or a set of NF service instances. In the latter case, the SCP selects an NF Service instance. If possible, the SCP interacts with NRF to get selection parameters such as location and capacity. The SCP routes the request to the selected NF service producer instance. Selecting this option configures the communication profile according to Model C and populates data for the respective input fields. • **Model D**: Indirect communication with delegated discovery to SCP. In this model, consumers such as PCF add discovery parameters and delegate the discovery of the producer to SCP. The delegated discovery applies to both on-demand and autonomous discovery scenarios. Selecting this option configures the communication profile according to Model D and populates data for the respective input fields. **Default Value**: Custom
NF Discovery Settings	Provide NF Discovery Settings details:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-31 (Cont.) Create NF Communication Profile

Field Name	Description
Initial Discovery Parameters	Indicates the discovery parameter to be used in the *3gpp-sbi-discovery-<discovery-parameter>* for all Policy Model D NF Communication. This parameter helps SCP to discover the suitable NF for discovery. Policy supports the following discovery parameters for Model D NF Communication: • `supi` • `data-set (may be included for UDR Discovery)` • `preferred-locality` • `dnn (may be included for BSF, SMF Discovery)` • `snssais` • `guami (maybe included for AMF Discovery)` • `group-id-list ( May be included for "UDR","CHF" discovery.)` Policy supports the following discovery parameters for Custom, Model B, and Model C NF Communications: • `target-nf-set-id` • `supi` • `group-id-list` **Note**: The Nbsf interface does not include SUPI as a discovery parameter that is, SUPI is not supported for BSF interface.
Send Discovery Header in Initial Messages	This switch indicates if PCF must include the *3gpp-sbi-discovery-<discovery-parameter>* parameters in the initial SBI message. By default the switch remains disabled.
Send Discovery Header in Subsequent Message	This switch indicates if PCF must include the following *3gpp-sbi-discovery-<discovery-parameter>* parameters in SBI messages: • Parameters to update a subscription, such as PUT messages when unable to fill in a `3gpp-sbi-routing-binding` header. • Parameters to delete a subscription, such as DELETE messages when unable to fill in a `3gpp-sbi-routing-binding` header. By default the switch remains disabled.
Send Target API Root Header in Initial Messages	Indicates if PCF must include `3gpp-sbi-target-apiroot` in initial request messages. If the user selects Model D for Policy NF Communication Model, the value is set to false. For other Policy NF Communication Model values, the default value is true.
On Demand Discovery Caching	Provide On Demand Discovery Caching details:
Force Discovery	Indicates whether to cache the NF profiles in NRF client or to skip caching and receive the response directly from NRF. Value of this parameter can be 0 or 1. • When the value of OC-Force-Rediscovery parameter is set to 0, global cache configuration is taken into account. • When the value of OC-Force-Rediscovery parameter is set to 1, global cache configuration is ignored and NF profiles get retrieved directly from NRF while responding to the query from the backend services. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-31 (Cont.) Create NF Communication Profile

Field Name	Description
Retention Period (in ms)	Indicates the time a record is allowed to stay in database after expiry. This parameter accepts an integer value to indicate the retention period in milliseconds. When retention period is not configured or saved as null, backend will not send this header to NRF connector. **Default value**: 0
NF Bindings Settings	Provide NF Bindings Settings details:
Binding Level	Indicates the binding level that must to be included in the *3gpp-sbi-binding* header when PCF adds this header in a message to another NF. Select any of the following values from the drop down menu: • NF Set • NF Instance **Default Value**: NF Set
Send Binding Header	Indicates if PCF includes the *3gpp-sbi-binding* header in SBI messages for the subscription creation, modification, or notification requests and responses, as applicable. By default the switch remains enabled.
Send PCF Service Name in Binding Header	Indicates whether to include the service name in the binding header or not. Possible values: • true: Includes `svcname` in the binding header sent towards NFs such as UDR, AMF, or BSF (customized) except for CHF, which contains the 3GPP defined PCF service name. • false: Does not include `svcname` in the binding header. **Default value** : false
Send Routing Binding Header	Indicates if PCF includes the *3gpp-sbi-routing-binding* header in SBI messages for the subscription creation, modification, or notification requests, as applicable. By default the switch remains disabled.
Send Callback Header	Indicates if PCF includes the *3gpp-sbi-callback* header in SBI messages for the subscription creation, modification, or notification requests, as applicable. By default the switch remains disabled.
NF Server Settings	Provide NF Server Settings details:
Send Server Header	Indicates if services Policy microservices include server header while sending an error response.
Server Header Error Codes	Specifies the error codes for which service header is generated. The error codes can be from 100 to 999. **Note**: If no error is specified, then Policy sends server header for all error responses.
Retry & Alternate Routing Settings	Provide Retry & Alternate Routing Settings details:
Retry Profile for Initial Messages	Specifies the retry or alternate routing options when an SBI message is not delivered successfully in any of the following scenarios: • POST operation to create a subscription • GET or PATCH request not belonging to a subscription
Retry Profile for Subsequent Messages	Specifies the retry or alternate routing options when an SBI message that updates, deletes or notifies a subscription is not delivered successfully.
NF Correlation Settings	Provide NF Correlation Settings details:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-31 (Cont.) Create NF Communication Profile

Field Name	Description
Send Correlation-info header	This specifies if the PCF should send Subscriber identifier as sbi-header-info or not. By default the switch remains disabled.
Allowed Correlation-info Header Generation Type(s)	Specifies that if correlation header is not received from Consumer NFs, PCF should generate the header. The Correlation-Type supported • SUPI • GPSI • (Select either both or none)
NF Peer Info Settings	Provide NF Peer Info settings details:
Send NF-Peer-Info Header	Enables PCF to send the received or generated NF peer info headers to peer NFs. **Default value**: false
Include NF Service Instance ID	Enables PCF to include the NF service instance ID when forwarding received or generated headers. **Default value**: false
Re-attempt Settings	Provide Re-attempt Settings details:
Enable NF Service Operation Re-attempt	This is a global flag to enable re-attempt for NF service operations. **Default value**: false
NF Service Operation Profiles	Configure the list of NF Service Operations along with Reattempts Profile.
NF Service Operation	Click Add **NF Service Operation** table. This opens **Add NF Service Operations Profiles** pop-up window. Here configure the list of NF Service Operations along with Reattempts Profile by using the following fields: Dropdown which lists filtered Reattempts Profiles for selected Service Operation • **NF Service Operation:** From the dropdown lists choose the reattempts profiles for selected service NAS operations: – `AMF Discovery` – `N1N2 Message Subscribe` – `N1N2 Message Transfer` – `N1N2 Transfer Failure Notification` • **Re-attempt Profile:** From the dropdown lists choose the Reattempts Profiles for the selected service operation. On selecting the `AMF Discovery` service operation, the field lists the Reattempts Profiles for NRF interface type. On selecting the `N1N2 Message Subscribe`, or `N1N2 Message Transfer`, or `N1N2 Transfer Failure Notification` service operation, the field lists the Reattempts Profiles for AMF interface type.

> **Note**
>
> If the Retry and Alternate Routing settings are configured on the NF Communication Profile page, these settings take precedence over the alternate routing settings configured on the service configurations page for each service.

4. Click **Save**.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The NF communication profile gets listed on the **NF Communication Profiles** page. The communication profile also get listed under the respective service configuration on the following pages:

- PCF Session Management
- PCF Access and Mobility
- PCF Policy Authorization
- PCF UE Policy Service
- Binding Service
- PCF User Connector

> **Note**
>
> The NF Communication Profile must be deleted in the service configurations before deleting from this page. As cyclic references are not handled currently.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the profile.

Importing NF Communication Profiles

To import NF Communication Profile:

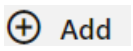
1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.1.6 Attribute Forwarding Profiles

The **Attribute Forwarding Profiles** page allows you to create new and manage existing Attribute Forwarding profiles. The page displays the list of defined profiles with the options to import, export, or add profiles.

For more details on Attribute Forwarding Profiles, see *Attribute Forwarding Profiles* section in Usage Monitoring on Gx Interface.

To configure Attribute Forwarding Profiles profile, perform the following steps:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **Common Data**, and then select **Attribute Forwarding Profiles**.
2. Click  .
   This opens the **Create Attribute Forwarding Profiles** page.
3. On the **Create Attribute Forwarding Profiles** page, enter the following information:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-32 Create Attribute Forwarding Profiles

Field Name	Description
Name	Enter the Attribute Forwarding Profile name.
Forwarded Attributes	Enter the list of attributes to be forwarded from one service to another.

4. To add new Forwarded Attributes, click ⊕ Add.
This opens the **Add Forwarded Attributes** page.
5. On **Add Forwarded Attributes** page, enter the following details:

Table 7-33 Add Forwarded Attributes

Field Name	Description
Attribute Name	Enter the name of the attribute.
Attribute Source	Specify the source of the attribute to be forwarded. Attribute Source provides the following options: • Request Message: The incoming request message such as Gx CCR message or SM Policy Association Create message. • User Data: Data received from different data sources such as UDR and CHF. • Session Data: Data saved in the session (association) previously, such as saved APN/DNN value.
Attribute Selection	Attribute Selection can be: • Predefined • Custom
Request Message Type	Request Message Type can be: • Diameter Message • HTTP Message **Note**: Currently, Policy supports only Diameter Messages for Request Message Type.
Diameter	This field appears when the Request Message Type is Diameter Message. Specifies the diameter message type such as 3GPP Gx and Gx CC Request.
Attribute Location	CNC Console displays this field when the Attribute Selection is of Custom type. It indicates the path/location at which this attribute can be found by the source (forwarder) micro-service.

6. Click **Save** on **Add Forwarded Attributes** page to add the new Forwarded Attribute.
7. Click **Save** on **Create Attribute Forwarding Profiles** page to add the new Attribute Forwarding Profile.

7.3.1.7 Rx Reauth Profiles

The **Rx Reauth Profiles** page allows you to create new and manage existing Rx Reauth Profiles. The page displays the list of defined profiles with the options to add profiles.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure Rx Reauth Profiles, perform the following steps:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **Common Data**, and then select **Rx Reauth Profiles**.
2. Click Add .
   This opens the **Create Rx Reauth Profiles** page.

> **Note**
>
> Predefined Setting exists for `ALL` and `Video` **Media Types**. User can edit these predefined settings based on the requirements and add new settings for additional Media Types.

3. On the **Create Rx Reauth Profiles** page, enter the following information:

Table 7-34 Create Rx Reauth Profiles

Field Name	Description
Name	Enter the Rx Reauth Profile name.
Settings	Enter the list of settings.

4. To add new settings, click Add .
   This opens the **Add Settings** page.
5. On the **Add Settings** page, enter the following details:

Table 7-35 Add Settings

Field Name	Description
Media Type	Enter the name of the media type. Allowed Values: ALL, AUDIO, DATA, APPLICATION, VIDEO, CONTROL, TEXT, MESSAGE, NOMEDIATYPE, OTHER Default Value: All
Precedence	When the Notify-Update triggered by Rx request towards SMF fails and if that respective Rx request had multiple media types resulting different Reauth Actions, then based on this precedence value Reauth Action will be finalized. Lowest Precedence will take the highest priority. Allowed Values: 1-99 Default Value: Null
Accept All Errors	If this field is true, Reauth Action is considered for any Error or Exception on Update Notify failure response from SMF triggered by Rx request. Allowed Values: True, False Default Value: False

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-35 (Cont.) Add Settings

Field Name	Description
Errors	When the Notify-Update triggered by Rx request towards SMF fails with any error code or cause and the **Accept All Errors** field is set as False, check the Table 7-36 example table and match the ErrorCode and ErrorCause of the failure. To add ErrorCode and ErrorCause , click ⊕ Add **Note:** If the ErrorCode is configured and ErrorCause is left empty, PCF will compare only the ErrorCode and allow any ErrorCause for that specific error to match. Default Value: Empty List
Exceptions	When the Notify-Update triggered by Rx Request towards SMF fails with any exception, then match the exception of the failure. To add Exceptions , click ⊕ Add Default Value: Empty List
Reauth Action	Given that all following conditions for current setting are met: a. MediaType specified matches b. Error matched successfully or Exception matches successfully Then PCF will take one of the following Reauth Actions: • **SEND_ASR**: this means PCF will continue to process as before the feature was implemented (send ASR to PCSCF/AF or RAR based on the pcc_rules removed). • **SUPPRESS_ASR**: this means PCF will NOT send an ASR to PCSCF/AF • **SEND_RAR**: this means PCF will send an RAR with **Failed Resource Allocation (FRA)** to PCSCF/AF – The RAR will be sent with FRA irrespective if the AAR-I/U came with FRA AVP. – In this case PCF will NOT send an ASR to PCSCF/AF. Allowed Values: SEND_ASR, SUPPRESS_ASR, SEND_RAR Default Value: SEND_ASR

The following table shows examples of the combinations configured in the Reauth Profile section in the CNC Console and Error/Exception received in UpdateNotify Response and the expected outcome from Reauth Profile configured logic:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-36 ErrorCode and ErrorCause Combination

Configuration mentioned in the CNC Console	ErrorCode in Update Notify Response	ErrorCause in Update Notify Response	Expected outcome from Reauth Profile configured logic
Nothing configured	5xx/4xx	NA	No match
`{"error code": 503, "error cause": ""}`	503	...	Match
	503	SERVICE_UNAVAILABLE	Match
	503	CUSTOM_503	Match
	404	...	No match
`{ "error code": 503, "error cause": "SERVICE_UNAVAILABLE", "error code": 503, "error cause": "NF_CONGESTED", "error code": 503, "error cause": "CUSTOM_503", "error code": 404, "error cause": "NOT_FOUND", }`	503	...	Match
	503	SERVICE_UNAVAILABLE	Match
	404	...	Match
`{ "error code": 503, "error cause": "SERVICE_UNAVAILABLE", "error code": 404, "error cause": "NOT_FOUND", "error code": 503, "error cause": "", }`	503	SERVICE_UNAVAILABLE	Match
	503	CUSTOM_503	Match
	404	NOT_FOUND	Match

6. Click **Save** on **Add Settings** page to add the new settings.
7. Click **Save** on **Create Rx Reauth Profiles** page to add the new Rx Reauth Profile.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.1.8 Message Profiles

Perform the following procedure to configure Message Profiles.

1. From the navigation menu under **Policy**, navigate to **Common Data** under **Service Configurations**. Browse to **Message Profiles** page.

   Message Profiles page is displayed. The page shows the existing configurations.

2. You can either edit an existing profile or create a new profile.

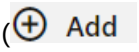
   The **Type to Filter** text box allows to filter the required list of profiles based on a given keyword.

3. Click **Create With Default** to create a profile using default values for different service types.

   In the **Create Message Profiles Using Default Values** window, configure the following:

Table 7-37 Create Message Profile with Default Values

Field Name	Description
Message Profile Name	Specifies the name of the message profile to be created.
Service Type	Select the service type for which the message profile is to be created. • PCF Session Management • Binding service • UDR Connector • CHF Connector

4. Click **Add** (

) to create a new Message Profile.

Table 7-38 Creating Message Profile

Field Name	Description
Message ID	A unique identifier representing specific message rule parameters, including interface type, message type, and priority. Multiple Message IDs can be configured per profile. When a request is received, the configured Message Profile based on message attributes is parsed to identify the appropriate MessageID. The Enhanced Overload Actions rules associated with that MessageID determines whether a Reject or Assume Positive or both actions are executed.
Rule Priority	A numeric value that uniquely identifies a rule when multiple rules have similar configurations. Range: 1–65535

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-38 (Cont.) Creating Message Profile

Field Name	Description
Interface Type	Defines the network interface through which the message is transmitted For example, `Npcf_SMPolicyControl`, `Npcf_PolicyAuthorization`, `Diameter_Rx`, and `Other`. For interface types `Npcf_SMPolicyControl`, `Npcf_PolicyAuthorization`, and `Diameter_Rx`, the supported message types are 'Create','Update' and 'Delete'. For `Other` interface type, the supported message type is `Bsf_Audit_Notification`.
Message Type	Denotes the type of message for the selected interface. The supported values of **Message Type** depends on the **Interface Type**. For example one of the following Message Type can be selected when the **Interface Type** is `Npcf_SMPolicyControl`: • Any (Any of the message types listed below) • Create • Update • Delete • Update_Notify • Terminate_Notify For the complete list of message types supported by each interface type, see Message Attributes Supported for Different Service Types and Interface Types.
Message Profile Filter Conditions	Configure the message profile filter conditions to filter out rules that matches these attributes as explained in Table 7-39 and click **Save**.
Request Priority Override	Determines the behavior for overwriting the incoming message's priority with the priority defined in the profile. Possible values: • Always • Never • IfNotPresent Default: Never **Note**: For the **Diameter_Rx** interface type, priority is always sent to the endpoint service and cannot be removed. Therefore, priority will always be present in SM service. Based on this behavior, the `IfNotPresent` option for priority override is not required for handling Diameter Rx messages.
Request Priority Value	Specifies the numeric priority value to apply when `Request Priority Override` is set to `Always` or `IfNotPresent`. Range: 0–31

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-38 (Cont.) Creating Message Profile

Field Name	Description
Response Priority Assign	It specifies the rule to specify response priority value. Possible values are: • `Never`: Indicates not to assign any response priority. • `Custom`: Allows to use specify the desired response priority in the **Response Priority Assign** field. • `EvaluatedRequestPriority`: Indicates that whatever is the final request priority, the same gets assigned to the response. **Default value**: Never

Table 7-39 Add Message Profile Filter Conditions

Field	Description
Attribute Name	Specifies the name of the attribute. Depending upon the value of **Interface Type**, message attributes list will be displayed. The following are some of the supported attribute names: • DNN • S-NSSAI • ServiceURN • 3GPP-SBI-Message-Priority • oc-message-priority For detailed list of message attributes supported for each interface type, see Message Attributes Supported for Different Service Types and Interface Types. While providing DNN or S-NSSAI as Message profile filter conditions, a comma separated list can be given to support overload actions to support multiple DNN or S-NSSAI in one rule. A max of 10 unique DNN's can be created under one rule. Similarly a max of 10 unique S-NSSAI can be created under one rule. **Note**: For a given Message Profile rule, if both message attributes, DNN and S-NSSAI for the Npcf_SMPolicyControl interface, or DNN and ServiceURN for the Diameter Rx or Npcf_PolicyAuthorization interface are configured, they function as an 'AND' condition. That is, both the attributes must match the corresponding parameters in the incoming request body to identify the correct MessageID. If no Message Attribute is configured for a given rule, all the messages having any DNN or S-NSSAI are considered for that rule.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-39 (Cont.) Add Message Profile Filter Conditions

Field	Description
Attribute Value	This field is used to mention the value of the attribute. The Attribute values for the selected attribute field is derived from the respective DNN Profile, S-NSSAI Profile, and ServiceUrn Profile.

5. Click **Save** to save the configuration.

Message Attributes Supported for Different Service Types and Interface Types

Service Type: PCF Session Management

Table 7-40 Interface Type: Npcf_SMPolicyControl

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Create	DNN	Yes	Yes	Yes
Update	DNN	Yes	Yes	Yes
Delete	DNN	Yes	Yes	Yes
Create	S-NSSAI	Yes	Yes	Yes
Update	S-NSSAI	Yes	Yes	Yes
Delete	S-NSSAI	Yes	Yes	Yes
Create	3GPP-SBI-Message-Priority	No	No	Yes
Update	3GPP-SBI-Message-Priority	No	No	Yes
Delete	3GPP-SBI-Message-Priority	No	No	Yes
Create	oc-message-priority	No	No	Yes
Update	oc-message-priority	No	No	Yes
Delete	oc-message-priority	No	No	Yes
Update_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Update_Notify	oc-message-priority	No	No	Yes
Terminate_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Terminate_Notify	oc-message-priority	No	No	Yes

> **Note**
>
> During SM pod congestion, emergency request acceptance depends on the message priority versus the configured discard thresholds. You should assign a higher priority (numerically lower value) for emergency requests using the Message Profile configurations. Set the emergency request message priority to a value above the congestion discard level to avoid rejection.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-41 Interface Type: Npcf_PolicyAuthorization

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Create	DNN	Yes	No	Yes
Update	DNN	Yes	No	Yes
Delete	DNN	Yes	No	Yes
Create	ServiceURN	Yes	No	No
Update	ServiceURN	Yes	No	No
Delete	ServiceURN	Yes	No	No
Create	S-NSSAI	No	No	Yes
Update	S-NSSAI	No	No	Yes
Delete	S-NSSAI	No	No	Yes
Create	3GPP-SBI-Message-Priority	No	No	Yes
Update	3GPP-SBI-Message-Priority	No	No	Yes
Delete	3GPP-SBI-Message-Priority	No	No	Yes
Create	oc-message-priority	No	No	Yes
Update	oc-message-priority	No	No	Yes
Delete	oc-message-priority	No	No	Yes
Subscribe	3GPP-SBI-Message-Priority	No	No	Yes
Subscribe	oc-message-priority	No	No	Yes
UnSubscribe	3GPP-SBI-Message-Priority	No	No	Yes
UnSubscribe	oc-message-priority	No	No	Yes
Update_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Update_Notify	oc-message-priority	No	No	Yes
Terminate_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Terminate_Notify	oc-message-priority	No	No	Yes

Table 7-42 Interface Type: Diameter_Rx

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Create	DNN	Yes	No	No
Update	DNN	Yes	No	No
Delete	DNN	Yes	No	No
Create	ServiceURN	Yes	No	No
Update	ServiceURN	Yes	No	No
Delete	ServiceURN	Yes	No	No

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-43 Interface Type: Other

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Bsf_Audit_Notification	-	Yes	No	No

Service Type: Binding

Table 7-44 Interface Type: Nbsf_Management

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Register	DNN	No	No	Yes
Register	S-NSSAI	No	No	Yes
Register	3GPP-SBI-Message-Priority	No	No	Yes
Register	oc-message-priority	No	No	Yes
Deregister	DNN	No	No	Yes
Deregister	S-NSSAI	No	No	Yes
Deregister	3GPP-SBI-Message-Priority	No	No	Yes
Deregister	oc-message-priority	No	No	Yes

Table 7-45 Interface Type: Npcf_Binding_Audit

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Audit_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Audit_Notify	oc-message-priority	No	No	Yes

Service Type: UDR Connector

Table 7-46 Interface Type: Nudr_DataRepository

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Get_Policy_Data	DNN	No	No	Yes
Get_Policy_Data	S-NSSAI	No	No	Yes
Get_Policy_Data	3GPP-SBI-Message-Priority	No	No	Yes
Get_Policy_Data	oc-message-priority	No	No	Yes
Get_Policy_Data	policy-data	No	No	Yes
Subscribe	DNN	No	No	Yes
Subscribe	S-NSSAI	No	No	Yes
Subscribe	3GPP-SBI-Message-Priority	No	No	Yes
Subscribe	oc-message-priority	No	No	Yes

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-46 (Cont.) Interface Type: Nudr_DataRepository

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Subscribe	policy-data	No	No	Yes
ReSubscribe	DNN	No	No	Yes
ReSubscribe	S-NSSAI	No	No	Yes
ReSubscribe	3GPP-SBI-Message-Priority	No	No	Yes
ReSubscribe	oc-message-priority	No	No	Yes
ReSubscribe	policy-data	No	No	Yes
UnSubscribe	3GPP-SBI-Message-Priority	No	No	Yes
UnSubscribe	oc-message-priority	No	No	Yes
UnSubscribe	policy-data	No	No	Yes
Patch_Policy_Data	3GPP-SBI-Message-Priority	No	No	Yes
Patch_Policy_Data	oc-message-priority	No	No	Yes
Patch_Policy_Data	policy-data	No	No	Yes
Policy_Data_Change_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Policy_Data_Change_Notify	oc-message-priority	No	No	Yes
Lookup_Subscription	DNN	No	No	Yes
Lookup_Subscription	S-NSSAI	No	No	Yes
Lookup_Subscription	3GPP-SBI-Message-Priority	No	No	Yes
Lookup_Subscription	oc-message-priority	No	No	Yes
Lookup_Subscription	policy-data	No	No	Yes

Service Type: CHF Connector

Table 7-47 Interface Type: Nchf_SpendingLimitControl

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Subscribe	3GPP-SBI-Message-Priority	No	No	Yes
Subscribe	oc-message-priority	No	No	Yes
UnSubscribe	3GPP-SBI-Message-Priority	No	No	Yes
UnSubscribe	oc-message-priority	No	No	Yes
Update_Subscription	3GPP-SBI-Message-Priority	No	No	Yes

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-47 (Cont.) Interface Type: Nchf_SpendingLimitControl

Message Type	Attribute	Enhanced Overload [Reject]	Enhanced Overload [Assume Positive]	SMP
Update_Subscription	oc-message-priority	No	No	Yes
Update_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Update_Notify	oc-message-priority	No	No	Yes
Terminate_Notify	3GPP-SBI-Message-Priority	No	No	Yes
Terminate_Notify	oc-message-priority	No	No	Yes

7.3.1.9 Message Attributes

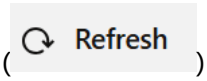
This section describes how to configure the message attributes such as DNN Profiles, S-NSSAI Profiles, and Service URN Profiles.

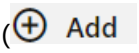
7.3.1.9.1 DNN

Perform the following procedure to configure Data Network Name (DNN) profiles.

1. From the navigation menu under **Policy**, navigate to **Common Data** under **Service Configurations**. Browse to **DNN** page under **Message Attributes**.

   DNN page is displayed. The page shows the existing configurations.
2. You can either create a new profile, edit an existing profile, or delete an existing profile.

   The **Type to Filter** text box allows to filter the required list of profiles based on a given keyword.
3. Click **Refresh** (

) to refresh the list of existing DNN Profiles.
4. Click **Add** (

to create a new DNN Profile.

Table 7-48 Create DNN Profile

Field Name	Description
DNN ID	Numeric identifier that uniquely represents a DNN entry. A unique ID must be assigned within the allowed range. **Range:** 1 to 255
DNN	Represents the DNN. This value uniquely identifies each DNN for configuration and reference within the system.

5. Click **Save** to save the configuration.

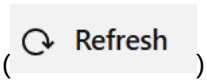
7.3.1.9.2 S-NSSAI

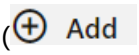
Perform the following procedure to configure S-NSSAI profiles.

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the navigation menu under **Policy**, navigate to **Common Data** under **Service Configurations**. Browse to **S-NSSAI** page under **Message Attributes**.

   S-NSSAI page is displayed. The page shows the existing configurations.
2. You can either create a new profile, edit an existing profile, or delete an existing profile.

   The **Type to Filter** text box allows to filter the required list of profiles based on a given keyword.
3. Click **Refresh** (

) to refresh the list of existing S-NSSAI profiles.
4. Click **Add** (

to create a new S-NSSAI Profile.

Table 7-49 Creating S-NSSAI Profile

Field Name	Description
S-NSSAI ID	Unique identifier for the S-NSSAI entry.
SST	The Slice or Service Type value associated with the S-NSSAI.
SD	Slice Differentiator value for the S-NSSAI.

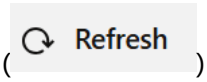
5. Click **Save** to save the configuration.

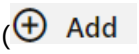
7.3.1.9.3 Service URN

Perform the following procedure to configure Service URN profiles.

1. From the navigation menu under **Policy**, navigate to **Common Data** under **Service Configurations**. Browse to **Service URN** page under **Message Attributes**.

   Service URN page is displayed. The page shows the existing configurations.
2. You can either create a new profile, edit an existing profile, or delete an existing profile.

   The **Type to Filter** text box allows to filter the required list of profiles based on a given keyword.
3. Click **Refresh** (

) to refresh the list of existing Service URN Profile Names.
4. Click **Add** (

to create a new Service URN Profile.

Table 7-50 Creating Service URN Profile

Field Name	Description
Service URN ID	Specifies the identifier for each Service URN. **Range**: 1–255
Service URN	Specifies the Uniform Resource Name (URN) for the service. A maximum of 255 unique Service URNs can be created. For example: `urn:service:sos.ambulance`

5. Click **Save** to save the configuration.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.1.10 Service Profiles

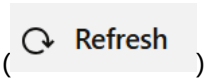
Perform the following procedure to configure Service Profiles.

1. From the navigation menu under **Policy**, navigate to **Common Data** under **Service Configurations**. Browse to **Service Profiles** page.

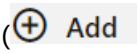
   Service Profiles page is displayed. The page shows the existing configurations.

2. You can either edit an existing profile or create a new profile.

   The **Type to Filter** text box allows to filter the required list of profiles based on a given keyword.

3. Click **Refresh** (

) to refresh the list of existing Service Profiles.

4. Click **Add** (

 to create a new Service Profile.

Table 7-51 Creating Service Profile

Field Name	Description
Service Profile Name	Specifies the unique name of the Service Profile. This Service Profile is later selected when associating the profile to an Overload rule for Assume Positive handling.
Service Type	Specifies the service for which this Service Profile applies. Service Profiles are used to control which internal interactions are allowed or skipped during overload handling for Policy microservice. **Note**: Currently Policy supports only PCF Session Management service.
Interface Type	Specifies the interface that the Service Profile governs. **Note**: Currently Policy supports only Npcf_SMPolicyControl.
Service Interactions	
Policy Evaluation	Indicates whether SM service interacts with PRE for policy evaluation when a request is processed under an Assume Positive overload rule. Possible values are true, false. When the value of this field is false, that is, when it is disabled, the response behavior of SM service is driven by the configured **Default Processing Profile**. For example, default PCC/session rules and related behaviors.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-51 (Cont.) Creating Service Profile

Field Name	Description
User Data Interaction	Indicates whether SM service interacts with PDS for User Data retrieval or subscription. Possible values are true, false. When this field is disabled, SM service does not perform User Data interactions (for example, GET/Subscribe), and User Data source communication is suppressed for overload recovery.
Spending Limit Data Interaction	Indicates whether SM service interacts with PDS for Spending Limit Data (CHF/OCS data) retrieval or subscription. Possible values are true, false. When this field is disabled, CHF-related interactions (sync/async) are suppressed as part of overload recovery.

5. Click **Save** to save the configuration.

7.3.1.11 Default Processing Profiles

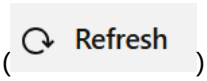
Perform the following procedure to configure Default Processing Profiles.

1. From the navigation menu under **Policy**, navigate to **Common Data** under **Service Configurations**. Browse to **Default Processing Profiles** page.

   Default Processing Profiles page is displayed. The page shows the existing configurations.

2. You can either edit an existing profile or create a new profile.

   The **Type to Filter** text box allows to filter the required list of profiles based on a given keyword.

3. Click **Refresh** () to refresh the list of existing Service Profiles.

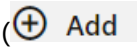
4. Click **Add** ( to create a new Default Processing Profiles.

Table 7-52 Creating Default Processing Profiles

Field Name	Description
Profile Name	Specifies a unique name of the Default Processing Profile. This profile is later mapped under **PCF Session Management** page to control the default response behavior when PRE policy evaluation is not performed (for example, due to Assume Positive restrictions or PRE failures). This is a mandatory field.
Service Type	Specifies the service to which this Default Processing Profile applies. Currently, Policy supports only PCF Session Management service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-52 (Cont.) Creating Default Processing Profiles

Field Name	Description
Interface Type	Specifies the interface on which the default processing behavior is applied. Currently, Policy supports only `Npcf_SMPolicyControl` interface with Default Processing Profile.
Message Profile	Specifies the Message Profile used to supply the list of MessageIDs that can be mapped to the default processing actions such as PCC rules, session rules, BSF registration, and CHF counter-fetch behavior.
Message Profile Mapping	
Message ID	This is a mandatory field. This field specifies the MessageID selected from the Message Profile. A MessageID represents a unique combination of interface type, message type, message attributes (for example, DNN and/or SNSSAI), and priority, and is used to determine which default actions are applied. The value for this field must be selected from the list of MessageIDs created for Message Profiles.
PCC Rules	Specifies the default PCC rules to include in the response when policy evaluation is not performed by PRE (for example when Assume Positive feature disables policy evaluation, PRE is disabled, or PRE returns an error).
Session Rules	Specifies the default session rules to include in the response when policy evaluation is not performed by PRE.
BSF Registration	Indicates whether to enable or disable BSF (binding) registration for the selected MessageID when default processing is applied. Possible values: • enable: BSF (binding) registration is performed for the selected MessageID when default processing is applied. • disable: BSF (binding) registration is not performed for the selected MessageID when default processing is applied. **Default value**: disabled
BSF Registration Mode	This field appears when BSF Registration is enabled. BSF Registration Mode is used to interact with the Binding/BSF service when BSF Registration is enabled. Possible values: • Synchronous • Asynchronous

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-52 (Cont.) Creating Default Processing Profiles

Field Name	Description
Spending Limit Interaction	This field is used to control CHF interaction for Policy counter retrieval when the default processing is applied. Possible values are: • None • CHF **Default value**: None
Fetch Counter	This field appears when **Spending Limit Interaction** is CHF. It specifies whether to fetch all the counters or only specific counters from CHF. Possible values are: • All: to fetch all the Policy counters from CHF. • Specific: to fetch only the specific counters from CHF.
Policy Counter IDs:	Appears when `Specific` option is chosen for **Fetch Counter** field. This field provides the list of Policy counter IDs to fetch from CHF.

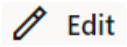
5. Click **Save** to save the configuration.

7.3.2 PCF Session Management

This procedure provides information about configuring the PCF Session Management Service.

The **PCF Session Management** page displays the SM Service configurations. The page allows you to edit the configurations.

To edit PCF Session Management Service:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, and select **PCF Session Management**.
   This opens the **PCF Session Management** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit PCF Session Management** page displaying the default configuration for the fields available in respective groups.
3. Expand the **System** group.
   This group allows you to edit system configurations.
4. Enter the values for the input fields, available under the group.
   The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-53 Edit System Configurations

Field Name	Description
Component Tracing	Determines, if component tracing is enabled. Component tracing is used to evaluate system process latency in detail level. By default, this switch remains disabled.
FQDN	The PCF FQDN used by the PCF to register Binding data to BSF. AF may use this FQDN to communicate with PCF on N5 reference point. FQDN needs to be in a standard FQDN format (RFC 1035). **Default Value**: `oc-diam-gateway` **Note** : If we have multiple PCF, Diameter identity and FQDN must be unique.
Diameter Realm	The PCF Diameter realm used by the PCF to register Binding data to BSF. Diameter based AF may use this Diameter realm to communicate with PCF on Rx reference point. **Default Value**: `oracle. com`
Diameter Identity	The PCF Diameter identity used by the PCF to register Binding data to BSF. Diameter based AF may use this Diameter identity to communicate with PCF on Rx reference point. **Default Value**: `oc-diam-gateway` **Note** : In case of multiple PCF, Diameter identity and FQDN must be unique.
Snssai	Used to register Binding data to BSF by PCF. AF or BSF may use this SNSSAI to discover proper PCF. Format is : sst,sd. **Default Value**: `0,000000`
Enable Metrics	This determines if system metrics is enabled. This takes priority on global metrics configuration. By default, this switch remains enabled. **Default Value**: `true`
Override Supported Features	Indicates a list of supported features that can be configured to override system embedded values. For example, • SessionRuleErrorHandling • NetLoc • PolicyDecisionErrorHandling • QoSMonitoring • ResShare • 3GPP-PS-Data_Off • ADC • UMC • RAN-NAS-Cause • ProvAFsignalFlow **Note:** If any supported feature is enabled in one site then the same needs to be enabled on all other sites at the same time. By default, it is blank.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-53 (Cont.) Edit System Configurations

Field Name	Description
Enable Custom Json	This determines if custom JSON is enabled. By default, this switch remains disabled. **Default Value**: false
SMF Notification Retry Profile	Defines the retry profile configuration for session management. For more information on configuring retry profile, see Retry Profiles.
SMF Communication Profile	Specifies the NF communication profile used by SMF. For more information about configuring NF communication profiles, see NF Communication Profiles.
Data Compression Scheme	Specifies the data compression scheme used by SM. Following are the allowed values for this field: • Disabled • MySQL_Compressed • Application Compressed By default, this value remains disabled.
DB Encoding	Specifies either to enable or disable database encoding. By default, this value remains disabled.
Rx Reauth Profile for Rx Create	Specifies the selection of the Rx Reauth Profile for Update Notify Failures happens due to Rx Create Request. Allowed Value: String (Only one profile) Default value: Empty
Rx Reauth Profile for Rx Update	Specifies the selection of the Rx Reauth Profile for Update Notify Failure happens due to Rx Update Request. Allowed Value: String (Only one profile) Default value: Empty

5. Expand the **User** group.
   This group allows you to edit the subscriber configurations.
6. Enter the values for the input fields, available under User group.
   The following table describes the fields:

Table 7-54 Edit User Configurations

Field Name	Description
Validate User	If the User profile, for any of the User Data types given under the **User Data Types** group, are fetched successfully, the user is considered to be a known user. However, if the user profile lookup has failed on the discovered data source, the user profile is marked as Unknown. If this switch is enabled and user is marked as Unknown, the session creation requests are rejected. If this switch is disabled and user is marked as Unknown, the session creation requests are handled and sessions are created successfully.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-54 (Cont.) Edit User Configurations

Field Name	Description
Query User	Determines if user query from UDR is enabled. When this option is enabled, PCF queries the UDR about the subscriber contained in the SM Association **create** request by sending a GET request for “sm-data” resource on the nudr-dr service. **Note:** The PDS service caches the subscriber profile when `Subscribe To Notify` option is enabled, in that case, the PCF may not always reach the UDR when the subscriber profile is found in the local cache. By default, this switch remains enabled.
Query User on Update	Determines if user query from UDR on update is enabled. When this option is enabled, PDS queries the UDR about the subscriber present in the SM Association **update** request by sending a GET request for `SmPolicyData` resource on the `nudr-dr service`. **Note**: If `Subscribe To Notify` is enabled for SM, then SM will not query the UDR during a Update requests. The PDS caches the subscriber profile when the `Subscribe To Notify` flag is enabled. In that case, Policy may not always reach the UDR when the subscriber profile is found in the local cache. When the `Subscribe To Notify` flag is enabled and previous subscription attempts failed, then along with the data query, PDS also sends a SUBSCRIBE request to UDR. By default, this option is disabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-54 (Cont.) Edit User Configurations

Field Name	Description
Query User on Terminate	Determines if user query from UDR on delete is enabled. When this option is enabled, PCF queries the UDR about the subscriber present in the SM Association **delete** request by sending a GET request for "SmPolicyData" resource on the nudr-dr service. **Note**: If `Subscribe To Notify` is enabled for SM, then SM will not query the UDR during a Terminate requests. The PDS caches the subscriber profile when the "Subscribe To Notify" option is enabled, in that case, the PCF may not always reach the UDR when the subscriber profile is found in the local cache. By default, this option is disabled. **Note** It should be enabled only when subscription to UDR is disabled. It should not be enabled if subscription to UDR is enabled.
Query User on Reauth	Determines if user query from UDR on reauth is enabled. When this option is enabled, PCF queries the UDR about the subscriber, when it receives a Reauthorization request, such as Rx or Policy Authorization request by sending a GET request for "SmPolicyData" resource on the nudr-dr service. **Note:** The PDS caches the subscriber profile when the "Subscribe To Notify" option is enabled, in that case, the PCF may not always reach the UDR when the subscriber profile is found in the local cache. By default, this option is disabled.
Disable Subscriber Variables	Determines if subscriber variables are stored or not in the PCF database. By default, the value is set to false.
User Data Types	To configure user data types.
SmPolicyData	If this switch is enabled, PCF fetches SMPolicyData from nUDR. For information on configuring SMPolicyData attributes, see Table 7-55.
Operator Specific Data	If this switch is enabled, PCF fetches OperatorSpecificData (imported using Custom Schema) from nUDR. For information on configuring SMPolicyData attributes, see Table 7-56.
Ldap Data	If this switch is enabled, PCF fetches user profile from LDAP through PDS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-54 (Cont.) Edit User Configurations

Field Name	Description
CHF Data	If this switch is enabled, PCF fetches policy counters from CHF. For information on configuring SMPolicyData attributes, see Table 7-57.
OCS Data	If this switch is enabled, PCF fetches policy counters from OCS. When this switch is enabled, PCF performs on-demand lookup of Policy Counters for a subscriber using the **Fetch Policy Counters** from *OCS* policy action. By default, this option is disabled. **Note**: It is possible to enable both CHF Data and OCS Data simultaneously. Based on PDS-PRE policy, PDS may make a choice between the two datasources. For information on configuring SMPolicyData attributes, see Table 7-58.

The following table describes the **SmPolicyData** switches available in the **Attributes** column:

Table 7-55 SmPolicyData Attributes

Attribute Name	Description
Subscribe to Notify	When this switch is enabled, Policy subscribes with the UDR to get notified on changes in subscriber profile. By default, this option is enabled.
Ignore Subs Notification Check	Ignore subscriber's notification check. By default, this option is false. **Note**: Currently, this field is not used by the Policy application.
Include Snssai in User Query	Determines if Snssai is included for SmPolicyData for PCF query and subscribe to UDR for Notification.
Include Dnn in User Query	Determines if Dnn is included for SmPolicyData for PCF query and subscribe to UDR for Notification.

The following table describes the **Operator Specific Data** switches available in the **Attributes** column:

Table 7-56 Operator Specific Data Attributes

Attribute Name	Description
Subscriber to Notify	When this switch is enabled, Policy subscribes with the UDR to get notified on changes in subscriber profile. By default, this option is false.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following table describes the **CHF Data** switches available in the **Attributes** column:

Table 7-57 CHF Data Attributes

Attribute Name	Description
Enable Async CHF Query	When this button is enabled, PCF interacts with CHF in Asynchronous mode. By default, this option is disabled.

The following table describes the **OCS Data** switches available in the **Attributes** column:

Table 7-58 OCS Data

Attribute Name	Description
Enable OCS Async Query	When this button is enabled, PCF performs on demand lookup for Policy Counters to be fetched from OCS. By default, this option is disabled.
Enable force lookup on Update	When this button is enabled, PCF performs force lookup for OCS Data. By default, this option is disabled.

7. Expand the **Policy** group.
   This group allows you to edit Policy configurations.
8. Under the **Policy** group, enable or disable the **Evaluate** switch.
   This switch determines, if policy evaluation is enabled.

   The default value is `true`.
9. Expand the **Policy Control Request Trigger** group.
   This group allows you to edit Policy Control Request Trigger configurations.
10. Under the **Policy Control Request Trigger** group, select values in the **Default Policy Control Request Triggers** drop-down list.
    This is the default Policy Control Request Trigger(s) to install on PDU session at SM Policy Association Establishment. You can select multiple values in a comma separated format.

    Some of the supported values are:

    - PLMN_CH
    - UE_IP_CH
    - DEF_QOS_CH
    - AC_TY_CH
    - SCNN_CH
    - RE_TIMEOUT
    - RES_RELEASE
    - SUCC_RES_ALLO
    - RAT_TY_CH
    - REF_QOS_IND_CH
    - SCELL_CH
    - USER_LOCATION_CH

Copyright © 2019, 2026, Oracle and/or its affiliates.

11. Expand the **Binding Configuration** group.
    This group allows you to edit the Binding configurations.
12. Enter the values for the input fields, available under the group.
    The following table describes the fields:

Table 7-59 Edit Binding Configurations

Field Name	Description
Binding Operation	Determines if binding operation (register and deregister) to the BSF is enabled. This service level global configuration applies to all session creation requests (belonging to all DNN and/or S-NSSAI. **Default Value**: TRUE After performing necessary configurations on this screen, user may use the policy action - **Set Binding Registration to** to update configurations for specific policies. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.
Binding Use Local Configured Bsf Always	Whether to use local configured BSF without Always discovering. **Default Value**: FALSE
Binding Use Local Configured Bsf When Not Discovered	Whether to use local configured (if having) BSF when not discovered or discover failed. Local configuration can be done using custom yaml. **Default Value**: FALSE
Use HTTP2	Determines if using http/2 to communicate with BSF. Otherwise use http/1.1. **Default Value** : TRUE
Abort or Terminate Session on Binding Error	Determines if PCF (SM service) should abort terminate session when binding error is received.
BSF Retry Profile for Initial Messages	Retry Profile to be used when PCF fails to send a create message to a producer node. For more information, see Retry Profiles. **Note:** This is a mandatory configuration to get the error codes from the **Attempt Alternate Route for Following Error Codes** option on the Retry Profiles page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-59 (Cont.) Edit Binding Configurations

Field Name	Description
BSF Retry Profile for Subsequent Messages	Retry Profile to be used when PCF fails to send an in-session message to a producer node. **Note:** • If both “Retry Profile for Initial Messages” and “Retry Profile for Subsequent Messages” are not configured (default case) no retry is attempted. • If both “Retry Profile for Initial Messages” and “Retry Profile for Subsequent Messages” are configured, retries is attempted accordingly. • If “Retry Profile for Initial Messages” is configured but “Retry Profile for Subsequent Messages” is not configured then the profile for initial messages is used for subsequent messages. (to be backward compatible with release 1.8.x) • If “Retry Profile for Initial Messages” is not configured but “Retry Profile for Subsequent Messages” is configured then retry is not attempted for initial messages but is attempted for subsequent messages.
Default Binding Operation Mode	Allows users to configure binding operation mode as synchronous or asynchronous. **Default value:** Synchronous **Note:** • The mode chosen during the CREATE request remains same during UPDATE and TERMINATE operations for the same SM session. • To ensure backward compatibility, if this attribute is not available in the database, the value is set to "Synchronous" After performing necessary configurations on this screen, user may use the policy action - **Set Binding Registration to** under **PCF-SM Category** to update configurations for specific policies. For more information, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.
BSF Communication Profile	Specifies the NF communication profile used by BSF. For more information about configuring NF communication profiles, see NF Communication Profiles.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-59 (Cont.) Edit Binding Configurations

Field Name	Description
BSF Binding Recreate Attempt	The switch to enable the BSF recreate attempts functionality. Possible values: • **Enabled:** The SM Service creates and updates the PendingOperations if the response from BSF applies for a reattempt and it updates the PendingOperation table in Audit Service. Audit Service sends notifications for retry timestamps that have been reached and SM Service triggers the Recreate attempt. • **Disabled:** SM Service deregisters the PendingOperation table in Audit Service and it does not create nor update entries in the PendingOperation table. • **Disable and Cleanup:** SM Service neither deregister the PendingOperation table in Audit Service nor it updates the table. Audit Service sends notifications to SM Service but the notifications does not get processed and SM service automatically deletes records from the PendingOperation table.
BSF Binding Recreate Attempt Profile	The Reattempt profile to be used for binding recreate attempts. For more information, see Reattempts Profile.
Service FQDN and IP Endpoints Configuration	Determines if Service FQDN and IP Endpoints are sent to BSF in the PCF Binding registration request. Possible Values: • SERVICE_FQDN • SERVICE_FQDN_AND_ENDPOINTS • SERVICE_ENDPOINTS **Default**: SERVICE_FQDN
NF Profile for Service FQDN and IP Endpoints	Determines from which NF Profile are the FQDN and IP Endpoints going to be taken from. Possible Values: • npcf-policyauthorization • npcf-smpolicycontrol **Default**: npcf-smpolicycontrol

13. Expand the **QoS** group.
    This group allows you to edit the QoS configurations.
14. Enter the values for the input fields, available under the group.
    The following table describes the fields:

Table 7-60 Edit QoS Configurations

Field Name	Description
Qos Data Id Prefix	This is the prefix of qos data id used by PCF to generate qos data id. For example, prefix is "qosdata_", the generated qos data id is qosdata_0. **Default Value** : qosdata_

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-60 (Cont.) Edit QoS Configurations

Field Name	Description
update Default Pcf Rule With Auth Def Qos	This determines whether to update Qos of default PccRule with the authDefQos of session rule. **Default Value** : TRUE
Install Default Qos If Not Requested	This determines whether to install default Qos to the PDU session if UE not requested. **Default Value** : TRUE
Default Qos 5qi	This is the 5Qi of default Qos which is applied if no default Qos is requested by UE. **Default Value**: 9
Default Qos Arp Preempt Cap	This is the ARP Preemption Capability of default Qos which is applied if no default Qos is requested by UE. **Default Value** : MAY_PREEMPT
Default Qos Arp Preempt Vuln	This is the ARP PreemptionVulnerability of default Qos which is applied if no default Qos is requested by UE. **Default Value** : NOT_PREEMPTABLE
Default Qos Arp Priority Level	This is the ARP Priority Level of default Qos which is applied if no default Qos is requested by UE. **Default Value**: 1

15. Configure **QoS Monitoring** section as follows:

Table 7-61 Configuring QoS Monitoring

Field	Description
QosMon Notification Target	Specifies the target for notifications that SMF triggers when PCF subscribes to QosMon. **Note**: Currently, PCF supports only AF/NEF as target for notification.

16. Expand the **Rule** group.
    This group allows you to edit the PCC Rule configurations.
17. Enter the values for the input fields, available under the group.
    The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-62 Edit Rule Configurations

Field Name	Description
Install Default Pcc Rule	This determines whether and how to install default pcc rule for a PDU session. Possible values are: • ALWAYS • IF_NO_PROVISIONED_RULE only if no other provisioned rule is configured • IF_NO_RULE only if no other rule (predefined or provisioned) is configured/ installed • NEVER **Default Value** : IF_NO_RULE
Default PCC Rule Profile	(Optional) If a default PCC Rule Profile is configured by the user, it is applied to the chosen PCC Rule.
Rule Id Prefix	This is the prefix of rule id of the pcc rule or session rule auto generated by PCF. for example, prefix is "0_", the generated rule id is 0_0, 0_1, etc.
Default Pcc Rule 5qi	This is the 5Qi of default pcc rule. **Default Value**: 9
Default Pcc Rule Precedence	This is the precedence of default pcc rule. **Default Value** : 3000
Default Pcc Rule Arp Preempt Cap	This is the ARP Preemption Capability of qos of default PCC rule. **Default Value** : NOT_PREEMPT
Default Pcc Rule Arp Preempt Vuln	This is the ARP PreemptionVulnerability of qos of default pcc rule. **Default Value** : PREEMPTABLE
Default PCC Rule Requested Rule Data	Used to set the default Requested Rule Data for the PCC Rule. **Default Value**: SUCC_RES_ALLO
App Rule Precedence Min	This value defines the minimum value for precedence of a PCC rule as authorized by the establishment of an application flow by the AF. If multiple rules are applied to the same packet flow or UE resource (i.e., overlapping rules) a rule with lower precedence value takes the priority over a rule with higher precedence value. The value of -1 is used to not set the precedence of a rule (NOT RECOMMENDED). **Default Value**: 400
App Rule Precedence Max	This value defines the maximum value for precedence of a PCC rule as authorized by the establishment of an application flow by the AF. If multiple rules are applied to the same packet flow or UE resource (i.e., overlapping rules) a rule with lower precedence value takes the priority over a rule with higher precedence value. The value of -1 is used to not set the precedence of a rule (NOT RECOMMENDED). **Default Value**: 899

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-62 (Cont.) Edit Rule Configurations

Field Name	Description
Default Pcc Rule Arp Priority Level	This is the ARP Priority Level of qos of default pcc rule The range is 1 to 15. Values are ordered in decreasing order of priority, for example, with 1 as the highest priority and 15 as the lowest priority. **Default Value** : 15
Switch Flow In To Out Enabled	This determines whether to switch "in" to "out" in flow description. The src and desc is switched as well. For example, if enabled, "permit in ip from 2800:a00:cc01:c056:1c00:de10:c481:f193/128 to 2800:a00:800:7::1:3b/128 36004" is changed to "permit out ip from 2800:a00:800:7::1:3b/128 36004 to 2800:a00:cc01:c056:1c00:de10:c481:f193/128" **Default Value**: FALSE
Set PacketFilterUsage to true for Preliminary Service Info	This determines whether the UE shall be provisioned with the packet filter for preliminary service.**Default Value**: FALSE
Install/Remove Rule Conflicts Strategy	When the remove action is **Remove ALL**(ALL, Predefined, Dynamic, Conditioned, non-conditioned): • INSTALL/MODIFY: SM Service removes all Session/PCC Rules previously installed and ignores all the remove actions for rules in conflict. • REMOVE: SM Service removes all Session/PCC Rules previously installed and ignores all the install actions for rules in conflict. • IGNORE: SM Service removes all Session/Pcc Rules previously installed and ignores all actions for rules in conflict, and does not run anything(install/remove). • Default: SM Service processes the remove actions and then the INSTALL or MODIFY actions.

18. Expand the **Charging** group.
    This group allows you to edit the charging configurations.
19. Enter the values for the input fields, available under the group.
    The following table describes the fields:

Table 7-63 Edit Charging Configurations

Field Name	Description
Charging Data Id Prefix	This is the prefix of chg data id used by PCF to generate chg data id. For example, prefix is "chgdata_", the generated chg data id is chgdata_0, chgdata_1, etc. **Default Value**: chgdata_
Primary CHF Address	Address of the primary CHF
Primary CHF Instance Id	Instance ID of the primary CHF
Primary CHF Set Id	Set ID of the primary CHF

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-63 (Cont.) Edit Charging Configurations

Field Name	Description
Secondary CHF Address	Address of the secondary CHF
Secondary CHF Instance Id	Instance ID of the secondary CHF
Secondary CHF Set Id	Set ID of the secondary CHF
Online	Indicates the online charging is applicable to the PDU session.
Offline	Indicates the offline charging is applicable to the PDU session.
Use Subscriber Default Charging Method	Indicates whether to use the online value defined in the PDU session. **Default Value**: true

20. Expand the **Traffic Control** group.
    This group allows you to edit Traffic Control configurations.
21. Under the **Traffic Control** group, enter value of the **Traffic Control Id Prefix** field.
    This is the prefix of traffic control data ID used by PCF to generate tc data id. For example, if prefix is "tcdata_", the generated tc data ID is tcdata_0, tcdata_1, and so on.

    Default Value: tcdata_
22. Expand the **IMS Emergency Session** group.
    This group allows you to edit IMS Emergency Session configurations.
23. Enter the values for the input fields, available under the group.
    The following table describes the fields:

Table 7-64 Edit IMS Emergency Session Configurations

Field Name	Description
Emergency DNNs	DNN included in the request from SMF to PCF to establish an emergency session.
Priority Level	Defines the relative importance of a resource request. **Default Value**: 1
Preemption Capability	Defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level. **Default Value**: MAY_PREEMPT
Preemption Vulnerability	Defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level. **Default Value**: NOT_PREEMPTABLE

24. Expand the **Audit** group.
    This group allows you to edit Audit configurations for **SM Policy Association**, **Pending Operation**, and **TDF Session** database tables.
25. Enter the values for the input fields, available under the **SM Policy Association** group.
    The following table describes the **SM Policy Association** fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-65 Edit SM Policy Association Configurations

Field Name	Description
Enabled	Determines whether to send registration request to Audit service or not. **Default Value**: True
Notification Rate (per second)	Defines the number of stale records which Audit service notifies to Session Management (SM) service in one second. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)
Policy Association Age (in minutes)	Defines the age of a SM policy association after which a record is considered to be stale on PCF and the SMF is queried for presence of such associations. **Default Value**: 1440
Policy Association Maximum Age (in minutes)	Defines the maximum age of a SM policy association after which a record is purged from PCF SM database without sending further queries to SM. **Default Value**: 2880
Minimum Audit Attempts	Specifies the minimum number of consecutive failed audit attempts until maxTTL / forceTTL is reached. If maxTTL is reached and audit_attempts + 1 >= Minimum Audit Attempts for maxTTL, Audit service sends notification to SM service with maxTTL flag set to *true*. SM Service sends DELETE request to PDS and Binding Service. **Range**: 0-99 **Default Value**: 0 **Note**: If maxTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until maxTTL is reached.
Minimum Audit Passes Interval (in minutes)	Defines the time when next audit for the SM service table is done after delta time if auditing this table has been finished before this specified time. **Default Value**: 10

26. Enter the values for the input fields, available under the **Pending Operation** group. The following table describes the **Pending Operation** fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-66 Edit Pending Operation Configurations

Field Name	Description
Notification Rate (per second)	Defines the number of pending operation records which Audit service notifies to Session Management (SM) service in one second. **Note:** The notification rate for all the operations of Audit service remains the same. Policy does not allow to configure different values for different operations. Therefore, by default the notification rate configured for the **SmPolicyAssociation** section applies for **Pending Operations**. **Default Value**: 50
Pending Operation Age (in minutes)	Defines the age of a pending operation after which a record is considered to be stale. This is a non modifiable field. **Default Value**: 0
Pending Operation Maximum Age	Defines the maximum age of a pending operation after which a record is purged from PCF SM database without sending further queries to SM. **Default Value**: 2880
Minimum Audit Passes Interval (in minutes)	Defines the frequency with which the Audit service performs audit of the pending operation table for the Retry Timestamps that have been reached. **Default Value**: 10
Alternate Site	The site takeover profile. For more information, see Site Takeover.
Enable Alternate Site	Specifies if the site takeover must be enabled in case of failure.

27. Enter the values for the input fields, available under the **TDF Session** group. The following table describes the fields:

Table 7-67 Edit TDF Session Configurations

Field Name	Description
Enabled	SM determines whether to send registration request to Audit service or not. **Default Value**: True
Query TDF	On true, SM sends a RAR request with Tdfsession toward TDF. On false, SM deletes the Tdfsession. **Default Value**: False
Notification Rate (per second)	Defines the number of TDF stale records which Audit service notifies to Session Management (SM) service in one second. **Default Value**: 50

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-67 (Cont.) Edit TDF Session Configurations

Field Name	Description
TDF Session Age (in minutes)	Defines the age of a TDF session after which a record is considered to be stale on PCF and the TDF is queried for presence of such associations. **Default Value**: 1440
TDF Session Maximum Age (in minutes)	Defines the maximum age of a TDF session after which a record is purged from TDF session table of SM database without sending further queries to TDF. **Default Value**: 2880
Minimum Audit Attempts	Specifies the minimum number of consecutive failed audit attempts until maxTTL / forceTTL is reached. If maxTTL is reached and audit_attempts + 1 >= Minimum Audit Attempts for maxTTL, Audit service sends notification to SM service with maxTTL flag set to *true*. SM Service deletes stale TDF Session from TdfSession table. If maxTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until maxTTL is reached. **Range**: 0-99 **Default Value**: 0
Minimum Audit Passes Interval (in minutes)	Defines the time frequency with which the Audit service performs audit for the stale sessions in TdfSession table. If the audit of TdfSession table is finished before this specified time, then next audit for this table happens after the delta time. **Default Value**: 10

28. Enter the values for the input fields, available under the **Pending Transaction** group. The following table describes the fields:

Table 7-68 Edit Pending Transaction Configurations

Field Name	Description
UpdateNotify Retry Backoff (in milliseconds)	Indicates the time between two consecutive retry UpdateNotify messages when UpdateNotify message is held back from being sent to SMF. The default value for this field is 1000.
UpdateNotify Retry Count	Indicates the count for UpdateNotify message to be retried when it is held back from sending to SMF. The default value for this field is 2.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-68 (Cont.) Edit Pending Transaction Configurations

Field Name	Description
Error Update Notify Handling Rx	On Update Notify to SMF triggered by Rx, this configuration decides if it should RETRY (with UpdateNotifyRetryBackoff and UpdateNotifyRetryCount settings) or DISCARD when receiving 400 Pending Transaction response from SMF. The default value for this field is DISCARD. The allowed values are: • DISCARD (0) • RETRY (1)
Error Update Notify Handling Subscription Notification	On Update Notify to SMF triggered by Subscriber Notification, this configuration decides if it should RETRY (with UpdateNotifyRetryBackoff and UpdateNotifyRetryCount settings) or DISCARD when receiving 400 Pending Transaction response from SMF. The default value for this field is RETRY. The allowed values are: • DISCARD (0) • RETRY (1)

> **Note**
>
> Enabling Audit to `true` under SM Policy Association will not enable the Pending Operation audit registration. In addition to that, you need to enable **BSF Binding Recreate Attempt** under **Binding Configuration** fields in the SM service configuration to activate the Audit for Pending Operation.

29. Under the **NWDAF** group, enable or disable the **Enable NWDAF Data** switch.
30. Perform the overload configuration Under **Overload Configuration** section:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-69 Overload Configuration

Field Name	Description
Enhanced Overload Control Level	Specifies the current status of the Enhanced Overload Control mechanism. It indicates whether advanced overload management features are active for this service. **Possible Values:** • DISABLED • L1 • L2 • L3 • L4 • L5 • L6 • L7 • L8 • L9 • L10 **Default Value:** Disabled **Note**: Setting one of these different control level to either 1, 2, 3..10 signifies that, if the configuration Control Level is set to L1, and the actual Load Level of SM service is either in L1 or above state (that is, L2 or L3), then only Enhanced Overload Actions will be applied. Similarly, if the Configuration control level is set to L2 and even if the service load Level of SM service is in L1 state, the Enhance Overload actions will not be applied. Once the system load level reaches L2, then the Overload actions will get applied. Similarly, if the configuration is in L3 state, then even if the SM service load level is in L1 or L2 state, enhance overload actions will not be performed.
Overload Configuration Profile	Specifies the name of the overload configuration profile assigned to this service. A profile includes specific rules for overload handling.

31. Configure the default processing profile under **Default Processing** section:

Table 7-70 Configuring Default Processing

Field Name	Description
SM Default Processing Profile	Select one of the default processing profiles created on **Default Processing Profile** page that must be applied for SM service.

32. Configure the Message Priority Profile under **Message Priority Profile** section:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-71 Configuring Message Priority Profile

Field Name	Description
Message Priority Profile	Select one of the message priority profiles created on **Message Profiles** page that must be applied for SM service. When a message profile is selected under **Message Priority Profile** section, support for `3GPP-SBI-Message-Priority` header gets enabled for SM service.

33. Perform the following steps to configure **Advanced Settings** that allows PCF to handle concurrent requests:

    a. Click the ⊕ Add
    The page opens the **Add Advanced Settings** dialog box.

    b. In the dialog box, enter the following **keys** and respective **values**:

The following table describes the keys and values:

Table 7-72 Add Advanced Settings Configurations

Key	Value
CONCURRENCY.LOCK_LEASE_DURATION_FOR_CREATE	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically.**Default value:** 6 seconds
CONCURRENCY.LOCK_WAIT_DURATION_FOR_CREATE	Duration by which the SM service waits for the response to get a lock.
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_CREATE	Number of attempts the service make to request the lock.
CONCURRENCY.BULWARK_ENABLED_FOR_N7_CREATE	Enables concurrency for create request. **Default value:** False
CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF	Defines the amount of time after which the service retries to gain the lock, in case of failure. **Default value:** 750ms
CONCURRENCY.LOCK_LEASE_DURATION_FOR_DELETE	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically.**Default value:** 6 seconds
CONCURRENCY.LOCK_WAIT_DURATION_FOR_N7_DELETE	Duration by which the SM service waits for the response to get a lock. **Default value:** 3 seconds
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_DELETE	Number of attempts the service make to request the lock. **Default value:** 3 seconds
CONCURRENCY.BULWARK_ENABLED_FOR_N7_DELETE	Specifies if the concurrency has to be enabled for the SM Delete requests. **Default value:** False
CONCURRENCY.LOCK_LEASE_DURATION_FOR_UPDATE	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically.**Default value:** 6 seconds

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.LOCK_WAIT_DURATION_FOR_UPDATE	Duration by which the SM service waits for the response to get a lock. **Default value:** 3 seconds
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_UPDATE	Number of attempts the service can make to request the lock. **Default value:** 3
CONCURRENCY.BULWARK_ENABLED_FOR_N7_UPDATE	Specifies if the concurrency has to be enabled for the SM Update requests. **Default value:** False
CONCURRENCY.LOCK_LEASE_DURATION_FOR_CLEANUP	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically.**Default value:** 6 seconds
CONCURRENCY.LOCK_WAIT_DURATION_FOR_CLEANUP	Duration by which the SM service waits for the response to get a lock. **Default value:** 3 seconds
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_CLEANUP	Number of attempts the service can make to request the lock. **Default value:** 3
CONCURRENCY.BULWARK_ENABLED_FOR_N7_CLEANUP	Specifies if the concurrency has to be enabled for the SM Clean requests. **Default value:** False
RESOURCEID.SUFFIX_LIST	Select a subscriber value type from the drop down for which the lock must be requested: • SUPI • GPSI
CONCURRENCY.LOCK_REQUEST_RETRY_BACKOFF	Defines the amount of time after which the service retries to gain the lock, in case of failure. **Default value:** 750ms
BINDING.BSF_REATTEMPT_THRESHOLD	Defines the frequency with which SM service calls the Audit service API for checking the **Pending Operation** threshold.
USER.RESET_CONTEXT_SM_POLICY_DATA_ON_SM_CREATE	If this configuration is enabled, the sm-service on receiving the sm-create for a SUPI, checks if there is no other `smPolicyAssociation` for the same SUPI and sets `resetContext` flag for the SM policy on the request towards PDS. **Default Value**: False
USER.RESET_CONTEXT_OSD_ON_SM_CREATE	If this configuration is enabled, the sm-service on receiving the sm-create for a SUPI, checks if there is no other `smPolicyAssociation` for the same SUPI and sets `resetContext` flag for the OSD on the request towards PDS. **Default Value**: False
USER.RESET_CONTEXT_CHF_DATA_ON_SM_CREATE	If this configuration is enabled, the sm-service on receiving the sm-create for a SUPI, checks if there is no other `smPolicyAssociation` for the same SUPI and sets `resetContext` flag for the CHF on the request towards PDS. **Default Value**: False

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
USER.RESET_CONTEXT_LDAP_DATA_ON_SM_CREATE	If this configuration is enabled, the sm-service on receiving the sm-create for a SUPI, checks if there is no other `smPolicyAssociation` for the same SUPI and sets `resetContext` flag for the LDAP on the request towards PDS. **Default Value**: False
USER.RESET_CONTEXT_SSV_ON_SM_CREATE	If this configuration is enabled, the sm-service on receiving the sm-create for a SUPI, checks if there is no other `smPolicyAssociation` for the same SUPI and sets `resetContext flag` for the SSV on the request towards PDS. **Default Value**: False
CONCURRENCY.LOCK_LEASE_DURATION_FOR_UPDATE_NOTIFY	Duration for which lock is held once it is acquired. After this duration, the lock will be released automatically. **Default Value**: 6 Seconds
CONCURRENCY.LOCK_WAIT_DURATION_FOR_UPDATE_NOTIFY	Duration for which the Policy service will wait for the response to get a lock. The same duration is used by Bulwark service to poll for the lock if a lock is not available. **Default Value**: 3 Seconds
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_UPDATE_NOTIFY	The number of retries when a request to Bulwark service fails. **Default Value**: 3
CONCURRENCY.BULWARK_ENABLED_FOR_N7_UPDATE_NOTIFY	Determines whether to enable Bulwark service for SM notification flow. **Default Value**: false
CONCURRENCY.UPDATE_USERDATA_IN_ASSOCIATION_ON_LOCKFAILURE	Facilitates the user to update user data in the database in the case of lock failure. **Default Value**: false
NWDAF.EVENT	Allow to add one or more Events to be send in the request towards NWDAF. **Default value**: SLICE_LOAD_LEVEL
NWDAF.REQUEST_TIMEOUT	Allow to control the timeout of the request from SM towards NWDAF. **Default value**: 3000 (ms)
SYSTEM.PA_MAX_APP_SESSIONS	Specifies the limit on the number of AppSessions per SM session. **Default value**: 4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
USER.excludeDnnSet.<dnnSetId>	Set of Data Network Names (DNNs) for which all the requests or sessions will be excluded for the specific User Data Types mentioned below. The DNN list can include the comma separated values. Regular expressions (regex) are allowed for the DNN names with the following conditions: • All white spaces are removed before processing values in the arrays. • The dnn exclude settings are case insensitive. • Every dnn contains regex characters '^' at the start and '$' at the end. The dnn can not be an empty string or it cannot be ignored. • For security reasons '\' (backslash) is not supported, to interpret regex conditions like '\d' it must be written as '/d', internally all '/' and is translated to '' for java to handle backslash regex conditions as desired. • { n, m } repetitions not supported as we use ',' to separate each dnn. Example: USER.excludeDnnSet.**dnnSet1** = **dnn1,dnn2**
USER.smPolicyData.excludeDnn.<Snssai>	Specify the Snssai corresponding to the DNNs for which all the requests or sessions are excluded for smPolicyData. Snssai corresponding to the DNN must be the dnnSetId configured in the key from USER.excludeDnnSet.<dnnSetId>. There is no regex applied to the snssai value. Example: USER.smPolicyData.excludeDnn.**snssai1** = **dnnSet1**
USER.ldapData.excludeDnn.<Snssai>	Specify the Snssai corresponding to the DNNs for which all the requests or sessions are excluded for the given Ldap Data. Example: USER.ldapData.excludeDnn.**snssai1** = **dnnSet1**
USER.operatorSpecificData.excludeDnn.<Snssai>	Specify the Snssai corresponding to the DNNs for which all the requests or sessions are excluded for the given Operator Specific Data. Example: USER.operatorSpecificData.excludeDnn.**snssai1** = **dnnSet1**
USER.chfData.excludeDnn.<Snssai>	Specify the Snssai corresponding to the DNNs for which all the requests or sessions are excluded for the given CHF Data. Example: USER.chfData.excludeDnn.**snssai1** = **dnnSet1**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
USER.ocsData.excludeDnn.<Snssai>	Specify the Snssai corresponding to the DNNs for which all the requests or sessions are excluded for the given OCS Data. Example: USER.ocsData.excludeDnn.**snssai1** = **dnnSet1**
USER.ssv.excludeDnn.<Snssai>	Specify the Snssai corresponding to the DNNs for which all the requests or sessions are excluded for the given SSV Data. Example: USER.ssv.excludeDnn.**snssai1** = **dnnSet1**
USER.CREATE_CONTEXT_ON_FAILURE_OCS_DATA	When the value of this key is true, PCRF core sends this flag as part request parameters to PDS. PDS creates a dummy context for OCS in case of getting error while performing OCS lookup. This will support the PDS when it receives notificaiton from UDR to fetch OCS data. This is applicable for SM Create and SM Update. This is applicable for SmCreate and SmUpdate with Asynchronous flow either set as true or false. **Default Value**: false
SYSTEM.SMF_MAX_WAIT_DURATION_FOR_DELETE	Specify the wait time for SMF to trigger delete request on receiving successful response for terminateNotify request. The allowed value range from 0 to 30000 milliseconds. **Note**: If value is either less than 0ms or more than 30000ms, by default 30000ms is considered. The default value for this parameter is 30000ms.
USE_TGPP_SBI_MSG_PRIORITY	Specify the use of `3gpp-sbi-message-priority` header for lock requests. Allowed values are `true` or `false`. **Default value**: true
REQUEST_PRIORITY_FOR_SM_DELETE	Specify the setting request priority for delete requests. Allowed integer number ranging from 0-100. **Default value**: 16
REQUEST_PRIORITY_FOR_SM_UPDATE	Specify the setting request priority for update requests. Allowed integer number ranging from 0-100. **Default value**: 18
REQUEST_PRIORITY_FOR_SM_UPDATE_NOTIFY	Specify the setting request priority for update notify requests. Allowed integer number ranging from 0-100. **Default value**: 18
REQUEST_PRIORITY_FOR_SM_CLEANUP	Specify the setting request priority for cleanup requests. Allowed integer number ranging from 0-100. **Default value**: 18

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
REQUEST_PRIORITY_FOR_SM_CREATE	Specify the setting request priority for cleanup requests. Allowed integer number ranging from 0-100. **Default value**: 24
ENABLE_SM_POLICY_ASSOCIATION_TABLE_SLICING	Indicates whether to enable/disable the database operations on sliced tables. That is, whenever ENABLE_SM_POLICY_ASSOCIATION_TABLE_SLICING flag is set to `true`, the create/retrieve/update/delete operations are performed on the database slices instead of the main database. **Default value**: false
TABLE_SLICING.SM_POLICY_ASSOCIATION.ENABLED	Indicates whether to enable/disable the table slicing for SmPolicyAssociation. **Default value**: false
TABLE_SLICING.SM_POLICY_ASSOCIATION.READ.ENABLED	when the value is true, the table slicing will be active for all DB read operations specifically. Note: This key will only be enabled when the TABLE_SLICING.SM_POLICY_ASSOCIATION.ENABLED key is set to true. **Default value**: true
TABLE_SLICING.SM_POLICY_ASSOCIATION.WRITE.ENABLED	when the value is true, the table slicing will be active for all DB Write operations specifically. Note: This key will only be enabled when the TABLE_SLICING.SM_POLICY_ASSOCIATION.ENABLED key is set to true. **Default value**: true
AUDIT_SMPOLICY_ASSOCIATION.MAX_TTL.TERMINATE_NOTIFY.ENABLED	When SM service receives a MaxTTL notification from Audit service, and if the value of this advanced settings key is set to `true`, SM service sends Terminate Notify to SMF. **Default value**: false
SYSTEM.COLLISION_DETECTION.TERMINATE_NOTIFY.ENABLED	When a collision is detected and the existing session is older than the new one, and if the value of this advanced settings key is set to `true`, SM service sends TerminateNotify to SMF. **Default value**: false
AUDIT.HTTP2_ENABLED	Determines whether to use http/2 or http/1.1 to communicate with Audit service for threshold polling task. Possible values: • true: http/2 is used to communicate with Audit service • false: http/1.1 is used to communicate with Audit service **Default value**: true

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
USER.CREATE_CONTEXT_ON_FAILURE_SM_POLICY_DATA	If this flag is enabled the SM service sends this as a request parameter toward PDS. At PDS, if it receives an error during SmPolicyData-UDR lookup, then PDS creates a dummy context for SmPolicyData. This creation of dummy context helps, when PDS receives next request for a UDR lookup and this time it is successful, then both the sessions will have the latest SmPolicyData. This is applicable for SmCreate and SmUpdate. **Default value**: false
USER.CREATE_CONTEXT_ON_FAILURE_CHF_DATA	If this flag is enabled the SM service sends this as a request parameter toward PDS. PDS creates a dummy context for CHF in case of getting error while performing CHF lookup. This creation of dummy context helps, when PDS receive next request for a CHF lookup and this time it is successful, then both the sessions will have the latest information. This is applicable for SmCreate and SmUpdate with Asynchronous flow either set as true or false. **Default value**: false
USER.CREATE_CONTEXT_ON_FAILURE_OPERATOR_SPECIFIC_DATA	If this flag is enabled the SM service sends this as a request parameter toward PDS. At PDS, if it receives an error during operatorSpecificData-UDR lookup, then PDS creates a dummy context for operatorSpecificData. This creation of dummy context helps, when PDS receives next request for a UDR lookup and this time it is successful, then both the sessions will have the latest operatorSpecificData. This is applicable for SmCreate and SmUpdate. **Default value**: false
RULE.ENABLE_PCC_RULE_REMOVE_ON_FAILURE	If this flag is enabled and the updatenotify request fails for PCC rule remove with any HTTP error, then the association will be updated with rule removed. **Default value**: false
ENABLE_LATE_PROCESSING	Indicates whether the stale request cleanup functionality for SM service is enabled or disabled. To enable the stale request cleanup functionality for SM service, set the value of this key to `true`. **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
USER.allDataTypes.excludeDnns	Specifies the comma separated list of DNNs. For any request that matches one of the DNNs in the list, the communication with PDS is excluded. Regular expressions (regex) are applied as supported by regex from java Pattern class with the following special cases: • All white spaces should be removed before processing any values in the arrays. • Every dnn should contain regex characters '^' at the start and '$' at the end. The dnn can not be an empty string. • dnn exclude settings are case insensitive. • For security reasons '\' (backslash) is not supported, to interpret regex conditions like '\d' it must be written as '/d',. Internally all '/' are translated to '\' for java to handle backslash regex conditions. • { n, m } repetitions are not supported as ',' they are used to separate each dnn. Example: USER.allDataTypes.excludeDnns = dnn1,dnn2
BINDING.excludeDnns	Specifies the comma separated list of DNNs. For any request that matches one of the DNNs in the list, the communication with Binding Service will be excluded. Regular expressions (regex) are applied as supported by regex from java Pattern class with the following special cases: • All white spaces should be removed before processing any values in the arrays. • Every dnn should contain regex characters '^' at the start and '$' at the end. The dnn can not be an empty string. • dnn exclude settings are case insensitive • For security reasons '\' (backslash) is not supported, to interpret regex conditions like '\d' it will need to be written as '/d',. Internally all '/' will be translated to '\' for java to handle backslash regex conditions. • { n, m } repetitions are not supported as ',' will be used to separate each dnn.
BINDING.FORCE_DELETE_ENABLED	Indicates whether to check if pcfBinding is in SmPolicyAssociation or to skip this validation and always send the ContextBinding Delete operation. By default the value is **true**, so it skips the validation and sends the delete as it is.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.LOCK_RETRY_MODE	Indicates whether the lock retry must be triggered under SM service. Possible values are: • **CLIENT_ONLY**: lock retry is triggered only in client services. • **SERVER_ONLY**: lock retry is triggered only in bulwark. • **CLIENT_AND_SERVER**: lock retry is triggered by both server and client.(server will retry to acquire the lock till the lockWaitTimeout is expired and client will retry after the configured request backOff timer is expired) • Consumer services's advance settings should be updated with the non-zero lockWaitTimeOut.
BULWARK.excludeDnns	Specifies the comma separated list of DNNs. For any request that matches one of the DNNs in the list, the communication with Bulwark Service will be excluded. Regular expressions (regex) are applied as supported by regex from java Pattern class with the following special cases: • All white spaces should be removed before processing any values in the arrays. • Every dnn should contain regex characters '^' at the start and '$' at the end. The dnn can not be an empty string. • dnn exclude settings are case insensitive • For security reasons '\' (backslash) is not supported, to interpret regex conditions like '\d' it will need to be written as '/d',. Internally all '/' will be translated to '\' for java to handle backslash regex conditions. • { n, m } repetitions are not supported as ',' will be used to separate each dnn.
SYSTEM.ENABLE_CLEANUP_DELAY_AFTER_FAILED_REQUEST	During SM create, when a request is rejected or there is an exception, this flag lets the user decide if unsubscribe request to UDR and CHF should be send immediately or after a certain delay. **Default value**: false
SYSTEM.CLEANUP_DELAY_AFTER_FAILED_REQUEST	When there is a delay on unsubscribe request after failure flag is enabled, this flag lets the user configure the delay before sending unsubscribe request to UDR and CHF. The value of this flag is in milliseconds. **Default value**: 2000

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
SYSTEM.ENABLE_APP_SESSION_INFO_CLEANUP_ON_DATA_TRUNCATION	When this flag is enable, while saving the SmPolicyAssociation for SMUpdate or SMUpdateNotify flows, if `SQL DataTruncation` exception happens, all of the oldest AppSessions related to the SmPolicyAssociation which are beyond the SYSTEM.PA_MAX_APP_SESSIONS limit will be cleaned up in X ms intervals (interval configured using SYSTEM.APP_SESSION_INFO_CLEANUP_DELAY_ON_DATA_TRUNCATION). This action cleans up the AppSessionInfo and the related pcc rules, sending SMF Update Notify if needed, and deleting directly the corresponding AppSessions from the database if present. **Default value:** false
SYSTEM.APP_SESSION_INFO_CLEANUP_DELAY_ON_DATA_TRUNCATION	Defines in milliseconds the time interval between each AppSessionInfo cleanup execution when SYSTEM.ENABLE_APP_SESSION_INFO_CLEANUP_ON_DATA_TRUNCATION takes action. **Default value:** 1000
SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED	Determines whether to enable or disable handling collision between AAR and STR messages during update notify timeout. When the value of this advanced settings key is set to `true`, PCF handles the collision between AAR-I, AAR-U, and STR as explained in Handling Collision Between AAR and STR Messages During Update Notify Timeout. **Default value**: false
SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.PROCESS_ON_UPDATE	When the value of this advanced settings key is set to `true`, PccRules with pendingConfirmation flag are sent to re-install during AAR-U. **Default value**: false
SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPONSE_CODES	The value of this key indicates that the Update Notify errors are handled as success and pccRules are saved as pendingConfirmation on AAR-I and AAR-U. **Default value**: 408
SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS	When the value of this advanced settings key is set to `true`, Update Notify exception will be handled as success and pccRules are saved as pendingConfirmation on AAR-I and AAR-U. **Default value**: java.util.concurrent.TimeoutException,java.util.concurrent.CancellationException
TDF.TDF_ENABLED	When this key is added and set to true, the N7-Sd feature in SM service is enabled.
SYSTEM.SMF_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-72 (Cont.) Add Advanced Settings Configurations

Key	Value
USER.SERVICE_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
BINDING.CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
RULE.SET_PACKETFILTERUSAGE_TRUE_FOR_FINALSERVICEINFO	This setting allows the user to enable the *packetFilterUsage* to be sent with `true` during request update notification to be sent to SMF when the main request has the value FINAL in `serviceInfoStatus` field. If the main request does not specify any value for `serviceInfoStatus` field, the SM service sets its value as *FINAL*, which may impact the user if it is set to `true`. **Note**: If the *setPacketFilterUsageToTrueForPreliminaryServiceInfo* is set to `false` in the version prior to 25.1.200, then the user needs to set RULE.SET_PACKETFILTERUSAGE_TRUE_FOR_FINALSERVICEINFO to `true` for a consistent behavior. **Default value**: false
ERROR_CODE_LIST_TO_BYPASS_BULWARK	This setting allows the user to process the message when all attempts to acquire the lock is exhausted. **Examples**: 423,503,500
SYSTEM.SEND_UMC_DATA_WHEN_NOT_SUPPORTED_BY_SMF	Indicates whether to send Usage Monitoring data to SMF when receiving the usage thresholds from the AF/NEF, for Monitoring the Sponsored Data Connectivity but UMC is not supported by the SMF. **Default value**: false
POLICY.PRE_RETRY_COUNT	Indicates the number of attempts the service can make to connect to PRE. **Default value**: 1
POLICY.PRE_RETRY_BACKOFF_DURATION_MILISEC	Indicates the amount of time in milliseconds after which the service retries to connect to PRE, in case of failure. **Default value**: 5 ms
POLICY.PRE_RETRY_RESPONSE_CODES	Comma separated list which determines for which response codes, PRE request will be retried. **Default value**: 408, 500, 503
POLICY.PRE_RETRY_EXCEPTIONS	Comma separated list which determines for which exceptions, PRE request will be retried. **Default value**: java.net.UnknownHostException, java.net.ConnectException, java.io.IOException, java.io.EOFException

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-73 Add Advanced Settings Configurations

Key	Value
SM.TDF.SESSION.DELETE.PRIORITY	Delete Tdf Session (Sd CCR-T). **Allowed Values**: 0-31 **Default Value**: 16
SM.TDF.SESSION.UPDATE.PRIORITY	Update Tdf Session (Sd CCR-U). **Allowed Values**: 0-31 **Default Value**: 18
SM.UPDATE.EVENT.SUBS.PRIORITY	Set request priority for creation or modification of an event subscription request. **Allowed Values**: 0-31 **Default Value**: 18
SM.CREATE.PRIORITY	Set request priority for SM create request. **Allowed Values**: 0-31 **Default Value**: 24
SM.SUB.FAIL.NOTIFY.PRIORITY	Set request priority for UDR subscription failure notification request. **Allowed Values**: 0-31 **Default Value**: 26
SM.USER.SERVICE.NOTIFY.PRIORITY	Set request priority for User Data change notification request. **Allowed Values**: 0-31 **Default Value**: 18
SM.UPDATE_PRIORITY	Set request priority for SM update request. **Allowed Values**: 0-31 **Default Value**: 18
SM.REAUTH_PRIORITY	Set request priority for SM reauthorization request. **Allowed Values**: 0-31 **Default Value**: 20
SM.DELETE.PRIORITY	Set request priority for SM delete request. **Allowed Values**: 0-31 **Default Value**: 16
SM.POLICY.CLEANUP.PRIORITY	Set request priority for clean up SM policies request. **Allowed Values**: 0-31 **Default Value**: 20
SM.APP.SESSION.CREATE.PRIORITY	Set request priority for Policy authorization create request. **Allowed Values**: 0-31 **Default Value**: 24
SM.APP.SESSION.DELETE.PRIORITY	Set request priority for Policy authorization delete request. **Allowed Values**: 0-31 **Default Value**: 16
SM.APP.SESSION.CLEANUP.PRIORITY	Set request priority for cleanup App sessions request. **Allowed Values**: 0-31 **Default Value**: 20

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-73 (Cont.) Add Advanced Settings Configurations

Key	Value
SM.AUDIT.NOTIFY.PRIORITY	Set request priority for Audit notification request. **Allowed Values**: 0-31 **Default Value**: 30
SM.GET.APP.SESSION.PRIORITY	Set request priority for Retrieve App Session request. **Allowed Values**: 0-31 **Default Value**: 28
SM.GET.ASSOC.PRIORITY	Set request priority for retrieve Policy association request. **Allowed Values**: 0-31 **Default Value**: 28
SM.GET.SUBSCRIBER.SESSIONS.PRIORITY	Set request priority configured retrieve any type of session for rest api endpoint. **Allowed Values**: 0-31 **Default Value**: 28
SM.GET.ASSOC.QUERY.PRIORITY	Set request priority for advanced search of Policy Association request. **Allowed Values**: 0-31 **Default Value**: 28
SM.PDS.LOCATION.INFO.NOTIFY.PRIORITY	To set the request priority of the request that updates `pds_loc_info` in SM service database. **Allowed Values**: 0-31 **Default Value**: 30
CONGESTION_RESPONSE_CODE	Configure the response code of any rejected requests by SM service due to congestion state. By default, SM service sends 503 as response code. If configured then it shall be 5xx only. **Allowed Values**: 503 **Default Value**: 5xx
ENABLE_N7_SESSION_LOOKUP_COOKIE	Determines whether to enable or disable the support for optimizing N7 session lookup for AAR-I messages in Rx callflows at SM service. Possible values: • true (to enable the feature) • false (to disable the feature) If this key is enabled: • During SM Create: If BSF is enabled, `ocnf-service-header` cookie is sent towards Binding service and also towards BSF. If BSF is disabled, `ocnf-service-header` is sent towards Binding service. • Primary key lookup happens when PA request is received by SM Service with `ocnf-service-header` in the header. **Default value:** false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-73 (Cont.) Add Advanced Settings Configurations

Key	Value
MSG_PROCESSING_DEFAULTS.ENABLED_ON_PRE_FAILURE	Determines if the default PCC rules and session rules configured using Default Processing Profile must be applied on Session creation in case of PRE failure (non 2xx response / exceptions). Possible values: • true • false When the value of this key is configured to `true`, the Defaults Processing Profile configured rules is applied in case of PRE failure.
SAVE_SRC_SERV_INST	This flag indicates whether to save the source service instance in the SmPolicy association database. This flag takes effect only when the global flag `ENABLE_NF_PEER_INFO` is enabled. **Default Value**: false
BINDING.DEPENDENTCONTEXTBINDING_PROCESSING	This value is used with the `POLICY_DEPLOYMENT_MODE` environment value to determine whether `dependentContextBinding` is created or deleted by calling the binding service. **Default Value**: true

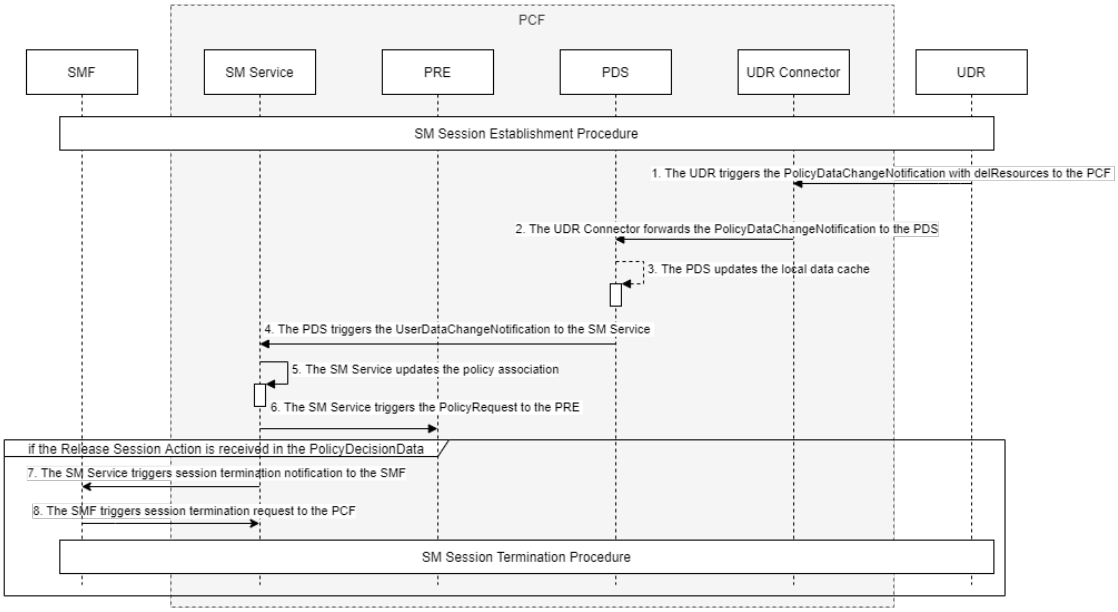
34. Click **Save** to save the PCF Session Management configurations.

7.3.2.1 UDR Subscriber Delete Resource Support

The PCF call flow has been updated to support terminating an active subscriber session by the deployed policy when the subscriber resources are deleted on the UDR.

The following figure describes a call flow for UDR subscriber resource deletion:

Figure 7-17 Call Flow for UDR Subscriber Resource Deletion



Copyright © 2019, 2026, Oracle and/or its affiliates.

The call flow consists of the following tasks:

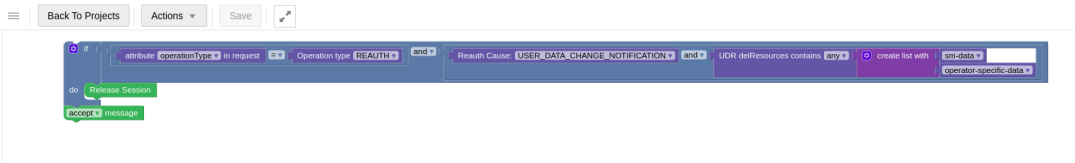
1. The UDR triggers the PolicyDataChangeNotification with the attribute "delResources" to the PCF.
2. The UDR connector forwards the received PolicyDataChangeNotification to the PDS.
3. After receiving the UDR notification, PDS calls UDR-Notify workflow, in this workflow, PDS compares the PolicyDataChangeNotification with the existing data in database and perform database update or delete, if needed, and notify the SM service (with the attribute "delResources"), if needed.
   If delResources exists in PolicyDataChangeNotification and the delResources URL meet the condition "contains '/policy-data/ues/{ueId}/operator-specific-data' or 'policy-data/ues/{ueId}/sm-data/' ", the existing subscriber information in database is be deleted.
4. After the data updates, the PDS triggers an UserDataChangeNotification with received PolicyDataChangeNotification to the SM service.
5. The related resources (smPolicyData or operatorSpecificData) within the SmPolicyAssociation are deleted when the delResources of the PolicyDataChangeNotification is received.
   The smPolicyData is deleted if the resource URL contains "sm-data".

   The operatorSpecificData is deleted if the resource URL contains "operator-specific-data".

   > **Note**
   >
   > Policy does not support recieving *opSpecData* in the PolicyDataChangeNotification.

6. The SM Service triggers the PolicyRequest with the UserDataChangeNotification to the PRE to get the PolicyDecisionData, if the "Release Session" action is received, Step 7 is triggered. New conditions and action have been added to support this.
   For more information on these conditions and action, see **PCF-SM Category** section in *Oracle Communcations Cloud Native Core, Converged Policy Design Guide*.

   The following screen capture illustrates an example of how to use these conditions and action to release a policy association:

7. The SM Service triggers session termination notification to the SMF if the "Release Session" action is received in the PolicyDecisionData.
8. The SMF triggers a session termination request to the PCF.

7.3.3 PCF Access and Mobility

This procedure provides information about configuring the Access and Mobility Service.

The **Access and Mobility** page displays the AM Service configurations. The page allows you to edit the configurations.

To configure the PCF Access and Mobility service:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the navigation menu under **Policy**, navigate to **Service Configurations** and select **PCF Access and Mobility**.
   This opens the **PCF Access and Mobility** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **PCF Access and Mobility** page.
3. Check the default configuration for the fields available in respective groups and edit as necessary.
   The following table describes the fields along with their valid input values under each group:

Table 7-74 Edit PCF Access and Mobility

Field Name	Description
System	Provide System details:
AMF Notification Retry Profile	Defines the retry profile configuration for Access and Mobility service. For more information about configuring retry profile, see Retry Profiles.
AMF Communication Profile	Specifies the NF communication profile used by AMF. For more information about configuring NF communication profiles, see NF Communication Profiles.
Enable Max Session Limit	Specifies whether to enable the Limiting the Number of Sessions functionality.
Max Session Limit Per User	Specifies the maximum number of sessions to be limited per user if **Enable Max Session Limit** flag is enabled. Range: 1-2 Default value: 1
Override Supported Features	Indicates a list of supported features that can be configured to override system embedded values. For example: • PendingTransaction • DNNReplacementControl • SliceSupport
Data Compression Scheme	Specifies the data compression scheme used by AM. Following are the allowed values for this field: • Disabled • MySQL_Compressed • Application Compressed By default, this value remains disabled.
User	Provide User details:
Validate User	When this button is enabled , and the subscriber is not found in the UDR, or PCF is not able to query an available/eligible UDR, PCF sends an HTTP '400 USER_UNKNOWN' error to AMF. However, when you disable Validate User button, PCF continues policy processing even after the subscriber is not found in the UDR, or PCF is unable to query an available/eligible UDR. Default value: false.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-74 (Cont.) Edit PCF Access and Mobility

Field Name	Description
Enable Subscriber State Variables	If this switch is enabled, AM Service controls the querying and saving of local and remote subscriber state variables (SSV) on PDS. Default value: false.
User Data Types	Provide User Data Types details:
AMPolicyData	If this switch is enabled, PCF fetches AMPolicyData from nUDR. For information on configuring AMPolicyData attributes, see **AMPolicyData Attributes table.**
CHF Data	If this switch is enabled, PCF fetches policy counters from CHF. For information on configuring CHF Data attributes, see **CHF Attributes table.**
AMPolicyData Attributes	Provide AMPolicyData Attributes details:
Subscribe to Notify	When **Subscribe to Notify** field is enabled, Policy subscribes with the UDR to receive notifications whenever a change is made to a subscriber profile. Further, AM service notifies PDS, which in turn looks for an existing subscription for that subscriber and do any of the following: • If a subscription already exists and `monitoredResourceUris` already contains "am-data", no action is taken by PDS. • If a subscription does not exist, PDS subscribes with the UDR using the POST method with monitoredResourceUris set to "am-data". By default, this option is disabled.
Query User on Create	When this parameter is enabled (default behavior), PDS queries the UDR about the subscriber contained in the AM Association create request. It is done by sending a GET request for "am-data" resource on the nudr-dr service. **Note:** If you enable the **Subscribe to Notify** parameter for AM service configurations, the Policy service may look up for the requested subscriber profile in its local cache before querying UDR. By default, this option is enabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-74 (Cont.) Edit PCF Access and Mobility

Field Name	Description
Query User on Update	When this parameter is enabled, PDS queries the UDR about the subscriber present in the AM Association update request by sending a GET request for “am-data” resource on the nudr-dr service. By default, this parameter is disabled. **Note**: If you enable the `Subscribe To Notify` flag for AM service configurations, the Policy service may look up for the requested subscriber profile in its local cache before querying UDR. When the `Subscribe To Notify` flag is enabled and previous subscription attempts failed, then along with the data query, PDS also sends a SUBSCRIBE request to UDR.
Query User on Terminate	When this parameter is enabled, PDS queries the UDR about the subscriber present in the AM Association delete request by sending a GET request for “am-data” resource on the nudr-dr service. **Note:** If you have enabled **Subscribe to Notify** button for AM service configurations, the PCF user service may look up for the requested subscriber profile in its local cache before querying UDR. By default, this button is disabled. **Note** It should be enabled only when subscription to UDR is disabled. It should not be enabled if subscription to UDR is enabled.
CHF Data Attributes	Provide CHF Data Attributes details:
CHF Data	If this switch is enabled, PCF fetches policy counters from CHF.
Async CHF Query Enabled	When this button is enabled, PCF interacts with CHF in Asynchronous mode.
Policy	Provide Policy details:
Evaluate	This determines if policy evaluate is enabled. By default, this button is enabled.
Rules	Provide Rules details:
Default Service Area Restriction	This field shows the default Service Area Restriction (SAR). To update your default Service Area Restriction, click **Edit** and select any one from the drop-down list of preconfigured SARs. For more information on how to create or configure SAR, see Service Area Restriction.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-74 (Cont.) Edit PCF Access and Mobility

Field Name	Description
Default RFSP Index	The RFSP Index refers to a particular UE information used locally by the Access Network for implementing specific radio resource management strategies. This field shows the default value for RFSP Index, which can be a number between 1 and 256.
Default Triggers	This field shows the default triggers. To update the default triggers, click **Edit** and select desired value(s) from drop-down list values. The supported values are: • LOC_CH, that is, change in location • PRA_CH, that is, change of UE presence in PRA • ALLOWED_NSSAI_CH • SMF_SELECT_CH
Audit	Provide Audit details:
Enabled	Determines whether to send registration request to Audit service or not. **Default Value**: True
Query AMF	When the Query AMF flag is set to **false**, the AM Service will terminate the session as soon as it is marked as stale by the Audit Service, without waiting for the maximum TTL (maxTTL) to expire. • If Query AMF is **false**, the session is removed immediately after it is detected as stale. • If Query AMF is **true**, the session will only be terminated after validation with the AMF, or once maxTTL is reached.
Notification Rate (per second)	Defines the number of stale records which Audit service notifies to AM service in one second. Value of this parameter ranges between 20 and 700. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)
Policy Association Age (in minutes)	Defines the age of an AM policy association after which a record is considered to be stale on PCF and the AMF is queried for presence of such associations. Value of this parameter ranges between 1 and 10080. **Default Value**: 1440
Policy Association Maximum Age (in minutes)	Defines the maximum age of an AM policy association after which a record is purged from PCF AM d Value of this parameter ranges between 1 and 20160. **Default Value**: 2880

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-74 (Cont.) Edit PCF Access and Mobility

Field Name	Description
Minimum Audit Attempts	Specifies the minimum number of consecutive failed audit attempts until maxTTL / forceTTL is reached. If maxTTL is reached and audit_attempts >= Minimum Audit Attempts for maxTTL, Audit service sends notification to AM service with maxTTL flag set to *true*. AM Service sends DELETE request to PDS. **Range**: 0-255 **Default Value**: 0 **Note**: If maxTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until maxTTL is reached.
Minimum Audit Passes Interval (in minutes)	Defines the time when next audit for the AM service table begins after delta time if auditing this table has been finished before this specified time. **Default Value**: 330
Pending Transaction	Provide Pending Transaction details:
UpdateNotify Retry Backoff (in milliseconds)	Defines the retry backoff for UpdateNotify in milliseconds. **Default Value**: 0 - 10000 milliseconds
UpdateNotify Retry Count	Defines the total number of retries for UpdateNotify. **Default Value**: 0 - 5

4. Perform the following steps to configure **Advanced Settings**:

   a. Click ⊕ Add
   The page opens the **Add Advanced Settings** dialog box.

   b. In the dialog box, enter the following **keys** and respective **values**:

The following table describes the keys and values:

Table 7-75 Add Advanced Settings Configurations

Key	Value
CONCURRENCY.BULWARK_SERVICE_ENABLED	Enables the communication to Bulwark service, if it is set to true. **Default value**: False
CONCURRENCY.N15.UPDATE.LOCK_LEASE_DURATION	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically. **Default value**: 2000
CONCURRENCY.N15.UPDATE.LOCK_WAIT_DURATION	Duration by which the UE service waits for the response to get a lock. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-75 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_COUNT	Number of attempts the service make to request the lock. **Default value**: 2
CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_BACKOFF	Defines the amount of time after which the service retries to gain the lock, in case of failure. **Default value**: 1000
CONCURRENCY.N15.UPDATE	Enables the communication to Bulwark service during UPDATE request flow. **Default value**: False
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_LEASE_DURATION	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically. **Default value**: 2000
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_WAIT_DURATION	Duration for which the Policy service will wait for the response. **Default value**: 0
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_COUNT	Number of attempts the service can make to request the lock. **Default value**: 2
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_BACKOFF	Number of retries to acquire the lock upon Failure response from Bulwark service for such a request. **Default value**: 1000
CONCURRENCY.N15.UPDATE_NOTIFY	Enables the communication to Bulwark service during update-notify request flow. **Default value**: False
BULWARK.SERVICE_CONNECTION_TIMEOUT	Allows to control the connection timeout of a Bulwark service. **Default value**: 3000
PENDING_TRANSACTION.NOTIFICATION_ERROR_HANDLING_APP	Allows to notify the pending transactions. **Default value**: 1
USER.RESET_CONTEXT_CHF_DATA_ON_AM_CREATE	Sets resetContext flag for the CHF on the request towards PDS. **Default value**: false
USER.RESET_CONTEXT_AM_POLICY_DATA_ON_AM_CREATE	Sets resetContext flag for the AM policy on the request towards PDS. **Default value**: false
CONCURRENCY.BULWARK_SERVICE_ENABLED	Enables the concurrency functionality. **Default value**: false
CONCURRENCY.N15.CREATE.ENABLED	Enables concurrency feature for AM-create call flow. **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-75 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.N15.CREATE.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.CREATE.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0
CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_COUNT	Wait time out for lock acquisition if not acquired. **Default value**: 2
CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Update flow. **Default value**: 1000
CONCURRENCY.N15.TERMINATE.ENABLED	Enables concurrency feature for AM-Delete call flow. **Default value**: false
CONCURRENCY.N15.TERMINATE.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Delete flow. **Default value**: 1000
CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.TERMINATE.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0
CONCURRENCY.N15.UPDATE.ENABLED	Enable concurrency feature for AM-Update call flow. **Default value**: false
CONCURRENCY.N15.UPDATE.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Update flow. **Default value**: 1000
CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.UPDATE.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-75 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.N15.UPDATE_NOTIFY.ENABLED	Enable concurrency feature for AM-Update-Notify call flow. **Default value**: false
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Update Notify flow. **Default value**: 1000
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0
CONCURRENCY.N15.CLEANUP.ENABLED	Enables concurrency feature for AM-Cleanup call flow. **Default value**: false
CONCURRENCY.N15.CLEANUP.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.CLEANUP.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Cleanup flow. **Default value**: 1000
CONCURRENCY.N15.CLEANUP.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.CLEANUP.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 3000
CONCURRENCY.N15.CLEANUP.ALLOW_ON_SERVICE_FAILURE	If bulwark lock is not obtained after all retries for the AM Cleanup flow, then if enabled, the request will continue, if disabled the request will be rejected. **Default value**: true

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-75 (Cont.) Add Advanced Settings Configurations

Key	Value
RESOURCEID.SUFFIXLIST	This flag will tell PCF which resource ID will be used to do bulwark lock for concurrency feature. The supported values are SUPI and GPSI. In case no value is configured or only GPSI is configured, then SUPI will be the default value. When configuring both SUPI and GPSI, values should be separated by a comma. For example: SUPI,GPSI or GPSI,SUPI. **Note**: If ENABLE.ASSOCIATION.ENCODING flag is enabled, the configured values in this flag will be added to the encoded section of the association ID. **Default value**: SUPI

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-75 (Cont.) Add Advanced Settings Configurations

Key	Value
ENABLE.ASSOCIATIONID.ENCODING	Enables the encoding of the Association ID in the format: `AMPolicyAssociationId_versionNoNumberOfEncodedDataEncoded(tlvFormat)` where: **versionNo**: This value indicates the encoding version being used. The version number starts from 1. It ensures compatibility with the existing encoding for base64 encryption. **Number of Encoded Data**: This number represents how much information is stored within the encrypted string. For example, the number of encoded data will be 01 for SUPI, 02 for both SUPI and GPSI, and the number will increment in case of more encrypted string: **encoded**: This value is limited to 99 different values in Tag Length Value (TLV) format. For an example, decoded value as 220imsi-450081000000001. Here, SUPI is identified with tag 2 followed by string length (20) and then the value. **value**: is key value pair of ***SUPI/GPSI*** **Default value**: false The encoding will have information for the currently supported features: • Table slicing • SUPI • GPSI • Pending transaction **Note**: When table slicing is enabled, the encoded information for table slicing will be added to association Id irrespective of the value in this flag.
PDS_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
AMF_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-75 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.N15.CREATE.ALLOW_ON_SERVICE_FAILURE	If the flag is set to true, the AM Create request is allowed to be processed further even after all the lock acquisition retries with Bulwark Service end up with an error. If this flag is set to false, the AM Create request is responded with 500 Internal Service Error, when all the lock acquisition retries with Bulwark Service end up with an error. **Default value**: true
CONCURRENCY.N15.UPDATE.ALLOW_ON_SERVICE_FAILURE	If the flag is set to true, the AM Update request is allowed to be processed further even after all the lock acquisition retries with Bulwark Service end up with an error. If this flag is set to false, the AM Update request is responded with 500 Internal Service Error, when all the lock acquisition retries with Bulwark Service end up with an error. **Default value**: true
CONCURRENCY.N15.UPDATE_NOTIFY.ALLOW_ON_SERVICE_FAILURE	If the flag is set to true, the AM Update Notify and Update Terminate requests are allowed to be processed further even after all the lock acquisition retries with Bulwark Service end up with an error. If this flag is set to false, the AM Update Notify and Update Terminate requests are responded with 500 Internal Service Error, when all the lock acquisition retries with Bulwark Service end up with an error. **Default value**: true
CONCURRENCY.N15.TERMINATE.ALLOW_ON_SERVICE_FAILURE	If the flag is set to true, the AM Terminate request is allowed to be processed further even after all the lock acquisition retries with Bulwark Service end up with an error. If this flag is set to false, the AM Terminate request is responded with 500 Internal Service Error, when all the lock acquisition retries with Bulwark Service end up with an error. **Default value**: true

The following table describes the keys and values to be added to support congestion control:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-76 Add Advanced Settings Configurations

Key	Value
AM_GET_SUBSCRIBER_SESSIONS_REQUEST_PRIORITY	Retrieve any type of AM Policy association: /npcf-am-policy-control/v1/sessions **Allowed Values**: 0-31 **Default Value**: 28
AM_CREATE_REQUEST_PRIORITY	Create a new individual AM policy association: /npcf-am-policy-control/v1/policies **Allowed Values**: 0-31 **Default Value**: 24
AM_UPDATE_REQUEST_PRIORITY	Update an individual AM policy association: /npcf-am-policy-control/v1/policies/{polAssoId}/update **Allowed Values**: 0-31 **Default Value**: 18
AM_NOTIFICATION_REQUEST_PRIORITY	Update notification from PDS: /npcf-am-policy-control/v1/am-policies/{ueid}/notify **Allowed Values**: 0-31 **Default Value**: 18
AM_UPDATE_PDSLOCATIONINFO_REQUEST_PRIORITY	Update the db with `pdsLocationInfo` for given `associationID`: /npcf-am-policy-control/v1/policies/{polAssocId} **Allowed Values**: 0-31 **Default Value**: 18
AM_DELETE_REQUEST_PRIORITY	Delete the individual AM policy association: /npcf-am-policy-control/v1/policies/{polAssoId} **Allowed Values**: 0-31 **Default Value**: 16
AM_AUDIT_NOTIFY_REQUEST_PRIORITY	Audit notification: /audit/notify **Allowed Values**: 0-31 **Default Value**: 30
CONGESTION_RESPONSE_CODE	Configure the response code of any rejected requests by AM service due to congestion state. By default, the service sends 503 as response code. If configured then it shall be either 1xx, or 3xx, or 4xx, or 5xx status code.
SYSTEM.SEND_UNSUPPDNN_ON_AM_RESPONSE	When the value of this key is set to `true`, the AMF requests DNN replacement if the UE requests an unsupported DNN during a PDU session establishment request. **Default value**: `false`

5. Click **Save**.
   The page saves the PCF Access and Mobility configurations.

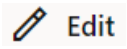
7.3.4 PCF UE Policy Service

This procedure provides information about configuring the PCF UE Policy Service.

The **PCF UE Policy** page displays the UE Service configurations. The page allows you to edit the configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure PCF UE Policy service:

1. From the navigation menu under **Policy** navigate to **Service Configurations** and select **PCF UE Policy**.
   This opens the **PCF UE Policy** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit PCF UE Policy** page.
3. Check the default configuration for the fields available in the respective groups and edit as necessary.
   The following table describes each field present under PCF UE policy along with the default configurations.

Table 7-77 Edit PCF UE Policy

Field Name	Description
System	Provide the system details:
Notification URI Root	Specifies the URI Root where the PCF (UE Policy service) is expected to receive notifications from AMF. **Example**: `http://localhost:8080` **Note:** Include the API prefix required by the API Gateway (if any). For example, `https://api-gateway.pcf.com/uepolicyservice`
Enable Max Session Limit	Specifies whether to enable the Limiting the Number of Sessions functionality.
Max Session Limit Per User	Specifies the maximum number of sessions to be limited per user if **Enable Max Session Limit** flag is enabled. Range: 1-2 Default value: 1
Override Supported Features	This configuration enables the pending transactions along with the Advanced Settings.
Data Compression Scheme	Specifies the data compression scheme used by UE. Following are the allowed values for this field: • Disabled • MySQL_Compressed • Application Compressed By default, this value remains disabled.
AMF	Provide AMF details:
AMF Discovery Criteria	Specifies the criteria to discover producer AMFs based on the AMF Set ID and the AMF Region ID. Valid options are:GUAMI, SetID, and RegionID. When this parameter is set to GUAMI, Policy parses the GUAMI to fetch the AMF SetID and AMF RegionID and uses these IDs to discover the producer AMF.
AMF Communication Profile	Specifies the NF communication profile used by AMF. For more information about configuring NF communication profiles, see NF Communication Profiles.
AMF Notification Retry Profile	Specifies the retry profile used by AMF. For more information about configuring retry profiles, see Retry Profiles.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-77 (Cont.) Edit PCF UE Policy

Field Name	Description
NAS Communication Profile	Specifies the NF communication profile used by NAS. For more information about configuring NF communication profiles, see NF Communication Profiles. This is where the NF communication profile with reattempt profile has to be attached to enable reattempts for all 4 service operations namely: `AMF Discovery`, `N1N2 Subscription`, `N1N2 Transfer`, and `N1N2 Transfer Failure Notification` . Use the same field to enable Reattempt for AMF Discovery.
NAS Retry Profile for Initial Messages	Specifies the retry profile used by NAS. For more information about configuring NF retry profiles, see Retry Profiles.
NAS Retry Profile for Subsequent Messages	Specifies the retry profile for subsequent messages used by NAS. For more information about configuring NF retry profiles, see Retry Profiles.
Send SBI Binding Header For N1N2 Transfer Requests	Indicates when to send the SBI binding information for N1N2Transfer request. The options can be: • When binding information changes • Always • Never **Default Value**: When binding information changes
Send Routing Binding Header For N1N2 Transfer Requests	Indicates when to send the routing binding information for N1N2Transfer request. The options can be: • Always • Never **Default (no value)**
Send Discovery Header For N1N2 Transfer Requests	Indicates when to send the discovery binding information for N1N2Transfer request. The options can be: • Always • Never **Default (no value)**
Enable Consolidation of UE Policy Decisions	Specifies whether to enable consolidation of policy decisions for a UE. When enabled, multiple sequenced policy decisions are consolidated as part of the next UE Policy Management Procedure. **Default value**: False
AMF Re-subscription Condition	Possible values are: • DISABLED • AMF Set ID and AMF Region ID • AMF Set ID • GUAMI If the value of this field is configured to any of the below mentioned values other than `DISABLED`, when the set ID or RegionID is different in the UE Update received from AMF, PCF sends unsubscribe to old AMF and subscribes to new AMF. **Default value**: DISABLED
User	Provide User details:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-77 (Cont.) Edit PCF UE Policy

Field Name	Description
Validate User	When **Validate User** is enabled, and the subscriber is not found in the UDR, or PCF is not able to query an available/eligible UDR, PCF fails the UE Association creation request with a 400 USER_UNKNOWN error. On the contrary when you disable **Validate User**, and the subscriber is not found in the UDR, or PCF is not able to query an available/eligible UDR, PCF does not fail the UE Association creation request, but continue policy processing. **Default Value**: `disabled`
Enable Subscriber State Variables	If this switch is enabled, UE Policy Service controls the querying and saving of local and remote subscriber state variables (SSV) on PDS. **Default value**: false
User Data Types	Provide User Data Types details:
UEPolicyData	If this switch is enabled, PCF fetches UEPolicyData from nUDR. For information on configuring UEPolicyData attributes, see **UEPolicyData Attributes table.**
CHF Data	If this switch is enabled, PCF fetches policy counters from CHF. For information on configuring CHF Data attributes, see **CHF Attributes table.**
UEPolicyData Attributes	Provide UEPolicyData Attributes details:
Subscribe to Notify	When **Subscribe to Notify** is enabled, Policy subscribes with the UDR to get notified on changes in subscriber profile. UE Policy notifies PDS, which in turn looks for an existing subscription for that subscriber and do any of the following: • If a subscription already exists and the `monitoredResourceUris` already contains "ue-policy-set", no action is taken by PDS. • If a subscription does not exist, PDS subscribes with the UDR using the POST method with monitoredResourceUris set to "ue-policy-set". **Default Value**: The button is `disabled` by default.
Query User on Create	Determines if user query from UDR is enabled. When this option is enabled, PDS queries the UDR about the subscriber contained in the UE Association create request by sending a GET request for “ue-policy-set” resource on the nudr-dr service. **Note:** The Policy Service caches the subscriber profile when **Subscribe To Notify** option is enabled. In that case, Policy may not always reach the UDR when the subscriber profile is found in the local cache. **Default Value**: The parameter is `disabled` by default.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-77 (Cont.) Edit PCF UE Policy

Field Name	Description
Query User on Update	Determines if user query from UDR on update is enabled. When this option is enabled, PDS queries the UDR about the subscriber present in the UE Association update request by sending a GET request for “ue-policy-set” resource on the nudr-dr service. **Default Value**: This parameter is `disabled` by default. **Note**: The Policy Service caches the subscriber profile when the `Subscribe To Notify` option is enabled. In that case, Policy may not always reach the UDR when the subscriber profile is found in the local cache. When the `Subscribe To Notify` flag is enabled and previous subscription attempts failed, then along with the data query, PDS also sends a SUBSCRIBE request to UDR.
Query User on Terminate	Determines if user query from UDR on delete is enabled. When this option is enabled, PCF queries the UDR about the subscriber present in the UE Association delete request by sending a GET request for “ue-policy-set” resource on the nudr-dr service. **Note:** The PCF User Service caches the subscriber profile when the **Subscribe To Notify** option is enabled, in that case, the PCF may not always reach the UDR when the subscriber profile is found in the local cache. **Default Value**: The button is `disabled` by default. **Note** It should be enabled only when subscription to UDR is disabled. It should not be enabled if subscription to UDR is enabled.
CHF Data Attributes	Provide the CHF Data Attributes:
CHF Data	If this switch is enabled, PCF fetches policy counters from CHF.
Async CHF Query Enabled	When this button is enabled, PCF interacts with CHF in Asynchronous mode.
Home PLMN	Provide Home PLMS details:
MCC	The Mobile Country Code and Mobile Network Code of the Home PLMN **Default Value**: NA
MNC	The Mobile Country Code and Mobile Network Code of the Home PLMN **Default Value**: NA
Rule	Provide the Rule details:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-77 (Cont.) Edit PCF UE Policy

Field Name	Description
Conflict Resolution Strategy	The conflict resolution strategy for managing conflicting UPSI/URSP rules in UE Policy evaluation. **Possible values**: INSTALL, REMOVE, and DROP. **Default Value**: NA (No selection)
N1 Message Transfer Settings	Provide N1 Message Transfer Settings details:
N1 Message Maximum Size	Maximum number of URSP Rules to be encoded in a single UE Policy Section (UPSI) container. **Default Value**: 2000
UE Policy Section Maximum Size	The maximum size in bytes of a "MANAGE UE POLICY COMMAND" after encoding to send out to AMF for delivery to UE. **Default Value**: 2000
Maximum Number of URSP Rules per UE Policy Section	Maximum number of URSP Rules to be encoded in a single UE Policy Section (UPSI) container. **Default Value**: 4
UE Policy Section Code (UPSC) Start	This fields indicate the range of UPSC allocation by PCF and can be used to maintain a dedicated range of UPSCs used by PCF generated UPSIs. Configuring these fields avoids the conflict of UPSCs between the UE built-in UPSC and the PCF delivered UPSC. **Note:** If the UPSI based policy action is also used for non-fragmented URSP delivery, then the range of UPSCs used by that method should be outside the range configured here. **Default Value**: Start: 0
UE Policy Section Code (UPSC) End	This fields indicate the range of UPSC allocation by PCF and can be used to maintain a dedicated range of UPSCs used by PCF generated UPSIs. Configuring these fields avoids the conflict of UPSCs between the UE built-in UPSC and the PCF delivered UPSC. **Note:** If the UPSI based policy action is also used for non-fragmented URSP delivery, then the range of UPSCs used by that method should be outside the range configured here. **Default Value**: End: 65535
Timer Settings	Provide Timer Settings details:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-77 (Cont.) Edit PCF UE Policy

Field Name	Description
T 3501 Timer Duration	PCF starts a T3501 Timer with the configured duration after it receives a successful response (200/202) to an N1N2 Transfer request from AMF. PCF expects an N1N2 Notification from AMF within this timer duration. **Note**: T3501 Timer should never be disabled when N1N2Message Transfer is carried out. Setting this field to 0 is not supported any more, and will be made obsolete or removed from CNC Console in the future release. **Default Value**: 5000 **Range**: 0 to 60000
Back-off Timer Duration	The action to be taken by PCF when the AMF notifies the PCF that it could not deliver the "MANAGE UE POLICY COMMAND" message to UE. **Default Value**: 15000
N1 Message Retransmission Settings	Provide the details for N1 Message Retransmission Settings details:
On T 3501 Timer Expiry	Provide On T 3501 Timer Expiry details:
Action	The action to be taken by PCF when N1 notification is not received within configured duration defined in T 3501 Timer Duration. **Default Value**: Abort N1 Delivery
Max Number of Re-transmissions	Maximum number of retransmissions to be attempted (excluding the initial attempt) after which UE service shall not try further to resend the same fragment to AMF. **Default Value**: 2
Re-transmission Failure Behavior	The behavior of PCF UE service if the N1 message is not delivered to the UE after a maximum number of re-transmissions have been tried. **Default Value**: Abort N1 Delivery
Enable Consolidation of UE Policy Decisions for Re-transmission on T3501 Expiration	Specifies whether to enable consolidation of UE policy decisions for re-transmission on T3501 expiration. When disabled, no consolidation is performed and sequenced policy decisions are processed after the current UE policy management procedure or re-transmission completes. **Default value**: False
On Transaction Failure Notification	Provide On Transaction Failure Notification details:
Action	The action to be taken by PCF when the AMF notifies the PCF that it could not deliver the "MANAGE UE POLICY COMMAND" message to UE. **Default Value**: Abort N1 Delivery

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-77 (Cont.) Edit PCF UE Policy

Field Name	Description
Max Number of Re-transmissions	Maximum number of re-transmissions to be attempted (excluding the initial attempt) after which UE service shall not try further to re-send the same fragment to AMF. **Default Value**: 2
Re-transmission Failure Behavior	The behavior of PCF UE service if the N1 message is not delivered to the UE after a maximum number of re-transmissions have been tried. **Default Value**: Abort N1 Delivery
On UE Policy Command Reject	Provide On UE Policy Command Reject details:
Action	The action to be taken by PCF when the UE notifies the PCF that it could not process the "MANAGE UE POLICY COMMAND" message. **Default Value**: Abort N1 Delivery
Maximum Number of Re-transmissions	Maximum number of re-transmissions to be attempted (excluding the initial attempt) after which UE service shall not try further to re-send the same fragment to AMF **Default Value**: 2
Re-transmission Failure Behavior	The behavior of PCF UE service if the N1 message is not delivered to the UE after a maximum number of re-transmissions have been tried. **Default Value**: Abort N1 Delivery
Audit	Provide Audit details:
Enabled	If this flag is enabled, UE service registers with Audit service for auditing the records in `UEPolicyAssociation` table. Once the registration is successful, a record for UE service is created in the `AuditRegistration` table. **Default Value**: true
Query AMF	When the Query AMF flag is set to **false**, the UE Service will terminate the session as soon as it is marked as stale by the Audit Service, without waiting for the maximum TTL (maxTTL) to expire. • If Query AMF is **false**, the session is removed immediately after it is detected as stale. • If Query AMF is **true**, the session will only be terminated after validation with the AMF, or once maxTTL is reached.
Notification Rate (per second)	Defines the maximum number of stale records, which Audit Service notifies to UE service in one second. Value of this parameter ranges between 20 and 700. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-77 (Cont.) Edit PCF UE Policy

Field Name	Description
Policy Association Age (in minutes)	Defines the age of the UE Policy Association, after which a record is considered to be stale on PCF and the AMF is queried (if query AMF is set to TRUE) for presence of such associations. Value of this parameter ranges between 1 and 10080. **Default Value**: 1440
Policy Association Maximum Age (in minutes)	Defines the maximum age of a UE Policy Association, after which a record is considered as stale and is purged from PCF UE database without sending further queries to AMF. Value of this parameter ranges between 1 and 20160. **Default Value**: 2880
Minimum Audit Attempts	Specifies the minimum number of consecutive failed audit attempts until maxTTL / forceTTL is reached. If maxTTL is reached and audit_attempts >= Minimum Audit Attempts for maxTTL, Audit service sends notification to UE Policy service with maxTTL flag set to *true*. UE Policy service sends DELETE request to PDS. **Range**: 0-255 **Default Value**: 0 **Note**: If maxTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until maxTTL is reached.
Minimum Audit Passes Interval (in minutes)	Defines the time when next audit for the UE service table is done after delta time if auditing this table has been finished before this specified time. Value of this parameter ranges between 1 and 1440. **Default Value**: 10
Pending Transaction	Provide Pending Transaction details:
UpdateNotify Retry Backoff (in milliseconds)	Defines the retry backoff for UpdateNotify in milliseconds. **Default Value**: 1000
UpdateNotify Retry Count	Defines the total number of retries for UpdateNotify. **Default Value**: 2

4. Perform the following steps to configure **Advanced Settings**:
   a. Click ⊕ Add
      The page opens the **Add Advanced Settings** dialog box.
   b. In the dialog box, enter the following **keys** and respective **values**:

The following table describes the keys and values:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-78 Add Advanced Settings Configurations

Key	Value
UE.POLICY.ACTION.NAME.AND.ID	When this is enabled, Name and ID of UPSI or URSP will be visible in the MARKER logs of Subscriber Activity Logging or PCAP. Based on this advance setting, PRE determines whether it will send UE Policy Actions with both ID and Name. Additionally for use cases, where request is sent from UE service to PRE, it will contain both ID and Name as determined by this advance setting, making this logic applicable to both inbound and outbound traffic. **Default value**: False
CONCURRENCY.ENABLED	Enables the communication to Bulwark service, if it is set to true. These will override Bulwark service enabled flag set during deployment using deployment yaml files. **Default value**: False
CONCURRENCY.N15.CREATE.LOCK_LEASE_DURATION	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically. **Default value**: 2000
CONCURRENCY.N15.CREATE.LOCK_WAIT_DURATION	Duration by which the UE service waits for the response to get a lock. **Default value**: 0
CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_COUNT	Number of attempts the service make to request the lock. **Default value**: 2
CONCURRENCY.N15.CREATE.ENABLED	Enables the communication to Bulwark service during CREATE request flow if these flag and Bulwark service flag in deployment yaml file are set to True. **Default value**: False
CONCURRENCY.N15.CREATE.ALLOW_ON_SERVICE_FAILURE	Allows the UE service to continue with the processing of CREATE request even if the response get from Bulwark service to lock/unlock was a failure. **Default value**: True
CONCURRENCY.N15.UPDATE.LOCK_LEASE_DURATION	Duration of the lock is kept once the block is successful. After this duration the lock will be released automatically. The duration is set only for UPDATE request flow. It can be set to 0 to indicate no release lock timeout. **Default value**: 2000
CONCURRENCY.N15.UPDATE.LOCK_WAIT_DURATION	Duration which consumer service will wait for the lock response. The duration is set only for UPDATE request flow. It can be set to 0 to indicate no release lock timeout. **Default value**: 0
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_COUNT	Number of retries when a request to bulwark service fails. The duration is set only for UPDATE request flow. **Default value**: 2
CONCURRENCY.N15.UPDATE.ENABLED	Enables the communication to Bulwark service during UPDATE request flow. If pendingtransaction feature is enabled then this Advance setting is avoided. **Default value**: False
CONCURRENCY.N15.UPDATE.ALLOW_ON_SERVICE_FAILURE	Allows the UE service to continue with the processing of UPDATE request even if the response get from Bulwark service to lock/unlock was a failure. **Default value**: True

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-78 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.N15.TERMINATE.LOCK_LEASE_DURATION	Duration of the lock is kept once the block is successful. After this duration the lock will be released automatically. The duration is set only for TERMINATE request flow. It can be set to 0 to indicate no release lock timeout. **Default value**: 2000
CONCURRENCY.N15.TERMINATE.LOCK_WAIT_DURATION	Duration of the lock is kept once the block is successful. After this duration the lock will be released automatically. The duration is set only for TERMINATE request flow. It can be set to 0 to indicate no release lock timeout. **Default value**: 0
CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_COUNT	Number of retries when a request to bulwark service fails. The duration is set only for TERMINATE request flow. **Default value**: 2
CONCURRENCY.N15.TERMINATE.ENABLED	Enables the communication to Bulwark service during TERMINATE request flow if these flag and Bulwark service flag in deployment yaml file are set to True. **Default value**: False
CONCURRENCY.N15.TERMINATE.ALLOW_ON_SERVICE_FAILURE	Allows the UE service to continue with the processing of TERMINATE request even if the response get from Bulwark service to lock/unlock was a failure **Default value**: True
CONCURRENCY.N15.NOTIFICATION.LOCK_LEASE_DURATION	Duration of the lock is kept once the block is successful. After this duration the lock will be released automatically. The duration is set only for NOTIFY request flow. It can be set to 0 to indicate no release lock timeout. **Default value**: 2000
CONCURRENCY.N15.NOTIFICATION.LOCK_WAIT_DURATION	Duration which consumer service will wait for the lock response. The duration is set only for NOTIFY request flow. It can be set to 0 to indicate no release lock timeout. **Default value**: 0
CONCURRENCY.N15.NOTIFICATION.LOCK_WAIT_DURATION	Duration which consumer service will wait for the lock response. The duration is set only for NOTIFY request flow. It can be set to 0 to indicate no release lock timeout. **Default value**: 2
CONCURRENCY.N15.NOTIFICATION.ENABLED	Set it to True will enable the communication to Bulwark service during NOTIFY request flow. IF pendingtransaction feature is enabled then this Advance setting is avoided. **Default value**: False
CONCURRENCY.N15.NOTIFICATION.ALLOW_ON_SERVICE_FAILURE	Allows the UE service to continue with the processing of NOTIFY request even if the GET response from Bulwark service to lock/unlock was a failure. **Default value**: True
BULWARK.SERVICE_CONNECTION_TIMEOUT	Duration which consumer service will wait for Bulwark response. **Default value**: 3000
USER.RESET_CONTEXT_SSV_ON_UE_CREATE	Sets resetContext flag for the SSV on the request towards PDS. **Default value**: false
USER.RESET_CONTEXT_CHF_DATA_ON_UE_CREATE	Sets resetContext flag for the CHF on the request towards PDS. **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-78 (Cont.) Add Advanced Settings Configurations

Key	Value
USER.RESET_CONTEXT_UE_POLICY_DATA_ON_UE_CREATE	Sets resetContext flag for the UE policy on the request towards PDS. **Default value**: false
CONCURRENCY.BULWARK_SERVICE_ENABLED	Enables the concurrency functionality. **Default value**: false
CONCURRENCY.N15.CREATE.ENABLED	Enables concurrency feature for AM-create call flow. **Default value**: false
CONCURRENCY.N15.CREATE.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.CREATE.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0
CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_COUNT	Wait time out for lock acquisition if not acquired. **Default value**: 2
CONCURRENCY.N15.CREATE.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Update flow. **Default value**: 1000
CONCURRENCY.N15.TERMINATE.ENABLED	Enables concurrency feature for AM-Delete call flow. **Default value**: false
CONCURRENCY.N15.TERMINATE.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Delete flow. **Default value**: 1000
CONCURRENCY.N15.TERMINATE.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.TERMINATE.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0
CONCURRENCY.N15.UPDATE.ENABLED	Enable concurrency feature for AM-Update call flow. **Default value**: false
CONCURRENCY.N15.UPDATE.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Update flow. **Default value**: 1000
CONCURRENCY.N15.UPDATE.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.UPDATE.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0
CONCURRENCY.N15.UPDATE_NOTIFY.ENABLED	Enable concurrency feature for AM-Update-Notify call flow. **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-78 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark for the AM Update Notify flow. **Default value**: 1000
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.UPDATE_NOTIFY.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 0
RESOURCEID.SUFFIXLIST	ResourceId because this is generic to all resources like AM or other service. Like in our case for AM we need this for association id which is a resource identifier. Hence ResourceId. Suffix because we are going to concatenate it with association id which will be after generated uuid. **Default value**: SUPI
ENABLE.ASSOCIATIONID.ENCODING	Enables the encoding of the Association ID in the format: `UEPolicyAssociationId_versionNoNumberOfEncodedDataEncoded(tlvFormat)` where: **versionNo**: This value indicates the encoding version being used. The version number starts from 1. It ensures compatibility with the existing encoding for base64 encryption. **Number of Encoded Data**: This number represents how much information is stored within the encrypted string. For example, the number of encoded data will be 01 for SUPI, 02 for both SUPI and GPSI, and the number will increment in case of more encrypted string: **encoded**: This value is limited to 99 different values in Tag Length Value (TLV) format. For an example, decoded value as 220imsi-450081000000001. Here, SUPI is identified with tag 2 followed by string length (20) and then the value. and the value. **value**: is key value pair of ***SUPI/GPSI*** **Default value**: false
ENABLE_LATE_ARRIVAL	Indicates whether to enable or disable validation of the incoming stale requests to UE Policy. To enable validation of the incoming stale requests by UE Policy service, set the value of this key as `true`. **Default value**: false
ENABLE_LATE_PROCESSING	Indicates whether to enable or disable validation of the stale requests to UE Policy during processing. To enable validation of the stale requests during processing, set the value of this key as `true`. **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-78 (Cont.) Add Advanced Settings Configurations

Key	Value
SKIP_LATE_PROCESSING_FOR_TERMINATE	When the value of this parameter is set to `true` , UE Policy service will not check if Terminate requests have gone stale. **Default value**: true
UE.POLICY.INSTALLATION.OPTIMIZATION.ENABLED	When the value of this parameter is set to `true` , UE Policy service will optimize the install action. **Default value**: false
CONCURRENCY.N15.T3501_TIMER_EXPIRY.LOCK_REQUEST_RETRY_COUNT	Indicates the number of retries when lock acquisition fails from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.T3501_TIMER_EXPIRY.LOCK_REQUEST_RETRY_BACKOFF	Indicates the duration for which AM service will wait once it receives ALREADY_LOCKED Response from Bulwark. **Default value**: 1000
CONCURRENCY.N15.T3501_TIMER_EXPIRY.LOCK_LEASE_DURATION	Indicates the duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically. **Default value**: 2000
CONCURRENCY.N15.T3501_TIMER_EXPIRY.LOCK_WAIT_DURATION	Indicates the duration by which the UE service waits for the response to get a lock. **Default value**: 3000
CONCURRENCY.N15.T3501_TIMER_EXPIRY.ENABLED	Indicates if bulwark lock is enabled for processing T3501 timer expiry. **Default value**: false
CONCURRENCY.N15.UE_NOTIFICATION.LOCK_REQUEST_RETRY_COUNT	Indicates the number of retry when lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.UE_NOTIFICATION.LOCK_REQUEST_RETRY_BACKOFF	Indicates the duration for which UE service will wait once it receives ALREADY_LOCKED Response from Bulwark. **Default value**: 1000
CONCURRENCY.N15.UE_NOTIFICATION.LOCK_LEASE_DURATION	Indicates the duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically. **Default value**: 2000
CONCURRENCY.N15.UE_NOTIFICATION.LOCK_WAIT_DURATION	Indicates the duration by which the UE service waits for the response to get a lock. **Default value**: 3000
CONCURRENCY.N15.UE_NOTIFICATION.ENABLED	Indicates if Bulwark lock is enabled for UE Notification from AMF. **Default value**: false
CONCURRENCY.N15.CLEANUP.ENABLED	Enables concurrency feature for UE Cleanup call flow. **Default value**: false
CONCURRENCY.N15.CLEANUP.LOCK_REQUEST_RETRY_COUNT	If lock acquisition failed from Bulwark due to lock request failed. **Default value**: 2
CONCURRENCY.N15.CLEANUP.LOCK_REQUEST_RETRY_BACKOFF	This is the duration for which UE service will wait once it receives ALREADY_LOCKED Response from Bulwark for the UE Cleanup flow. **Default value**: 1000

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-78 (Cont.) Add Advanced Settings Configurations

Key	Value
CONCURRENCY.N15.CLEANUP.LOCK_LEASE_DURATION	Lease duration for which lock will be acquired. After this time, Bulwark will automatically release the lock. **Default value**: 2000
CONCURRENCY.N15.CLEANUP.LOCK_WAIT_DURATION	Wait time out for lock acquisition if not acquired. **Default value**: 3000
CONCURRENCY.N15.CLEANUP.ALLOW_ON_SERVICE_FAILURE	If bulwark lock is not obtained after all retries for the UE Cleanup flow, then if enabled, the request will continue, if disabled the request will be rejected. **Default value**: true
CANCEL.ON.NEW.TRIGGER.ENABLED	If this key is set to `true` and UE Policy service receives an Update, Delete, or a data change notification from any of the NFs such as UDR or CHF, UE Policy service cancels the active retryAfter timer and immediately initiates the N1N2MessageTransfer . If this key is set to `false`, UE service does not cancel the active retryAfter timer and sequences any incoming UPSI for next N1N2Transfer evaluated as part of service operation coming as new trigger (data change notification from NFs such as UDR or CHF). **Default value**: false
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.ENABLED	This key determines if Bulwark service is enabled to acquire a lock for processing RetryAfter timer expiry notification. **Default value**: false
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_LEASE_DURATION	Specifies the duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically. **Default value**: 2000 (millisecond)
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_BACKOFF	Specifies the duration for which UE Policy service waits once it receives ALREADY_LOCKED response from Bulwark service. **Default value**: 1000 (millisecond)
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_COUNT	Specifies the number of retries when lock acquisition from Bulwark service failed due to lock request failed. **Default value**: 2
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_WAIT_DURATION	Specifies the duration for which the UE Policy service waits for the response from Bulwark service to get a lock. **Default value**: 3000 (millisecond)
RETRY.AFTER.IE.MAX.SECONDS	Specifies the maximum retryAfter duration in seconds for which the UE Policy service must wait before attempting a reAttempt for a failed N1N2Transfer. **Range**: 1-600 **Default value**: 600 (seconds)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-78 (Cont.) Add Advanced Settings Configurations

Key	Value
RETRY.AFTER.IE.TIMER.CAPACITY	Specifies the capacity threshold defining the number of N1N2 Transfer operations to be queued for retryAfter. **Range**: 0-360000 **Default value**: 50000 **Note**: The UE Policy service adjusts the value to the nearest valid range for capacity whenever an out-of-bounds value is configured. For instance, if the maximum capacity is set to 360000 and the configured value is 370000 , the UE Policy service adjusts it to 360000.
RETRY.AFTER.IE.TIMER.RATE	Indicates the request rate per second to limit the retryAfter Timer Expiry notifications. **Range**: 2-700 **Default value**: 50 **Note**: The UE Policy service adjusts the value to the nearest valid range for rate limit whenever a user configures an out-of-bounds value. For example, if the maximum capacity is set to 700 and the value is configured as 800, the UE Policy service adjusts it to 700.
TIMER_EXP_RANGE_MIN_SEC	Indicates the minimum value of timer in seconds.

Table 7-79 Advanced Settings for Congestion Control

Key	Value	Description
UE.GET.SUBSCRIBER.SESSIONS.PRIORITY	28	Retrieve any type of subscriber session priorities. **Allowed Values**: 0- 31
UE.GET.POLICY.ASSOCIATION.PRIORITY	18	Retrieve the individual UE policy association priority. **Allowed Values**: 0- 31
UE.CREATE.PRIORITY	24	Create a new individual UE policy association. **Allowed Values**: 0- 31
UE.UPDATE.PRIORITY	18	Report observed event triggers and possibly obtain updated policies for the individual UE policy association **Allowed Values**: 0- 31
UE.UPDATE.NOTIFICATION.PRIORITY	18	Update notification from PDS **Allowed Values**: 0- 31
UE.DELETE.PRIORITY	16	Delete the individual UE policy association. **Allowed Values**: 0- 31
UE.AUDIT.NOTIFY.PRIORITY	30	To handle Audit notification. **Allowed Values**: 0- 31
UE.N1.NOTIFICATION.MESSAGE.PRIORITY	18	To handle UE N1 notification messages. **Allowed Values**: 0- 31

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-79 (Cont.) Advanced Settings for Congestion Control

Key	Value	Description
UE.N1.FAILURE.NOTIFICATION.MESSAGE.PRIORITY	18	To handle UE N1 Failure notification messages. **Allowed Values**: 0- 31
CONGESTION.HTTP.RESPONSE.CODE	503	Configure the response code of any rejected requests by UE service due to congestion state. By default, the service sends 503 as response code. If configured then it shall be either 1xx, or 3xx, or 4xx, or 5xx status code.

Table 7-80 Add Advanced Settings for Bulwark Configurations for Timer

Key	Value	Description
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_COUNT	2	Number of retry when lock acquisition failed from Bulwark due to lock request failed
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_REQUEST_RETRY_BACKOFF	1000	This is the duration for which UE service will wait once it receives ALREADY_LOCKED Response from Bulwark
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_LEASE_DURATION	2000	The duration for which lock is kept once the acquisition is successful. After this duration, the lock gets released automatically
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.LOCK_WAIT_DURATION	3000	Duration by which the UE service waits for the response to get a lock.
CONCURRENCY.N15.REATTEMPT_TIMER_EXPIRY.ENABLED	false	If Bulwark lock is enabled for processing Reattempt timer expiry Notification
AMF.OPTIMIZED.DISCOVERY.AND.SUBS.ENABLED	true	True: Discovery and subscription to AMF occur only when an N1MessageTransfer is required False: In-Advance AMF Discovery and Subscription are performed, N1Message Transfer may or may not be initiated, depending on the UE policy action
AMF_CONNECTOR_TIMEOUT_GUARD	integer	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-80 (Cont.) Add Advanced Settings for Bulwark Configurations for Timer

Key	Value	Description
PDS_CONNECTOR_TIMEOUT_GUARD	integer	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0

5. Click **Save**.
   The page saves the PCF UE Policy configurations.

7.3.5 PCF Policy Authorization

This procedure provides information about configuring the PCF Policy Authorization Service.

The **PCF Policy Authorization** page displays the authorization service configurations. The page allows you to edit the configurations.

To configure the PCF Policy Authorization Service:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, and select **PCF Policy Authorization**.
   This opens the **PCF Policy Authorization** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit PCF Policy Authorization** page.
3. Check the default configuration for all the fields in all groups and edit as necessary.
   The following table describes the input fields displayed under each group:

Table 7-81 Edit PCF Policy Authorization

Field Name	Description
System	Provide System details:
Af Direct Reply	Determines, if reply must be sent to AF before the PCF that sends the policy decision to SMF, after successful session binding.**Default Value**: `true`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-81 (Cont.) Edit PCF Policy Authorization

Field Name	Description
Override Supported Features	Defines the supported features that can be configured to override system embedded values. Represent a string separated by comma. For example, "InfluenceOnTrafficRouting,SponsoredConnectivity". The "" means an empty supported feature set. **Note** This field lists all the features from the specification. However, only the following features are supported by PCF and should be selected: • IMS_SBI • NetLoc • SponsoredConnectivity • ProvAFsignalFlow • RAN_NAS_Cause • PatchCorrection • QoSMonitoring • EnhancedSubscriptionToNotification
AF Terminate Uri Segment	Specifies AF notify to terminate uri segment appended to AF notify uri. For example, {NotificationUri}/termination. "termination" is the terminate uri segment.**Default Value**: `terminate`
AF Subscriber Notify Segment	Specifies AF subscription notify uri segment appended to AF subs notify uri. For example, {NotificationUri}/notify. "notify" is the subscription notify uri segment.**Default Value**: `terminate`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-81 (Cont.) Edit PCF Policy Authorization

Field Name	Description
Rx Resource Allocation Partial Failure Report Presence	After PCF triggers a notification to Diameter Connector, the connector generates a RAR message. The partial failed specific action in the RAR message depends on the priority of the action subscribed in the AAR message. The priority of the actions is INDICATION_OF_FAILED_RESOURCES_ALLOCATION > INDICATION_OF_RELEASE_OF_BEARER > INDICATION_OF_LOSS_OF_BEARER. If you want to assign the action not depend on the priority, you can assign the action in this field. The default configuration is empty, you can choose one action from the following options. Once the value is defined in this field, the connector uses the configured action not depend on the priority. Valid Options are: • INDICATION_OF_FAILED_RESOURCES_ALLOCATION • INDICATION_OF_RELEASE_OF_BEARER • INDICATION_OF_LOSS_OF_BEARER
AF Notifications Retry Profile	Defines the retry profile configuration for Policy Authorization. For more information on configuring retry profile, see Retry Profiles.
AF Communication Profile	Specifies the NF communication profile used by AF. For more information about configuring NF communication profiles, see NF Communication Profiles.
Data Compression Scheme	Specifies the data compression scheme that can be used. Following are the allowed values for this field: • Disabled • MySQL_Compressed • Application Compressed By default, this value remains disabled.
Enable Authorization Lifetime	Specifies whether to enable feature negotiation for Authorization Lifetime of Rx Sessions. **Default Value**: false
QoS Monitoring	

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-81 (Cont.) Edit PCF Policy Authorization

Field Name	Description
Accept Request on Missing QoS Monitoring Attributes	Indicates whether to accept or reject any PA Create request with `QOS_MONITORING` event. Possible values: • `false`: Rejects any PA Create request with `QOS_MONITORING` event that misses any mandatory value required to subscribe to such event. • `true`: Accepts any request with `QOS_MONITORING` event, irrespective of whether all the mandatory values required to subscribe were provided or not. This allows to derive the missing values via Policy Evaluation. **Default value**: false
Accept Request on QoS Monitoring Not Supported/Not Negotiated	Indicates whether to accept or reject any PA Create request with `QOS_MONITORING` event that is not supported or not negotiated. Possible values: • `false`: Rejects any PA Create request with `QOS_MONITORING` event, which did not negotiate QosMonitoring feature based on one of the following: – QosMonitoring feature is not negotiated by SMF during SM operations (not passed in suppFeat attribute or not present in Override supported features configuration for PCF Session Management service. – QosMonitoring feature is not added as supported in Override supported features configuration for PCF Policy Authorization service. • `true`: Accepts any PA Create request with `QOS_MONITORING` event but ignores the event and its related data if the feature was not negotiated based on the same conditions mentioned above. **Default value**: `true`
IMS Emergency Session	Provide IMS Emergency Session details:
Emergency Service URNs	Defines the Uniform Resource Name (URN) values for emergency and other well-known services.
Reservation Priority Types	Determines the IMS Signaling Priority.**Default Value**: PRIO_6
NWDAF	Provide NWDAF details:
Enable NWDAF Data	Enables or disables the **Enable NWDAF Data** switch.
Audit	Provide Audit details:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-81 (Cont.) Edit PCF Policy Authorization

Field Name	Description
Audit Enabled	Specifies whether to enable or disable the stale Rx session audit and deletion. When this parameters is enabled, SM Service registers with Audit service for monitoring Rx sessions. **Default Value**: false
App Session Age (in minutes)	Specifies the Time To Live (TTL) of Rx sessions. **Range**: 0-21600 **Default Value**: 1440
App Session Maximum Age (in minutes)	Specifies the maximum Time To Live (TTL) of Rx sessions. **Default Value**: 4320 **Range**: 0-21600
Notification Rate (per second)	Maximum amount of app session cleanup requests per second. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)
Minimum Audit Passes Interval (in minutes)	Specifies how long the Audit Service waits for next audit cycle. **Default Value**: 10
Handle NULL As Stale	If `EXPIRY_TIMESTAMP` or `SITEID` contains `NULL` value, (legacy stale records after upgrade) they will be considered in the next audit cycle as TTL expired. **Default Value**: false

4. Perform the following steps to configure **Advanced Settings**:

   a. Click ⊕ Add
   The page opens the **Add Advanced Settings** dialog box.

   b. In the dialog box, enter the following **keys** and respective **values**:

The following table describes the keys and values:

Table 7-82 Add Advanced Settings Configurations

Key	Value
PA.NWDAF.EVENT	Allow to add one or more Events to be send in the request towards NWDAF. **Default value**: SLICE_LOAD_LEVEL
PA.NWDAF.REQUEST_TIMEOUT	Allow to control the timeout of the request from SM towards NWDAF. **Default value**: 3000 (ms)
SYSTEM.PA_ERROR_HANDLER_ENABLED	Allows to enable the RAA error handling feature. **Default value**: False

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-82 (Cont.) Add Advanced Settings Configurations

Key	Value
SYSTEM.PA.EVENT_TRIGGERS	This is a comma separated list of Event-Trigger names that are installed on SMF by PCF upon PA session establishment. For example: ACCESS_TYPE_CHANGE, SUCCESSFUL_RESOURCES_ALLOCATION, USAGE_REPORT To reset value to default, the advance setting needs to be deleted. **Default value**: an empty list ("")
SYSTEM.RX.EVENT_TRIGGERS	This is a comma separated list of Event-Trigger names that are installed on SMF by PCF upon Rx session establishment. For example: ACCESS_TYPE_CHANGE, SUCCESSFUL_RESOURCES_ALLOCATION, PLMN_CHG To reset value to default, the advance setting needs to be deleted. **Default value**: ACCESS_TYPE_CHANGE **Supported values**: • ACCESS_TYPE_CHANGE • FAILED_RESOURCES_ALLOCATION • PLMN_CHG • QOS_NOTIF • SUCCESSFUL_RESOURCES_ALLOCATION • USAGE_REPORT • ANI_REPORT
SYSTEM.PA_TERMINATE_NOTIFY_TIMEOUT_TRIGGER_PA_DELETE	When the value of this key is set to `true`, Policy Authorization service cleans up the AppSession as soon as the ASR request times out, irrespective of whether it receives ASA or not. **Default value**: `false`
SYSTEM.ENABLE_ONLINE_ATTRIBUTE_IN_CHARGING_DATA	Possible values are: • true (to enable the key) • false (to disable the key) When Sponsored Data connectivity feature is enabled, this key allows to enable or disable the `Online` attribute in Charging data. If this key is disabled, by default, the `Online` attribute is disabled and the sponsored connectivity data will not be sent in the Charging Data. The `Offline` attribute is enabled. If this key is enabled, the `Offline` attribute is disabled and the online attribute will be enabled to send the sponsored connectivity data in Charging Data. Default value: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-82 (Cont.) Add Advanced Settings Configurations

Key	Value
SYSTEM.ACCEPT_REQUEST_WHEN_MISSING_SPONSORED_CONNECTIVITY_DATA	This key determines whether PCF must reject the Policy Authorization Create/ Update request or accept the request and treat it as a Normal Policy Authorization Create/ Update request when the following conditions are met: • SponCon Feature Enabled in PCF and • "SponsoredConnectivity" supported by AF and • "sponStatus" Received from AF as disabled and • sponId and/or aspId not received from AF/NEF When this key is disabled, the request is rejected. **Note**: Only applies to requests with sponStatus of SPONSOR_DISABLED, when sponStatus is received as SPONSOR_ENABLED, this flag will not have any functional impact on PCF behavior. **Default value**: false **Important**: `SYSTEM.ACCEPT_CREATE_WHEN_MISSING_SPONSORED_CONNECTIVITY_DATA` which was used to reject the Policy Authorization Create request or accept the request is currently deprecated. Hence, instead of `SYSTEM.ACCEPT_CREATE_WHEN_MISSING_SPONSORED_CONNECTIVITY_DATA`, `SYSTEM.ACCEPT_REQUEST_WHEN_MISSING_SPONSORED_CONNECTIVITY_DATA` must be configured for the same purpose.
SYSTEM.INCLUDE_SPONID_ASPID_DIMENSIONS	This key is used to control whether the dimensions sponId and aspId are added to the *pa_sponsored_sessions_total and pa_sponsored_session_update_notify_total* metrics. Default value: false
SYSTEM.RETAIN_USAGE_REPORT_WHEN_USG_THRES_NULL	When this key is set to `true` (default behavior), the PCF retains (keeps the previously saved value) the USAGE_REPORT subscription for the NEF/AF, even if: • The session does not have USAGE_MONITORING enabled, and • UsageThreshold is provided as null in the PA-Update request. When the flag is set to `false`, the PCF removes the existing USAGE_REPORT subscription from the event list, effectively disabling the report for that subscription. Default value: true

5. Click **Save**.
   The page saves the PCF Policy Authorization configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.6 PCF User Connector

This procedure provides information about configuring the PCF User Connector Service.

The **PCF User Connector** page displays the User Connector Service configurations. The page allows you to edit the configurations.

To configure the PCF User Connector service:

1. From the navigation menu under **Policy**, navigate to **Service Configurations** and select **PCF User Connector**.
   This opens the **PCF User Connector** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit PCF User Connector** page.
3. Check the default configuration for all the fields in all groups and edit as necessary.
   The following table describes the input fields displayed under each group:

Table 7-83 Edit PCF User Connector

Field Name	Description
System	Provide System details:
Server Root URL	Specifies the callback URI for notifications to be received by the User service. For example, while creating a subscription for the user with .UDR
Common	Provide Common details:
Request Timeout	Request timeout in milliseconds for: • AmPolicyData change notification request sent to AM service • UePolicySet change notification request sent to UE service • SmPolicyData change notification request sent to SM service • SpendingLimit status change notification/ terminate request sent to SM service • On demand discovery request sent to NRF client for dynamic discovery of UDR **Default Value**: 2000 milliseconds
UDR	Provide UDR details:
Base Uri	Base Uri specifies the part of resource uri, which follows apiRoot. The Base Uri is common to all Policy Data resources. For example – In the Resource Uri `{apiRoot}/nudr-dr/{apiVersion}/policy-data/ues/{ueId}/sm-data`, `nudr-dr/{apiVersion}` is the base Uri. **Default Value**: /nudr-dr/v1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-83 (Cont.) Edit PCF User Connector

Field Name	Description
Supported Features	Refers to the value set to **supportedFeatures** field in PolicyDataSubscription while sending subscriptions request to UDR for notifying changes in policy data. **Default Value**: f **Note**: When Immediate Reporting feature is enabled, value configured in this flag will be merged to Immediate reporting feature capability value, which is 30th bit enabled.
SM Data VSA Names	Indicates to provision subscriber name from Vendor Specific Attribute (VSA) data in SM Policy data for subscriber profile. **Example**: VendorSpecific-000111 **Note**: This field must be configured for Cloud Native Core PCRF deployments that have Usage Monitoring enabled that interacts with UDR to fetch Subscriber Profile Data over 3GPP N36 interface. This field indicates a list of Vendor Specific Attribute names that are provisioned in the SessionManagementPolicyData Resource on UDR that needs to be fetched by the Cloud Native PCRF Function to be used in PCRF Core and Usage Monitoring.
AM Data Uri	It refers to the section of resource uri that represents all UE related access and mobility policy attributes in the UDR for a given "ueId". AM Data Uri follows base uri part of the resource uri. **Default Value**: /policy-data/ues/{ueId}/am-data
UE Policy Set Uri	It refers to the section of resource uri that represents UE policy set attributes in the UDR for a given "ueId". UE Policy Set Uri follows base uri part of the resource uri. **Default Value**: /policy-data/ues/{ueId}/ue-policy-set
SM Data Uri	It refers to the section of resource uri that represents all PDU session related subscription attributes in the UDR for a given "ueId". SM Data Uri follows base uri part of the resource uri. **Default Value**: /policy-data/ues/{ueId}/sm-data
Usage Mon Uri	It refers to the section of resource uri that represents an individual usage monitoring resource created in the UDR and associated with a ueId and a usageMonId. Usage Mon Uri follows base uri part of the resource uri. **Default Value**: /policy-data/ues/{ueId}/sm-data/{usageMonId}
Subs To Notify Uri	It refers to the section of resource uri that represents subscriptions to notification of policy data modification. Subs To Notify Uri follows base uri part of the resource uri. **Default Value**: /policy-data/subs-to-notify

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-83 (Cont.) Edit PCF User Connector

Field Name	Description
Subs To Notify Subs Id Uri	It refers to the section of resource uri that represents an individual subscription to notification of policy data modification. Subs To Notify Subs Id Uri follows base uri part of the resource uri. **Default Value**: /policy-data/subs-to-notify/{subsId}
SM Data Subscription Resource	Default value would be 1 on selection of "Sm-data" and other value is 2 on selection of "As requested by SM service".
Discover UDR with Policy as Supported Data Set	Indicates whether to send "POLICY" as data-set to be supported by the UDR during NRF discovery procedure. In turn, this configuration helps NRF filter and responds with only those UDR NF Profiles which support "POLICY" as one of the data-sets. By default, the value for this parameter is set to `false`.
Request Timeout	Specifies the timeout interval in milliseconds in which a request to UDR fails if UDR fails to respond within this value of timeout. **Default Value**: 1000 milliseconds
Enable Discovery On Demand	When this field is set to true, UDR discovery from NRF takes place for each UeId. **Default Value**: false
Retry Profile for Initial Messages	Retry Profile to be used when PCF fails to send a create message to a producer node.
Retry Profile for Subsequent Messages	Retry Profile to be used when PCF fails to send an in-session message to a producer node.
Retry Subscription Message as:	Retry Subscription Message enables the operator to choose Retry Logic for SUBSCRIBE/POST towards UDR from the follow possible options: • **Initial Message**: PCF will treat POST as Initial message and apply Initial Retry Logic for Session Retry. • **Subsequent Message**: PCF will treat POST as Subsequent message and apply Subsequent Retry Logic for Session Retry.
NF Communication Profile	The NF communication profile created for the service. This profile is created using the NF Communication Profiles page.
Send Target API Root Header in Subscribe to Notify Request	Specifies whether to include Target API Root header in the subscribe to notify request sent by PCF towards UDR. **Note**: If the user selects Model D for Policy NF Communication Model, the value for this field can be set to true or false. For other Policy NF Communication Model values, the value for this field must be set to true. By default, the value for this parameter is set to true.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-83 (Cont.) Edit PCF User Connector

Field Name	Description
Send Initial Discovery Parameters in Subscribe to Notify Request	Specifies whether to include initial discovery parameters in the subscribe to notify request sent by PCF towards UDR. By default, the value for this parameter is set to false.
Send Producer Id in Discovery Header in Subscribe to Notify Request	Specifies whether to include Producer ID in discovery header in the subscribe to notify request sent by PCF towards UDR. By default, the value for this parameter is set to false.
Enable Immediate Report on Subscription	Specifies whether to include the attribute "immRep" and set it to "true" in the subs-to-notify request message to UDR. **Note**: With this configuration enabled, behavior of UDR-Discovery towards NRF will not change, that is., PCF shall not perform additional feature negotiation. By default, the value for this parameter is set to false.
Enable Data Retrieval Fallback for Immediate Report	When this configuration is set to true, PCF attempts to retrieve the subscriber data from UDR using GET procedure in the following scenario: • Immediate Report feature is enabled, and • PCF sent a POST message to UDR with "immRep" attribute set to true, and • UDR responded with a successful subscription but the response message body did not contain the "immReports" attribute By default, the value for this parameter is set to false.
Message Priority Profile	Select one of the message priority profiles created on **Message Profiles** page that must be applied for UDR Connector. When a message profile is selected under **Message Priority Profile** section, support for `3GPP-SBI-Message-Priority` header gets enabled for UDR Connector.
CHF	Provide CHF details:
Retry Profile for Initial Messages	Retry Profile to be used when PCF fails to send a create message to a producer node.
Retry Profile for Subsequent Messages	Retry Profile to be used when PCF fails to send an in-session message to a producer node.
NF Communication Profile	The NF communication profile created for the service. This profile is created using the NF Communication Profiles page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-83 (Cont.) Edit PCF User Connector

Field Name	Description
PCF Service name in Binding Header	Specifies the custom/3GPP defined PCF service name to be included in the binding header in the subscription request or notification responses sent towards CHF. Possible values: • Aggregate or custom service name that represents a group of PCF services with aggregated service level information. For example: `npcf-custom-service` • Any of the 3GPP defined PCF service names such as `npcf-smpolicycontrol` or `npcf-am-policy-control` There is no default value configured for this field.
Request Timeout	
Message Priority Profile	Select one of the message priority profiles created on **Message Profiles** page that must be applied for CHF Connector. When a message profile is selected under **Message Priority Profile** section, support for `3GPP-SBI-Message-Priority` header gets enabled for CHF Connector.

Note

- If both **Retry Profile for Initial Messages** and **Retry Profile for Subsequent Messages** are not configured (default case) no retry is attempted.
- If both **Retry Profile for Initial Messages** and **Retry Profile for Subsequent Messages** are configured, retries is attempted accordingly.
- If **Retry Profile for Initial Messages** is configured but **Retry Profile for Subsequent Messages** is not configured then the profile for initial messages is used for subsequent messages. (to be backward compatible with release 1.8.x)
- If **Retry Profile for Initial Messages** is not configured but **Retry Profile for Subsequent Messages** is configured, then retry is not attempted for initial messages. But it is attempted for the subsequent messages.
- If **Send PCF Service Name in Binding Header** parameter under **NF Bindings Setting** section in **NF communication profile** page is enabled for CHF interface , the aggregate custom Service name or a 3gpp defined pcf service name must be defined in **PCF Service name in Binding header** parameter. This service name will be included in the binding header towards CHF sent over N28/Nchf interface.

4. Perform the following steps to configure **Advanced Settings** that sets the key precedence on user connector:
   a. Click ⊕ Add
      The page opens the **Add Advanced Settings** dialog box.
   b. In the dialog box, enter the following **key** and respective **value**:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-84 Parameters for Advanced Settings

Keys	Value
UDR.KeyPrecedence	It is used to set the Key Precedence given on User Connector. **Default Value**: SUPI, GPSI
CONCURRENCY_LOCK_FAILURE_ERROR_CODE	Indicates an error in PDS Service in acquiring a lock from Bulwark Service to process a notification from UDR or CHF. **Default Value**: 500
RETAIN_ORIGINAL_MONITORED_RESOURCE_URI_ON_REVALIDATION	If the flag is set to true the monitoredResourceUri sent in the POST will be retained for the subsequent PUT request. **Default Value**: false
UDR_errorHandlerEnabled	This flag enables error handling configuration with UDR connector service. **Default Value**: false
CHF_errorHandlerEnabled	This flag enables error handling configuration with CHF connector service. **Default Value**: false
UDR_NF_PROFILE_COOKIE_ENABLED	This flag indicates whether the UDR profiles discovered during UDR-GET needs to be cached till UDR-POST is completed (success/failure). **Default Value**: false
UDR_NF_PROFILE_COOKIE_COMPRESS	This flag indicates whether to compress the UDR profiles cached between GET and POST request. **Default Value**: false
UDR_NF_PROFILE_COOKIE_LIMIT	This flag indicates the number of UDR profiles between GET and POST that can be cached. **Default Value**: 10 **Note:** It is recommended to enable UDR_NF_PROFILE_COOKIE_COMPRESS to true so that we can support caching of upto 10 UDR profiles. For supporting lesser number of UDR profile caching (like 3-4), we can disable the compression. Caching of more than 10 profiles is not supported.
UDR_GET_USE_RELATED_RESOURCE	This flag allows GET for related resources (for example, amPolicyData and uePolicySet) from the same UDR where previous GET was done. **Default Value**: false
UDR.enable.late.arrival	Indicates whether to validate an incoming request if went stale during arrival in UDR connector. Set the value of this key to `true` to validate staleness of the incoming requests to UDR connector. **Default value**: Disabled

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-84 (Cont.) Parameters for Advanced Settings

Keys	Value
CHF.enable.late.arrival	Indicates whether to validate an incoming request if went stale during arrival in CHF connector. Set the value of this key to `true` to validate staleness of the incoming requests to CHF connector. **Default value**: Disabled
UDR.enable.late.processing	Indicates whether to validate an a request if went stale during processing at UDR connector. Set the value of this key to `true` to validate staleness of the requests that went stale during processing at UDR connector. **Default value**: Disabled
CHF.enable.late.processing	Indicates whether to validate an a request if went stale during processing at CHF connector. Set the value of this key to `true` to validate staleness of the requests that went stale during processing at CHF connector. **Default value**: Disabled
UDR.skip.late.processing.for.terminate	Indicates whether to skip validation to request of type delete if went stale during arrival and processing in UDR connector. Set the value of this key to `true` to skip validation to request of type delete if went stale during processing in UDR connector. **Default value**: Disabled **Note**: Validation of the TERMINATE requests are skipped only in case of late processing. Late arrival TERMINATE requests are rejected similar to the other late arrival requests.
CHF.skip.late.processing.for.terminate	Indicates whether to skip validation to request of type delete if went stale during arrival and processing in CHF connector. Set the value of this key to `true` to skip validation to request of type delete if went stale during processing in CHF connector. **Default value**: Disabled **Note**: Validation of the TERMINATE requests are skipped only in case of late processing. Late arrival TERMINATE requests are rejected similar to the other late arrival requests.
UDR_NOTIFY_UNSPECIFIED_MSG_FAILURE_CAUSE_ENABLE	This flag indicates that in UDR Notify POST request, error cause UNSUPPORTED_MONITORED_URI and error code 501 will be replaced with error cause UNSPECIFIED_MESSAGE_FAILURE and error code 400. **Default Value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-84 (Cont.) Parameters for Advanced Settings

Keys	Value
IMM_REP_CAPABILITY_CHECK	When this configuration is set to false in advance setting, PCF shall ignore the capability check for UDR and send POST with immediate Reporting. If it is set to true, PCF will check the capability and decide either to send GET+POST or POST request. **Default Value**: true
SAVE_SRC_SERV_INST	This flag indicates whether to save the source service instance in the subscription info database. This flag takes effect only when the global flag `ENABLE_NF_PEER_INFO` is enabled. **Default value**: false

You can add the following keys to configure the message priority for different rest endpoints. If any invalid or incorrect values are provided then the default priority values shall be considered.

Table 7-85 Advanced Settings for Congestion Control

Key	Default Value	Allowed Values
UDR_GET_USER_DATA_REQUEST_PRIORITY	24	Get User data from UDR. **Allowed Values**: 0-31
UDR_DELETE_USER_DATA_REQUEST_PRIORITY	16	Delete User data from UDR. **Allowed Values**: 0-31
UDR_PATCH_USER_DATA_REQUEST_PRIORITY	18	Update the User data at UDR. **Allowed Values**: 0-31
UDR_SUBS_TO_NOTIFY_REQUEST_PRIORITY	22	Subscribe to UDR Notification. **Allowed Values**: 0-31
UDR_NOTIFY_REQUEST_PRIORITY	18	UDR Notification **Allowed Values**: 0-31
UDR_UM_NOTIFY_REQUEST_PRIORITY	18	UDR UM Notification. **Allowed Values**: 0-31
CHF_GET_SPENDING_LIMIT_REQUEST_PRIORITY	24	Get spending limit from CHF. **Allowed Values**: 0-31
CHF_DELETE_SPENDING_LIMIT_REQUEST_PRIORITY	16	Delete spending limit at CHF. **Allowed Values**: 0-31
CHF_TERMINATE_NOTIFY_REQUEST_PRIORITY	17	Terminate notification from CHF. **Allowed Values**: 0-31
CHF_NOTIFY_REQUEST_PRIORITY	18	CHF notification. **Allowed Values**: 0-31

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-85 (Cont.) Advanced Settings for Congestion Control

Key	Default Value	Allowed Values
UDR_CONGESTION_RESPONSE_CODE	503	This key is used for configuring congestion response code for UDR. You can configure any valid non-2xx response codes only. If any invalid value is provided, then the requests is rejected with default 503 response code.
CHF_CONGESTION_RESPONSE_CODE	503	This key is used for configuring congestion response code for CHF. You can configure any valid non-2xx response codes only. If any invalid value is provided, then the requests is rejected with default 503 response code.
UDR_ADD_3GPP_SBI_MSG_PRIORITY	false	This key decides if the user wants to send `3gpp-sbi-message-priority` header to Egress Gateway and NRF Client or not from UDR Connector. **Allowed Values**: `true/false`
CHF_ADD_3GPP_SBI_MSG_PRIORITY	false	This key decides if the user wants to send `3gpp-sbi-message-priority` header to Egress Gateway and NRF Client or not from CHF Connector. **Allowed Values**: `true/false`
CHF_CONNECTOR_TIMEOUT_GUARD	number	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
UDR_CONNECTOR_TIMEOUT_GUARD	number	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
PDS_CONNECTOR_TIMEOUT_GUARD	number	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-85 (Cont.) Advanced Settings for Congestion Control

Key	Default Value	Allowed Values
IMM_REP_CAPABILITY_CHECK	Boolean	If this configuration is disabled in the advance settings, the PCF will bypass the capability check for UDR and transmit a POST request with immediate reporting. Otherwise, it will perform the capability check and subsequently determine whether to send a GET+POST or a POST request. **Default value**: true

5. Click **Save**.
   The page saves the PCF User Connector configurations.

7.3.7 Timer Service

This procedure provides information about configuring the Timer Service

The **Timer Service** page displays the Timer Service configurations. The page allows you to edit the configurations.

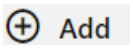
To configure the Timer service:

1. From the navigation menu under **Policy**, navigate to **Service Configurations** and select **Timer Service**.
   This opens the **Timer Service** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit Timer Service** page.
3. Enter values for the following input fields, as described in the following table:

Table 7-86 Edit Timer Service

Field Name	Description
Timer Enabled	Toggle to enable or disable timer service. (if disabled then processing of timers and sending notification will not be done). **Default value**: false

4. Perform the following steps to configure **Advanced Settings**:
   a. Click 

      The page opens the **Add Advanced Settings** dialog box.
   b. In the dialog box, enter the following **key** and respective **value**:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-87 Advanced Settings for Timer Service

Key	Value	Description
TIMER_EXP_RANGE_MIN_SEC	20	This indicates the minimum expiry range for creation of timers, beyond which timers cannot be created. The default value is 20 (timers in range of grace interval are supported). **Note**: When both Reattempt after Back-off and retryAfter features are enabled, the value of `TIMER_EXP_RANGE_MIN_SEC` key must be set to 1.
TIMER_EXP_RANGE_MAX_SEC	2678400	This indicates the maximum expiry range for creation of timers, beyond which timers cannot be created.
TIMER_NOTIFICATION_RETRY_MAX_COUNT	3	This indicates the maximum retry count for sending timer notification.
TIMER_STALE_INTERVAL_SEC	300	This indicates the interval after which an expired timers can be marked as stale.
TIMER_STUCK_INTERVAL_SEC	3600	This indicates the interval after which an expired timer can be marked as stuck.
TIMER_NOTIFY_ON_STUCK	true	This indicates a flag to enable or disable notifications from a timer that is in stuck state.
TIMER_SCAN_HEART_BEAT_ACTIVITY_FREQUENCY	1	This indicates the frequency to run heart beat activity between the self and fostered pods. This is responsible for updating the heartbeat of self and fostered pods. By default, the frequency is set to 1 cycle. This activity runs every time timer scan runs, and by default the scan runs every 30 seconds, hence the heartbeat activity will run every 30 seconds
TIMER_SCAN_ORPHAN_LOCAL_ACTIVITY_FREQUENCY	2	This indicates the frequency to run orphan local scan activity for checking the dead pods on `local site` and them if necessary. The default frequency is set to 2 cycles. This activity runs every time timer scan runs, and by default the scan runs every 30 seconds, hence the orphan local scan will run every 60 seconds.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-87 (Cont.) Advanced Settings for Timer Service

Key	Value	Description
TIMER_SCAN_ORPHAN_REMOTE_ACTIVITY_FREQUENCY	4	This indicates the frequency to run orphan remote scan activity for checking the dead site and adopt them if necessary. The default frequency is set to 4 cycles. This activity runs every time timer scan runs, and by default the scan runs every 30 seconds, hence the orphan remote scan will run every 120 seconds.
TIMER_SCAN_CLEAN_UP_ACTIVITY_FREQUENCY	1000	This indicates the frequency to perform cleanup of dead and fostered records. The default frequency is set to 1000 cycles.
MISSED_HB_CYCLES_TO_CONSIDER_POD_DEAD	2	This indicates the missed heartbeat cycles since the pods last heartbeat update after which the pod will be considered dead. The default frequency is set to 2 cycles.
MISSED_HB_CYCLES_TO_CONSIDER_SITE_DEAD	60	This indicates the missed heartbeat cycles since the pod site's last heartbeat update after which the site will be considered dead. The default frequency is set to 60 cycles. **Note**: A site is considered dead when no pod belonging to the site has updated its heartbeat for configured cycles.
MAX_NUM_OF_DAYS_TO_KEEP_DEAD_POD_RECORD_KEY	32	This indicates the maximum number of days since a pod that did its adoption will keep the dead pod record and also the adoption records in the database. The default maximum number of days to keep dead pod records is 32. Once the configured days are over the pod did the adoption during its clean up activity will remove the records from the database. **Note**: The configured value should be more than maximum configurable timer value in Reattempt Profile in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-87 (Cont.) Advanced Settings for Timer Service

Key	Value	Description
TIMER_COUNT_SYNCHRONIZATION_ACTIVITY_FREQUENCY	1440	This indicates the frequency to run timer count synchronization activity wherein we check synchronize timer count of timer registration records with actual timer record count in Timer table, default timer count sync activity will run every 1440th cycle of Timer Scan. By default, timer Scan runs every 30 second so timer count synchronization activity will be executed every 12 hours. **Note**: Since this activity is a database intensive operation this should be configured to large values. Also to completely disable this activity the key value should be set to a value <= 0, and also below advanced setting key TIMER_COUNT_SYNCHRONIZATION_ACTIVITY_DAILY_SCHEDULED_TIME_IN_UTC key should not be configured.
TIMER_COUNT_SYNC_ACTIVITY_DAILY_TIME_UTC	NA	Indicates a configuration key to override the default frequency-based timer count synchronization logic. It enables the scheduling of the synchronization activity to occur once daily at a specified UTC time. This customization ensures efficient timer management. The time format follows the ISO-8601 extended local time format, represented as hh:mm:ss, where hh is the hour (00-24), mm is minutes (00-59), and ss is seconds (00-60). For example, 08:15:45 or 08:15."

5. Click **Save**.
   The page saves the Timer Service configurations.

   To discard the changes, click **Cancel**.

7.3.8 Configuring Usage Monitoring

This procedure provides information about managing configurations for Usage Monitoring service.

The Usage Monitoring page allows you to edit default Usage Monitoring configurations.

To configure, perform the following steps:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the navigation menu, under **Policy**, click **Service Configurations**, and select **Usage Monitoring**.
   This opens the Usage Monitoring page with the default configurations.
2. Click **Edit**.

   This opens the Edit Usage Monitoring page.
3. Enter values for the input fields, described in the following table:

Table 7-88 Usage Monitoring Configurations

Field Name	Description
Enable PRE	Specifies whether to enable or disable interaction with PRE for Policy evaluation as per the match list.
Minimum Volume Grant (bytes)	Enter the minimum grant value (in bytes) that can be approved for volume based usage monitoring. If the grant value published by PRE is less than the value for this field, then Policy considers the minimum grant value out of the two. After deducting the current grant, if the remaining grant value is less than the minimum grant value, then the remaining grant is also added to the current grant. **Default value**: 2048 **Range**: 512 - 1048576 (1MB)
Maximum Volume Grant (bytes)	Enter the maximum grant value (in bytes) that can be approved for volume based usage monitoring. If the grant value published by PRE is greater than the value for this field, then Policy considers the maximum grant value out of the two. **Default value**: 2048 Range: 1024- 1000,000,000,000
Minimum Time Grant (seconds)	Enter the minimum grant value (in seconds) that can be approved for time based usage monitoring. If the grant value published by PRE is less than the value for this field, then Policy considers the minimum grant value out of the two. After deducting the current grant, if the remaining grant value is less than the minimum grant value, then the remaining grant is also added to the current grant. **Default value**: 300 Range: 30 - 3600 (1 hour)
Maximum Time Grant (seconds)	Enter the maximum grant value (in seconds) that can be approved for time based usage monitoring. If the grant value published by PRE is greater than the value for this field, then Policy considers the maximum grant value out of the two. **Default value**: 21600 (6 hours) Range: 1 - 31536000 (1 year)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-88 (Cont.) Usage Monitoring Configurations

Field Name	Description
Inactivity Time (seconds)	Enter the time interval (in seconds) during which if no packets are received for a given monitoring key, PGW or SMF stops measuring the time. **Default value**: 86400 Range: 0 - 604800 (7 Days)
Usage Accumulation Start Date and Time	Select the start time and date from when the Usage Monitoring service starts counting the usage reset periodicity. The values are: • **Plan Start Date and Time**: Counted from the plan start date and time as provisioned on the UDR. • **Plan Activation Date and Time**: Counted from the plan activation date and time as provisioned on the UDR. • **Period Start Date and Time**: Counted from the period start date and time.
Week Start Day	Enter the starting day of the week. **Default value**: Sunday
Default Data Rollover Profile	Indicates the default data rollover profile to use for UDR provided data limits for which rollover is applicable. That is, "Data Rollover" attribute is set to "true" and a separate "Data Rollover Profile" attribute is not provided.
Enable Quota Migration	Indicates whether to enable retrieval of OCPM data from CnUDR. If enabled, CnPCRF interacts with CnUDR to collect the quota details of the OCPM (4G) subscribers. **Default value**: false **Note**: Disabling this flag while Subscriber Data Migration from OCUDR (4G) to CnUDR (5G) is incomplete may result in Quota loss. It is recommended to not fallback to OCPM PCRF once this flag is disabled as after this, the data provided to OCPM PCRF may NOT be up to date.
Reverse Priority	Indicates the priority consideration order. When this flag is enabled: Higher number indicates lower priority When this flag is disabled: Higher number indicates higher priority **Default value**: `false`
Enable Pro-rated Data at The Time of Activation	Indicates whether pro-rated data calculation should be applied to the selected plan at a time of activation or not. **Default value**: false
Enable Pro-rated Data at The Time of Billing Day Change	Indicates whether pro-rated data calculation should be applied to the selected plan at a time billing day change . **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-88 (Cont.) Usage Monitoring Configurations

Field Name	Description
Apply Billing Day / Data Plan Change	Indicates if the flexible billing cycle option is enabled. The accepted values are: • Current Billing Cycle • Next Billing Cycle **Default value**: Next Billing Cycle
Data Compression Scheme	Used to configure the data compression in UmContext table. This flag accepts the following values: • `Disabled`: Indicates that the data will not be compressed and will be stored in the column in uncompressed format. The value of `COMPRESSION_SCHEME` for that row is set to the default value 0. • `MySQL Compressed`: Indicates that the data will be compressed using MySQL and will be stored in the column in compressed format. The value of `COMPRESSION_SCHEME` for that row is set to 1. • `Application Compressed`: Indicates that the data will be compressed using Zlib and will be stored in the column in compressed format. The value of `COMPRESSION_SCHEME` for that row is set to 2. **Default value**: Disabled When accessing the data from `UmContext .v`, the application determines the compression status based on the value of `COMPRESSION_SCHEME` and does the decompression accordingly. For more details on data compression, see *Data Compression in Usage Monitoring* section in Usage Monitoring on Gx Interface.
Default Volume Grant	Provide Default Volume Grant details:
Grant Unit	Select a value from the drop-down list: • **Percent**: Grant volume is calculated as a percentage. • **Bytes**: Grant volume is calculated as an absolute value. **Default value**: Percent

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-88 (Cont.) Usage Monitoring Configurations

Field Name	Description
Grant Value (Percent)	**Note**: This field becomes active when you select **Grant Unit** as percent. Enter the default Grant Volume in percentage, which is considered when PRE is not invoked or PRE does not return a decision. This value is applied to the Total Volume and divided equally among the Uplink and Downlink Volumes when available. **Default value**: 10 **Range**: 1-100 When the grant value is 0 and Grant is not calculated by PRE, then volume based Usage Monitoring is disabled for the session.
Grant Value (Bytes)	**Note**: This field becomes active when you select **Grant Unit** as Bytes. Enter the default Grant Volume in Bytes, which is considered when PRE is not invoked or PRE does not return a decision. This value is applied to the Total Volume and divided equally among the Uplink and Downlink Volumes when available. **Default value**: 2048 **Range**: 512 - 1048576 (1 MB) When the grant value is 0 and Grant is not calculated by PRE, then volume based Usage Monitoring is disabled for the session.
Grant Source	**Note**: This field becomes active when you select **Grant Unit** as Percent. Select a value from the drop-down list: • **Initial Volume**: Calculate grant volume from the initial volume. • **Used Volume**: Calculate grant volume from the used volume. • **Remaining Volume**: Calculate grant volume from the remaining volume. **Default value**: Initial Volume
Default Time Grant	Provide Default Time Grant values:
Grant Unit	Select a value from the drop-down list: • **Percent**: Grant time is calculated as a percentage. • **Seconds**: Grant time is calculated as an absolute value. **Default value**: Percent

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-88 (Cont.) Usage Monitoring Configurations

Field Name	Description
Grant Value (Percent)	**Note**: This field becomes active when you select **Grant Unit** as percent. Enter the default Grant time in percentage, which is considered when PRE is not invoked or PRE does not return a decision. **Default value**: 10 **Range**: 1-100 When the grant value is 0 and grant is not calculated by PRE, then time based Usage Monitoring is disabled for the session.
Grant Value (seconds)	**Note**: This field becomes active when you select **Grant Unit** as seconds. Enter the default Grant time in seconds, which is considered when PRE is not invoked or PRE does not return a decision. **Default value**: 3600 **Range**: 30 - 86400 (1 day) When the grant value is 0 and grant is not calculated by PRE, then time based Usage Monitoring is disabled for the session.
Grant Source	**Note**: This field becomes active when you select **Grant Unit** as Percent. Select a value from the drop-down list: • **Initial Duration**: Calculate grant time from the initial duration. • **Used Duration**: Calculate grant time from the used duration. • **Remaining Duration**: Calculate grant time from the remaining duration. **Default value**: Initial Volume
Default Usage Levels	Provide Default Usage Levels details:
Minor Usage Level (%)	Enter threshold value in percentage indicating minor usage. **Default value**: 50
Major Usage Level (%)	Enter threshold value in percentage indicating major usage. **Default value**: 75
Critical Usage Level (%)	Enter threshold value in percentage indicating critical usage. **Default value**: 95
Exhausted Usage Level (%)	Enter threshold value in percentage indicating usage level has exhausted allowed limit. **Default value**: 100
Custom Attribute Mapping	Provide Custom Attribute Mapping details:
Reset Day & Time	Enter a string identifying the custom attribute in UDR response that represents the usage reset day. **Example**: `SmPolicyData/umDataLimits/{limitId}/billingDay`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-88 (Cont.) Usage Monitoring Configurations

Field Name	Description
Data Plan Name	To map the custom attribute available in the UDR provided data limit to name. A "name" associated with the data limit can be used in a Selection Profile to select the plan to apply when multiple active plans are found. **Default value**: SmPolicyData/umDataLimits/{limitId}/name
Data Plan Priority	To map the custom attribute available in the UDR provided data limit to priority. A "priority" associated with the data limit would help to select the plan to apply when multiple active plans are found. Possible values allowed in this field in UDR Data Limit are: any integer. **Default value**: SmPolicyData/umDataLimits/{limitId}/priority
Data Plan Type	To map the custom attribute available in the UDR provided data limit to type. A "type" associated with the data limit would help to order the selection of the plan. Possible values are: "base", "pass", "top-up". A separate configuration would order the selection, for example: Pass > Base Plan > Top-up. Default: SmPolicyData/umDataLimits/{limitId}/type Default value: base **Note**: The Plan Type, Priority within that Plan Type and the Selection Order of Plan Types together decide the order of selection of Data Plans.
Data Rollover	To map the custom attribute available in the UDR provided data limit to indicate whether rollover is enabled for this data limit. Possible values allowed in this field in UDR Data Limit are: "true" and "false". **Default value**: SmPolicyData/umDataLimits/{limitId}/rollover Default value to apply if this mapped attribute is absent: false
Data Rollover Profile	To map the custom attribute available in the UDR provided data limit to a pre-configured rollover profile. See "Data Rollover Profile" for more information. Possible values allowed in this field in UDR Data Limit are: A "Data Rollover Profile" name pre-configured on Policy. **Default value**: SmPolicyData/umDataLimits/{limitId}/rolloverProfile

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-88 (Cont.) Usage Monitoring Configurations

Field Name	Description
Parent Plan Name	To map the custom attribute available in the UDR provided data limit to parent plan name. Attributes not present in the UmDataLimit shall be picked up from the "parent" (if present). The parent plan name may be a configured Data Limit Profile Name. **Default value**: SmPolicyData/umDataLimits/{limitId}/parent
Parent Plan Source	To map the custom attribute available in the UDR provided data limit to parent plan source. A parent plan source "parent" (if present). The parent plan name may be a configured Data Limit Profile Name. Possible values allowed in this field in UDR Data Limit are: "data-limit-profile", "um-data-limit". **Default value**: SmPolicyData/umDataLimits/{limitId}/parentSource Default value to apply if this mapped attribute is absent: "data-limit-profile"

4. To add selection proles for the **Data Limit Selection**, perform the following configurations:

Table 7-89 Data Limit Selection

Field Name	Description
Default Data Limit Profile	Indicates the default data limit profile to apply when no (usable) data limits were obtained from UDR and no (usable) data limits were applied by policy.
Default Data Limit Selection Profile	Indicates the default data limit selection profile to use while selecting a data limit among more than one active data limits provided by UDR.
Default Data Limit Sorting Profile	Indicates the default data limit sorting profile to use while selecting a data limit among more than one active data limits provided by UDR.
Selection Order 1	Selection Order determines the order/priority of selection of different types of plans. Default Value of Selection Order 1 : Pass
Selection Order 2	Default Value of Selection Order 2 : Base Plan
Selection Order 3	Default Value of Selection Order 3: Top-Up

5. Enter values for the input fields, described in the following table:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-90 Conflict Resolution Configurations

Field Name	Description
Enable ETag / If-Match headers	Indicates if the ETag functionality is enabled or disabled between PDS and UDR. By default, this is disabled. Following scenarios may occur if it is enabled: • When the Usage Monitoring service sends a GET request for the first time, then PDS will fetch latest ETag details from UDR and update it in THE pdssubscriber table. • when the Usage Monitoring service sends PATCH request to PDS, PDS sends the request to UDR using if-match header. UDR matches the ETag of PDS with UDR. If it matches, then UDR replies with the latest ETag that gets updated on PDS. • If the If-Match headers fails, it means ETag on PDS does not match with UDR. UDR replies with 412 error response and based on the response code, Usage Monitoring service sends a force request to PDS to get the latest ETag from UDR and update it on PDS database.
Maximum Number of Conflict Resolution Attempts	Specifies the number of retry the Usage Monitoring service will do when if-match will fail on UDR. Default value: 5

6. Enter values for as described in the following table to configure audit cycles for Usage Monitoring Gx sessions:

Table 7-91 Audit Configurations

Field Name	Description
Enable	Used to enable or disable the Audit registration for Usage Monitoring service. When this field is enabled, Usage Monitoring sends registration request to Audit service. When this field is disabled, Usage Monitoring sends de-registration request to Audit service. **Default value**: true
Notification Rate (per second)	Indicates the number of stale records that Audit service notifies to Usage Monitoring service in one second. Value of this parameter ranges between 20 and 700. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-91 (Cont.) Audit Configurations

Field Name	Description
Policy Association Age (in minutes):	Indicates the age of a Usage Monitoring session, after which the session is considered to be stale and the PCRF Core service is queried for the presence of such associations. **Note**: This value should be higher than the Gx session audit. Value of this parameter ranges between 1 and 10080. **Default Value**: 1440
Policy Association Maximum Age (in minutes):	Indicates the maximum age of a UMPolicyAssociation, after which the session is purged from UMContext database without sending further queries. **Note**: This value should be higher than the Gx session audit. Value of this parameter ranges between 1 and 20160. **Default Value**: 2880
Minimum Audit Attempts	Indicates the minimum number of queries to PCRF Core service before deleting a session. **Range**: 0-255 **Default Value**: 0
Minimum Audit Passes Interval (in minutes)	Defines the time when next audit for the Usage Monitoring service table is done after delta time if auditing this table has been finished before this specified time. **Default Value**: 10

7. Enter values for the input fields, described in the following table to configure message priorities for Congestion Control in Usage Monitoring:

Table 7-92 Message Default Priority for Congestion Control Configurations

Field Name	Description
UM Session Create API	Set request priority for UM session creation (CCR-I) request. **Allowed Values**: 0-31 **Default Value**: 20
UM Session Update API	Set request priority for UM session update (CCR-U) request. **Allowed Values**: 0-31 **Default Value**: 17
UM Session Terminate API	Set request priority for UM session terminate (CCR-T) request. **Allowed Values**: 0-31 **Default Value**: 15

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-92 (Cont.) Message Default Priority for Congestion Control Configurations

Field Name	Description
UM Session Notify API	Set request priority for UM session notification request. **Allowed Values**: 0-31 **Default Value**: 17
UM Session Search Subscriber API	Set request priority for UM session search for subscriber request. **Allowed Values**: 0-31 **Default Value**: 30
UM Session Audit Notify API	Set request priority for terminate session (CCR-T) request. **Allowed Values**: 0-31 **Default Value**: 31
Congestion Error Code	Configure the response code of the any rejected requests by Usage Monitoring due to congestion state. By default, Usage Monitoring sends 503 as response code. If configured then it shall be 5xx only. **Allowed Values**: 5xx **Default Value**: 503

8. Perform the following steps to configure **Advanced Settings** for Usage Monitoring:

   a. Click the ⊕ Add
   The page opens the **Add Advanced Settings** dialog box.

   b. In the dialog box, enter the following **keys** and respective **values**:

The following table describes the keys and values:

Table 7-93 Add Advanced Settings Configurations

Key	Value
PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT	Used to configure the previous slicing count for UMContext table. If `UM_CONTEXT_TABLE_SLICING_COUNT` Helm parameter is changed and the Usage Monitoring service cannot find the data with the current slicing count, it uses `PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT` to search for the data. If there are multiple values for `PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT`, the Usage Monitoring service uses the latest previous count and if the data is still not found, it uses the next previous count. That is, if `PREVIOUS_UM_CONTEXT_TABLE_SLICING_COUNT` contains two values such as 0,5, the Usage Monitoring service first uses the previous count as 5 to search for the data. If it is still not found, the service uses the previous count as 0 to search for the data. **Default value**: 0

Copyright © 2019, 2026, Oracle and/or its affiliates.

9. Click **Save** to save Usage Monitoring service configurations.

7.3.9 PCRF Core Service Configurations

This section describes how to configure the PCRF Core service.

To access PCRF Core service configurations from CNC Console home page, expand **Policy**, navigate to **Service Configurations** and select **PCRF Core**.

On clicking PCRF Core, you can select to customize any of the following configurations:

- Settings
- Serving Gateway
- Network Element

7.3.9.1 Settings

This procedure provides information about configuring the PCRF Core settings.

The **Settings** page under **PCRF Core** displays the PCRF Core service settings. The page allows you to edit the configurations.

To edit the PCRF Core settings:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **PCRF Core**, and select **Settings**.
   This opens the **Settings** page. The page displays the existing settings for PCRF Core service.
2. Click Edit .
   This opens the **Edit Settings** page.
3. Expand the **User** group, to enable or disable switches, described in the following table:

Table 7-94 User Group Settings

Field Name	Description
Validate User	If the User profile, for any of the User Data types given under the **User Data Types** group, are fetched successfully, the user is considered to be a known user. However, if the user profile lookup has failed on all the configured data sources, the user profile is marked as Unknown. If this switch is enabled and user is marked as Unknown, the session creation requests are rejected. If this switch is disabled and user is marked as Unknown, the session creation requests are handled and sessions are created successfully.
Enable Subscriber Variables	If this switch is enabled, PCRF Core controls the querying and saving of remote subscriber state variables (SSV) on PDS. When CCR message is received by PCRF Core, then it queries PDS to fetch SSV for the user, instead of retrieving it locally. By default, the switch remains disabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-94 (Cont.) User Group Settings

Field Name	Description
User Data Types	Provide **User Data Types** details:
SmPolicyData	If this switch is enabled, PCRF-Core fetches SMPolicyData from nUDR. To configure the SMPolicyData attributes, see SmPolicyData Attributes.
Operator Specific Data	If this switch is enabled, PCRF fetches OperatorSpecificData (imported using Custom Schema) from nUDR. To configure the SMPolicyData attributes, see Table 7-96.
Ldap Data	If this switch is enabled, PCRF-Core fetches user profile from LDAP through PDS.
OCS Spending Limit	If this switch is enabled, PCRF-Core fetches policy counters for a subscriber from 4G OCS. Irrespective of whether OCS is configured as primary datasource or on-demand datasource, this switch must be enabled to retrieve policy counters. To configure the OCS spending limit attributes, see Table 7-97.

The following table describes the **SmPolicyData** switches available in the **Attributes** column:

Table 7-95 SmPolicyData Attributes

Attribute Name	Description
Subscribe to Notify	When this switch is enabled, PCRF Core subscribes with the UDR to get notified on changes in subscriber profile. **Note**: When this switch is disabled, Usage Monitor feature cannot be tested. It will not be functional. By default, this option is false.
Query User on Update	Determines if user query from UDR on update is enabled. When this option is enabled, PCRF Core queries the UDR about the subscriber present in the CCR request or GX message by sending a GET request for “SmPolicyData” resource on the nudr-dr service. **Note**: If `Subscribe To Notify` is enabled for PCRF Core, then PCRF services will not query the UDR during a Update requests. The PDS caches the subscriber profile when the “Subscribe To Notify” option is enabled, in that case, the PCRF core may not always reach the UDR when the subscriber profile is found in the local cache. By default, this option is disabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-95 (Cont.) SmPolicyData Attributes

Attribute Name	Description
Query User on Terminate	Determines if user query from UDR on delete is enabled. When this option is enabled, PCRF Core queries the UDR about the subscriber present in the CCR request or the GX message by sending a GET request for “SmPolicyData” resource on the nudr-dr service. **Note**: If `Subscribe To Notify` is enabled for PCRF Core, then PCRF service will not query the UDR during a Terminate requests. The PDS caches the subscriber profile when the “Subscribe To Notify” option is enabled, in that case, the PCRF Core may not always reach the UDR when the subscriber profile is found in the local cache. By default, this option is disabled. **Note** It should be enabled only when subscription to UDR is disabled. It should not be enabled if subscription to UDR is enabled.
Query User on Reauth	Determines if user query from UDR on reauth is enabled. When this option is enabled, PCRF Core queries the UDR about the subscriber, when it receives a Reauthorization request, such as Rx or Policy Authorization request by sending a GET request for “SmPolicyData” resource on the nudr-dr service. **Note:** The PDS caches the subscriber profile when the “Subscribe To Notify” option is enabled, in that case, the PCRF Core may not always reach the UDR when the subscriber profile is found in the local cache. By default, this option is disabled.
Auto Enrollment on UDR	To specify whether to enable or disable the auto provisioning of the subscriber profile at UDR when the subscriber profile is not available.
Default-S-NSSAI	To configure a default S-NSSAI, which will be used when a subscriber is auto-enrolled on the UDR. This parameter is applicable only when Auto-Enrollment on UDR is set to `true`. The value configured here must match the Default S-NSSAI configured on UDR.

The following table describes the **Operator Specific Data** switch available in the **Attributes** column:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-96 Operator Specific Data Attributes

Attribute Name	Description
Subscribe to Notify	When this switch is enabled, PCRF Core subscribes to get notified of any changes in the profile. By default, this option is true.

The **OCS Spending Limit** switches available in the **Attributes** column:

Table 7-97 OCS Spending Limit Attributes

Attribute Name	Description
Async Query	When this switch is enabled, PCRF Core performs on-demand lookup of Policy Counters for a subscriber using the **Fetch Policy Counters** from *OCS* policy action. By default, this option is disabled.
Enable force lookup on Update	When this switch is enabled, the core services (PCRF Core and SM) sends OCS request skipping the PDS optimizations. By default, this option is disabled.

4. Under the **Usage Monitoring** group, update the values for the fields, described in the following table:

Table 7-98 Usage Monitoring Settings

Field Name	Description
Enabled	Specifies whether to enable or disable Usage Monitoring service for PCRF. By default, this switch is `disabled`.
APN List	Specifies the list of APNs for which usage monitoring is enabled. If you leave this field empty, Usage Monitoring is enabled for all APNs.
Attribute Forwarding	**To configure the attribute forwarding details.**
Interface Type	Indicates the interface type for which the profile applies. For more details on Attribute Forwarding Profiles, see *Attribute Forwarding Profiles* section in Usage Monitoring on Gx Interface.
Message Type	Indicates the message type for which the profile applies.
Forwarding Profile	Refers to the configured Attribute Forwarding Profile.

5. Under **MCPTT** group, apply the configurations to set the default ARP and default preemption control.

Table 7-99 MCPTT Settings

Parameter	Description
Default ARP Settings	**To configure the default ARP details.**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-99 (Cont.) MCPTT Settings

Parameter	Description
Priority Level	Indicates the priority level. Range: 1-15 Default Value: 1
Preemption Capability	Indicates if the preemption capability is enabled or disabled. It can take the following values: • PREEMPTION_CAPABILITY_ENABLED • PREEMPTION_CAPABILITY_DISABLED Default Value: PREEMPTION_CAPABILITY_ENABLED
Preemption Vulnerability	Indicates if the preemption vulnerability is enabled or disabled. It can take the following values: • PREEMPTION_VULNERABILITY_ENABLED • PREEMPTION_VULNERABILITY_DISABLED Default Value: PREEMPTION_VULNERABILITY_DISABLED
Default Preemption Control	**To configure Default Preemption Control details.**
Default Preemption Control info	Includes the Default Preemption Control information: • LEAST_RECENT_ADDED_FLOW • MOST_RECENT_ADDED_FLOW • HIGHEST_BANDWIDTH_FLOW Default Value: LEAST_RECENT_ADDED_FLOW

6. Expand the **Audit** group, and update the values for the fields described in the following table:

Table 7-100 Audit Group Settings

Field Name	Description
Enabled	Determines whether to send registration request to Audit service or not. By default, this switch is enabled.
Notification Rate (per second)	Defines the number of stale records which Audit service notifies to PCRF Core service in one second. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)
Policy Association Age (in minutes) for Gx Session	Defines the age of a Gx session after which a record is considered to be stale on PCRF Core and the PGW is queried for presence of such associations. **Default Value**: 1440

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-100 (Cont.) Audit Group Settings

Field Name	Description
Policy Association Maximum Age (in minutes) for Gx Session	Defines the maximum age of a Gx session after which a record is purged from PCRF Core database (Gx Session table) without sending further queries to PGW. **Default Value**: 2880
Minimum Audit Attempts for Gx session	Specifies the minimum number of consecutive failed audit attempts until maxTTL / forceTTL is reached. If maxTTL is reached and audit_attempts >= Minimum Audit Attempts for maxTTL, Audit service sends notification to PCRF Core service with maxTTL flag set to *true*. PCRF Core service triggers the TERMINATE (CCR-T) leg. **Range**: 0-255 **Default Value**: 0 **Note**: If maxTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until maxTTL is reached.
Policy Association Age (in minutes) for Rx Session	Defines the age of an Rx session after which a record is considered to be stale on PCRF Core. When the **maxTTL** flag is **TRUE**, Rx sessions are cleaned. **Note**:The cleanup functionality is not implemented for Rx sessions, if the**maxTTL** flag is **false** **Default Value**: 1440
Policy Association Maximum Age (in minutes) for Rx Session	Defines the maximum age of an Rx session after which a record is purged from PCRF Core database (Rx Session table) without sending further queries to PGW. **Default Value**: 2880
Policy Association Age (in minutes) for Sd Session	Defines the age of an Sd session after which a record is considered to be stale on PCRF Core. **Default Value**: 1440
Policy Association Maximum Age (in minutes) for Sd Session	Defines the maximum age of an Sd session after which a record is purged from PCRF Core database (Sd Session table) without sending further queries to PGW. **Default Value**: 2880

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-100 (Cont.) Audit Group Settings

Field Name	Description
Minimum Audit Attempts for Sd session	Specifies the minimum number of consecutive failed audit attempts until maxTTL / forceTTL is reached. If maxTTL is reached and audit_attempts >= Minimum Audit Attempts for maxTTL, Audit service sends notification to PCRF Core service with maxTTL flag set to *true*. PCRF Core service triggers the TERMINATE (CCR-T) leg. **Range**: 0-255 **Default Value**: 0 **Note**: If maxTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until maxTTL is reached.
Minimum Audit Passes Interval (in minutes)	Defines the time when next audit for the PCRF Core service table begins after delta time if auditing this table has been finished before this specified time. **Default Value**: `330`

7. Enter the values for the input fields, available under the **Pending Transaction** group. The following table describes the fields:

Table 7-101 Edit Pending Transaction Configurations

Field Name	Description
Enabled	Specifies whether to enable or disable Pending Transaction. By default, this switch is `disabled`.
RAR Retry Backoff (in milliseconds)	Indicates the time gap between the consecutive retry RAR messages when PGW is sending error response with cause of DIAMETER_PENDING_TRANSACTION and RAR message is triggered by PDS/AF/PRE. **Default Value**: `1000`
RAR Retry Count	Indicates the count for RAR messages when PGW is sending error response with cause of DIAMETER_PENDING_TRANSACTION and RAR message is triggered by Notification message from PDS/AF/PRE. **Default Value**: 2
User Notify Reauth Error Handling	Indicates if an RAR initiated by User Notification message need to be discarded or retried when it is responded by P-GW with an error of DIAMETER_PENDING_TRANSACTION. **Default Value**: RETRY
AF Reauth Error Handling	Indicates if an RAR initiated by AF message should be discarded or retried when it is responded by PGW with an error of DIAMETER_PENDING_TRANSACTION. **Default Value**: RETRY

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-101 (Cont.) Edit Pending Transaction Configurations

Field Name	Description
Reauth Error Handling:	Indicates if an RAR initiated by any message should be discarded or retried when it is responded by PGW with an error of DIAMETER_PENDING_TRANSACTION. **Default Value**: RETRY

8. Perform the following steps to configure Advanced Settings that allows PCRF Core to handle concurrent requests:

   a. Click the Add
   The page opens the **Add Advanced Settings** dialog box.

   b. In the dialog box, enter the following **keys** and respective **values**:

The following tables describe the keys and values:

Table 7-102 General

Key	Default Value
CONCURRENCY.ENABLED	false
Gx.DisableSupportedFeatures	false
Rx.DisableSupportedFeatures	false
SY.OptimizationType	This key is used for optimization handling of reauthorization flows triggered by OCS notifications. This affects notification-driven optimization behavior and may be relevant in deployments using Async OCS or related flows. Possible values: • NO_OPTIMIZATION: always send RAR. • RULES_MATCH: do not send RAR if rules did not change. • EVERYTHING_MATCHES: do not send RAR if rules and QoS did not change.
DISTRIBUTE_GX_TRAFFIC_USING_TABLE_SLICING	When this key is enabled, traffic for Gx Sessions are distributed across all the new tables. PCRF Core service will register the new tables with Audit Service and also distributes the new sessions to the new slices. **Default value**: false
USER.ocsSpendingLimit.resetContextOnGxCreate	When the value of this key is set to `true`, PCRF Core sets `resetContext` to `true` in PDS request reqParam for the first Gx session and PDS will revalidate the Sy session. **Default value**: false
sbi.timer.enabled	When the value of this key is set to `true`, PCRF-Core handles the following HTTP SBI headers at incoming and outgoing requests: • 3gpp-Sbi-Origination-Timestamp • 3gpp-Sbi-Max-Rsp-Time • 3gpp-Sbi-Sender-Timestamp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-102 (Cont.) General

Key	Default Value
RESOURCEID.SUFFIX_LIST	When both IMSI and GPSI keys are present in the request/session, and if `bulwark.service.enabled` is enabled for that request, `RESOURCEID.SUFFIX_LIST` setting allows to choose the userID key(s) which will be sent to make the lock request. Possible values: • " " (<empty string>): This is the default setting which sends IMSI key if available and GPSI key if available. • `IMSI`: If both IMSI and GPSI keys are present it will only send IMSI key. • `GPSI`: If both IMSI and GPSI keys are present it will only send GPSI key. • `IMSI, GPSI`: Same as empty string, this sends IMSI key if available and GPSI key if available **Default value**: empty string
DIAMETER.Gx.Update.AllowedOptionalEventTriggers	On CCR-U, for each of the event triggers present in this setting, if the request contains the required AVP fields to match as if the event trigger was part of the request as well, then the event trigger will be added as if it came in the request. Supported event triggers can be mentioned in comma separated list or an empty field denoting no triggers. **Default value**: ACCESS_NETWORK_INFO_REPORT
DIAMETER.ENF.AFDirectReply.SendRarAfterAAA	If DIAMETER.ENF.AFDirectReply and this parameter are true, then this setting will ensure that the Rx session is saved and AAA is sent before Gx RAR is triggered. **Note**: It is applicable for AAR-I and AAR-U message types and corresponding Gx RAR.
USER.SEQUENTIAL_SSV_UPDATE_AND_TERMINATE	When enabled, if the request triggers SSV_UPDATE towards PDS (which is async) and the response has not yet been received, then the attempt to send DELETE request towards PDS waits until SSV_UPDATE is done or times out. When disabled, PDS delete won't check if SSV_UPDATE is still in progress by the same request. **Default value**: true
USER.allowQueryOnInternalReauth	When enabled, an internal reauth for a Gx session caused by policy (REAUTH_PCEF_TDF_SESSION_WITH_SCOPE) will be able to query PDS by using the same settings for querying PDS on reauth. **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-102 (Cont.) General

Key	Default Value
USER.SEQUENTIAL_SSV_UPDATE_AND_REAUTH_PCEF_SESSION	When enabled, and if USER.allowQueryOnInternalReauth is enabled, the query to PDS will wait until any SSV Update is done from the original request to avoid a race condition in PDS, only applies if SSV Update and internal reauth (REAUTH_PCEF_TDF_SESSION_WITH_SCOPE) are both triggered by the same policy response. **Default value**: true
USER.allowQueryOnInternalReauth	If enabled, an internal reauth for a Gx session caused by policy (REAUTH_PCEF_TDF_SESSION_WITH_SCOPE) will be able to query PDS by using the same settings for querying PDS on reauth. **Default value**: false
USER.SEQUENTIAL_SSV_UPDATE_AND_REAUTH_PCEF_SESSION	If enabled, and if USER.allowQueryOnInternalReauth is enabled, the query to PDS will wait until any SSV Update is done from the original request to avoid a race condition in PDS, only applies if SSV Update and internal reauth (REAUTH_PCEF_TDF_SESSION_WITH_SCOPE) are both triggered by the same policy response. **Default value**: true

Table 7-103 Add Advanced Settings Configurations for Gx CCR-I

Key	Default Value
CONCURRENCY.GX.CREATE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.GX.CREATE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.CREATE.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.CREATE.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.CREATE.ENABLED	True
CONCURRENCY.GX.CREATE.ALLOW_ON_SERVICE_FAILURE	True
USER.ocsSpendingLimit.createContextOnFailure	If this flag is enabled the PCRF Core sends this as a request parameter toward PDS. PDS creates a dummy context for OCS in case of getting error while performing OCS lookup. This will support the PDS when it receives notification from UDR to fetch OCS data. This is applicable for CCR-I and CCR-U messages with Asynchronous flow either set as true or false. **Supported values**: true/false **Default Value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-103 (Cont.) Add Advanced Settings Configurations for Gx CCR-I

Key	Default Value
USER.smPolicyData.createContextOnFailure	If this flag is enabled the PCRF Core sends this as a request parameter toward PDS. At PDS, if it receives an error during SmPolicyData-UDR lookup, then PDS creates a dummy context for SmPolicyData. This creation of dummy context helps, when PDS receives next request for a UDR lookup and this time it is successful, then both the sessions will have the latest SmPolicyData. This is applicable for CCR-I and CCR-U Messages too. **Supported values**: true/false **Default value**: false
USER.operatorSpecificData.createContextOnFailure	If this flag is enabled the PCRF Core sends this as a request parameter toward PDS. At PDS, if it receives an error during operatorSpecificData-UDR lookup, then PDS creates a dummy context for operatorSpecificData. This creation of dummy context helps, when PDS receives next request for a UDR lookup and this time it is successful, then both the sessions will have the latest operatorSpecificData. This is applicable for CCR-I and CCR-U Messages too. **Supported values**: true/false **Default value**: false

Table 7-104 Add Advanced Settings Configurations for Gx CCR-U

Key	Default Value
CONCURRENCY.GX.MODIFY.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.GX.MODIFY.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.MODIFY.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.MODIFY.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.MODIFY.ENABLED	True
CONCURRENCY.GX.MODIFY.ALLOW_ON_SERVICE_FAILURE	True

Table 7-105 Add Advanced Settings Configurations for Gx CCR-T

Key	Default Value
CONCURRENCY.GX.DELETE.LOCK_REQUEST_RETRY_COUNT	2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-105 (Cont.) Add Advanced Settings Configurations for Gx CCR-T

Key	Default Value
CONCURRENCY.GX.DELETE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.DELETE.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.DELETE.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.DELETE.ENABLED	True
CONCURRENCY.GX.DELETE.ALLOW_ON_SERVICE_FAILURE	True

Table 7-106 Add Advanced Settings Configurations for Gx RAR

Key	Default Value
CONCURRENCY.GX.REAUTH.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.GX.REAUTH.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.GX.REAUTH.LOCK_LEASE_DURATION	2000
CONCURRENCY.GX.REAUTH.LOCK_WAIT_DURATION	3000
CONCURRENCY.GX.REAUTH.ENABLED	True
CONCURRENCY.GX.REAUTH.ALLOW_ON_SERVICE_FAILURE	True

Table 7-107 Add Advanced Settings Configurations for SD TSR

Key	Default Value
CONCURRENCY.SD.CREATE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.SD.CREATE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.SD.CREATE.LOCK_LEASE_DURATION	2000
CONCURRENCY.SD.CREATE.LOCK_WAIT_DURATION	3000
CONCURRENCY.SD.CREATE.ENABLED	True
CONCURRENCY.SD.CREATE.ALLOW_ON_SERVICE_FAILURE	True

Table 7-108 List of Keys for Rx AAR-I

Key	Default Value
CONCURRENCY.RX.CREATE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.RX.CREATE.LOCK_REQUEST_RETRY_BACKOFF	1000

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-108 (Cont.) List of Keys for Rx AAR-I

Key	Default Value
CONCURRENCY.RX.CREATE.LOCK_LEASE_DURATION	2000
CONCURRENCY.RX.CREATE.LOCK_WAIT_DURATION	3000
CONCURRENCY.RX.CREATE.ENABLED	true
CONCURRENCY.RX.CREATE.ALLOW_ON_SERVICE_FAILURE	true

Table 7-109 List of Keys for Rx AAR-U

Key	Default Value
CONCURRENCY.RX.MODIFY.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.RX.MODIFY.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.RX.MODIFY.LOCK_LEASE_DURATION	2000
CONCURRENCY.RX.MODIFY.LOCK_WAIT_DURATION	3000
CONCURRENCY.RX.MODIFY.ENABLED	true
CONCURRENCY.RX.MODIFY.ALLOW_ON_SERVICE_FAILURE	true

Table 7-110 List of Keys for Rx STR

Key	Default Value
CONCURRENCY.RX.DELETE.LOCK_REQUEST_RETRY_COUNT	2
CONCURRENCY.RX.DELETE.LOCK_REQUEST_RETRY_BACKOFF	1000
CONCURRENCY.RX.DELETE.LOCK_LEASE_DURATION	2000
CONCURRENCY.RX.DELETE.LOCK_WAIT_DURATION	3000
CONCURRENCY.RX.DELETE.ENABLED	true
CONCURRENCY.RX.DELETE.ALLOW_ON_SERVICE_FAILURE	true

Table 7-111 Bulwark Service Advanced Settings for Http Client and Request Timeout Configurations.

Key	Default Value
bulwark.service.enabled	true
BULWARK.REQUEST.URL	http://ocpcf-occnp-bulwark:8000/v1/locks
BULWARK.REQUEST.TIMEOUT	3000
BULWARK.CONNECTION.HTTP2.ENABLED	true

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-111 (Cont.) Bulwark Service Advanced Settings for Http Client and Request Timeout Configurations.

Key	Default Value
BULWARK.CONNECTION.HTTP2.IDLE.TIMEOUT	600000
BULWARK.CONNECTION.HTTP2.CONNECT.TIMEOUT	3000
BULWARK.CONNECTION.HTTP2.MAX.CONNECTIONS.PER.DESTINATION	6
BULWARK.CONNECTION.HTTP2.MAX.REQUESTS.QUEUED.PER.DESTINATION	5000
BULWARK.CONNECTION.HTTP2.INITIAL.SESSION.RECV.WINDOW	16777216

Table 7-112 PDS Service Advanced Settings for Http Client and Request Timeout Configurations.

Key	Default Value
POLICYDS.REQUEST.URL	http://localhost:8084/pds/v2/user-data
POLICYDS.REQUEST.TIMEOUT	3000
POLICYDS.CONNECTION.HTTP2.ENABLED	false
POLICYDS.CONNECTION.HTTP2.IDLE.TIMEOUT	600000
POLICYDS.CONNECTION.HTTP2.CONNECT.TIMEOUT	3000
POLICYDS.CONNECTION.HTTP2.MAX.CONNECTIONS.PER.DESTINATION	6
POLICYDS.CONNECTION.HTTP2.MAX.REQUESTS.QUEUED.PER.DESTINATION	5000
POLICYDS.CONNECTION.HTTP2.INITIAL.SESSION.RECV.WINDOW	16777216

Table 7-113 PRE Service Advanced Settings for Http Client and Request Timeout Configurations.

Key	Default Value
Policy.PREEngineEnabled	true
PRE.REQUEST.URL	http://localhost:5806/v1/policy/engine/pcrf-core
PRE.REQUEST.TIMEOUT	2000
PRE.CONNECTION.HTTP2.ENABLED	false
PRE.CONNECTION.HTTP11.IDLE.TIMEOUT	600000
PRE.CONNECTION.HTTP11.CONNECT.TIMEOUT	3000
PRE.CONNECTION.HTTP11.MAX.CONNECTIONS.PER.DESTINATION	6
PRE.CONNECTION.HTTP11.MAX.REQUESTS.QUEUED.PER.DESTINATION	5000
PRE.CONNECTION.HTTP11.INITIAL.SESSION.RECV.WINDOW	16777216

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-114 Binding Service Advanced Settings for Http Client and Request Timeout Configurations.

Key	Default Value
BindingService.Enabled	true
BINDING.REQUEST.URL	http://localhost:8080/binding/v1
BINDING.REQUEST.TIMEOUT	3000
BINDING.CONNECTION.HTTP2.ENABLED	false
BINDING.CONNECTION.HTTP2.IDLE.TIMEOUT	600000
BINDING.CONNECTION.HTTP2.CONNECT.TIMEOUT	3000
BINDING.CONNECTION.HTTP2.MAX.CONNECTIONS.PER.DESTINATION	6
BINDING.CONNECTION.HTTP2.MAX.REQUESTS.QUEUED.PER.DESTINATION	5000
BINDING.CONNECTION.HTTP2.INITIAL.SESSION.RECV.WINDOW	16777216

Table 7-115 Usage Monitoring Service Advanced Settings for Http Client and Request Timeout Configurations.

Key	Default Value
USAGEMON.REQUEST.URL	http://localhost:1080/occnp-usage-mon/v1/um-sessions
USAGEMON.REQUEST.TIMEOUT	3000
USAGEMON.CONNECTION.HTTP2.ENABLED	true
USAGEMON.CONNECTION.HTTP2.IDLE.TIMEOUT	600000
USAGEMON.CONNECTION.HTTP2.CONNECT.TIMEOUT	3000
USAGEMON.CONNECTION.HTTP2.MAX.CONNECTIONS.PER.DESTINATION	6
USAGEMON.CONNECTION.HTTP2.MAX.REQUESTS.QUEUED.PER.DESTINATION	5000
USAGEMON.CONNECTION.HTTP2.INITIAL.SESSION.RECV.WINDOW	16777216

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-116 Advanced Settings to exclude specific APNs for the User Data Types

Key	Description
USER.allDataTypes.excludeApns	List the Access Point Names (APNs) for which all the requests or sessions from the PDS requests will be excluded for all the User Data Types (even if they are enabled). The list can include the comma separated values. Regular expressions are allowed for the APN names with the following conditions: • must not contain white spaces. • must be case insensitive. • can not be an empty string. • '\' (backslash) must be specified as '/d'. • the names must be separated only with commas (,).
USER.smPolicyData.excludeApns	List the APNs for which all the requests or sessions from the PDS requests will be excluded for the given SmPolicyData (even if they are enabled).
USER.ldapData.excludeApns	List the APNs for which all the requests or sessions from the PDS requests will be excluded for the given Ldap Data (even if they are enabled).
USER.ocsSpendingLimit.excludeApns	List the APNs for which all the requests or sessions from the PDS requests will be excluded for the given OCS Spending Limit (even if they are enabled).
USER.operatorSpecificData.excludeApns	List the APNs for which all the requests or sessions from the PDS requests will be excluded for the given Operator Specific Data (even if they are enabled).
USER.ssv.excludeApns	List the APNs for which all the requests or sessions from the PDS requests will be excluded for SSV (even if they are enabled).

Table 7-117 Advanced Key/Values for configuring congestion response codes

Key	Value	Description
CONGESTION.HTTP.RESPONSE.CODE	503	Configure the response code of any rejected requests by PCRF Core service due to congestion state. By default, the service sends 503 as response code. If configured then it shall be either 1xx, 3xx, 4xx or 5xx response code.
PDS.NOTIFY.REQUEST.PRIORITY	18	Set request priority for post PDS notification request. **Allowed Values**: 0-100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-117 (Cont.) Advanced Key/Values for configuring congestion response codes

Key	Value	Description
UM.NOTIFY.REQUEST.PRIORITY	18	Set request priority for post Usage monitoring notification request. **Allowed Values**: 0-100
PCRF.SESSION.DELETE.REQUEST.PRIORITY	30	Set request priority for deleting PCRF session request. **Allowed Values**: 0-100
PCRF.SESSION.GET.REQUEST.PRIORITY	30	Set request priority for fetching PCRF session request. **Allowed Values**: 0-100
AUDIT.NOTIFY.REQUEST.PRIORITY	30	Set request priority for post Audit notification request. **Allowed Values**: 0-100

Table 7-118 Advanced Key/Values for configuring congestion response codes

Key	Value	Description
CONGESTION.USE.EXPERIMENTAL.RESULT.CODE	false	To set if user wants to use experimental result code when rejecting diameter messages. Allowed values are true or false. By default it will be false.
CONGESTION.VENDOR.ID	0	To set the vendor id when user wants to send experimental response code. To use experimental result code, set `CONGESTION.USE.EXPERIMENTAL.RESULT.CODE` as true, and set `CONGESTION.VENDOR.ID` as non-zero positive integer.
CONGESTION.DIAMETER.RESPONSE.CODE	3004	To set response code when rejecting diameter messages. Only valid 3xxx, 4xxx, 5xxx response codes are allowed.
GX.CREATE.REQUEST.PRIORITY	24	Set message priority for Diameter message Gx CCR-I. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100
GX.MODIFY.REQUEST.PRIORITY	18	Set message priority for Diameter message Gx CCR-U. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-118 (Cont.) Advanced Key/Values for configuring congestion response codes

Key	Value	Description
GX.DELETE.REQUEST.PRIORITY	16	Set message priority for Diameter message Gx CCR-T. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100
RX.CREATE.REQUEST.PRIORITY	24	Set message priority for Diameter message Rx AAR-I. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100
RX.MODIFY.REQUEST.PRIORITY	18	Set message priority for Diameter message Rx AAR-U. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100
RX.DELETE.REQUEST.PRIORITY	16	Set message priority for Diameter message Rx STR. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100
SD.MODIFY.REQUEST.PRIORITY	18	Set message priority for Diameter message Sd CCR-U. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100
SD.DELETE.REQUEST.PRIORITY	16	Set message priority for Diameter message Sd CCR-T. If user provides invalid value then the default request priority shall be considered. **Allowed Values**: 0-100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-119 Advanced Settings Configurations for Handling the Race Condition between Different Diameter Interface Messages in Single Site and Multi-sites for CCR-U

Key	Default Value
DIAMETER.Gx.Update.RaceModeratorEnabled	This is used to enable or disable race condition detection on CCR-U. If this flag is enabled, on detecting the race condition the following settings are used to decide the actions to take: • DIAMETER.Gx.Update.RetryOnRarRaceEventTriggers • DIAMETER.Gx.Update.RetryAttemptsOnRarRace • DIAMETER.Gx.Update.RetryWaitTimeOnRarRace • DIAMETER.Gx.Update.RejectionErrorCodeOnRarRace **Supported values**: true/false **Default value**: false
DIAMETER.Gx.Update.RetryOnRarRaceEventTriggers	If `DIAMETER.Gx.Terminate.RaceModeratorEnabled` is true, then a validation is made for all of the Event Triggers in the CCR-U request that are also included in this setting. **Note**: There must be at least one `registeredHandler` present in the Gx session that will make use of this event. If the validation fails for at least one of them, then the CCR-U will be put on hold, read the session again, and retry based on these settings: • DIAMETER.Gx.Update.RetryAttemptsOnRarRace • DIAMETER.Gx.Update.RetryWaitTimeOnRarRace • DIAMETER.Gx.Update.RejectionErrorCodeOnRarRace **Supported values**: These values can be provided as comma separated list. **Rx Triggers**: • ACCESS_NETWORK_INFO_REPORT • SUCCESSFUL_RESOURCE_ALLOCATION • LOSS_OF_BEARER **Sd Triggers**: • APPLICATION_START • APPLICATION_STOP **Default value**: ACCESS_NETWORK_INFO_REPORT
DIAMETER.Gx.Update.RetryAttemptsOnRarRace	The maximum number of retries when `DIAMETER.Gx.Update.RetryOnRarRaceEventTriggers` validation fails. **Supported values**: integer (0-n) **Default value**: 1
DIAMETER.Gx.Update.RetryWaitTimeOnRarRace	The amount of delay in milliseconds between retries when `DIAMETER.Gx.Update.RetryOnRarRaceEventTriggers` validation fails. **Supported values**: integer (0-n) **Default value**: 100

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-119 (Cont.) Advanced Settings Configurations for Handling the Race Condition between Different Diameter Interface Messages in Single Site and Multi-sites for CCR-U

Key	Default Value
DIAMETER.Gx.Update.RejectionErrorCodeOnRarRace	The error code response for the CCA-U when `DIAMETER.Gx.Update.RetryOnRarRaceEventTriggers` validation fails, and `DIAMETER.Gx.Update.RetryAttemptsOnRarRace` retries are exhausted. **Supported values**: Diameter Error codes • 5012 (DIAMETER_UNABLE_TO_COMPLY) • 3002 (DIAMETER_UNABLE_TO_DELIVER) **Default value**: 5012 **Note**: If invalid value is provided, fallback will be the default value 5012.
DIAMETER.Gx.Update.AllowOnRetriesExhaustedOnRarRace	When enabled, if the validation for DIAMETER.Gx.Update.RetryOnRarRaceEventTriggers key fails and DIAMETER.Gx.Update.RetryAttemptsOnRarRace retries are exhausted, this flag will override the DIAMETER.Gx.Update.RejectionErrorCodeOnRarRace setting and continue processing the request normally. **Default value**: true

Table 7-120 Advanced Settings Configurations for Handling the Race Condition between Different Diameter Interface Messages in Single Site and Multi-sites for CCR-T

Key	Default Value
DIAMETER.Gx.Terminate.RaceModeratorEnabled	This is used to enable or disable race condition detection on CCR-T. If this flag is enabled, on detecting the race condition the following settings are used to decide the actions to take: • DIAMETER.Gx.Terminate.RetryOnRarRaceEventTriggers • DIAMETER.Gx.Terminate.RetryAttemptsOnRarRace • DIAMETER.Gx.Terminate.RetryWaitTimeOnRarRace • DIAMETER.Gx.Terminate.RejectionErrorCodeOnRarRace **Supported values**: true/false **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-120 (Cont.) Advanced Settings Configurations for Handling the Race Condition between Different Diameter Interface Messages in Single Site and Multi-sites for CCR-T

Key	Default Value
DIAMETER.Gx.Terminate.RetryOnRarRaceEventTriggers	If `DIAMETER.Gx.Update.RaceModeratorEnabled` is true, then a validation is made for all of the Event Triggers in the CCR-T request that are also included in this setting. **Note**: There must be at least one `registeredHandler` present in the Gx session that will make use of this event. If the validation fails for at least one of them, then the CCR-T will be put on hold, read the session again, and retry based on these settings: • DIAMETER.Gx.Terminate.RetryAttemptsOnRarRace • DIAMETER.Gx.Terminate.RetryWaitTimeOnRarRace • DIAMETER.Gx.Terminate.RejectionErrorCodeOnRarRace **Supported values in comma separated list**: **Rx Triggers**: • ACCESS_NETWORK_INFO_REPORT • SUCCESSFUL_RESOURCE_ALLOCATION • LOSS_OF_BEARER **Sd Triggers**: • APPLICATION_START • APPLICATION_STOP **Default value**: ACCESS_NETWORK_INFO_REPORT
DIAMETER.Gx.Terminate.RetryAttemptsOnRarRace	The maximum number of retries when `DIAMETER.Gx.Terminate.RetryOnRarRaceEventTriggers` validation fails. **Supported values**: integer (0-n) **Default value**: 1
DIAMETER.Gx.Terminate.RetryWaitTimeOnRarRace	The amount of delay in milliseconds between retries when `DIAMETER.Gx.Terminate.RetryOnRarRaceEventTriggers` validation fails. **Supported values**: integer (0-n) **Default value**: 100
DIAMETER.Gx.Terminate.RejectionErrorCodeOnRarRace	The error code response for the CCA-T when `DIAMETER.Gx.Terminate.RetryOnRarRaceEventTriggers` validation fails, and `DIAMETER.Gx.Terminate.RetryAttemptsOnRarRace` retries are exhausted. **Supported values**: Diameter Error codes • 5012 (DIAMETER_UNABLE_TO_COMPLY) • 3002 (DIAMETER_UNABLE_TO_DELIVER) **Default value**: 5012 **Note**: If invalid value is provided, fallback will be the default value 5012.
DIAMETER.Gx.Terminate.AllowOnRetriesExhaustedOnRarRace	When enabled, if DIAMETER.Gx.Terminate.RetryOnRarRaceEventTriggers validation fails, and DIAMETER.Gx.Terminate.RetryAttemptsOnRarRace retries are exhausted, this flag will override the DIAMETER.Gx.Terminate.RejectionErrorCodeOnRarRace setting and continue processing the request as it would normally. **Default value**: true

Copyright © 2019, 2026, Oracle and/or its affiliates.

9. (Optional) To avoid sending stale session notification to PGW for Gx sessions when maxTTL value is reached, user can add **Override Cleanup Audit** parameter as AVP with its value set to true. To do so, perform the following steps:

   a. Expand the **Advanced Settings** group and click ⊕ Add
   The page opens the **Add Advanced Settings** dialog box.

   b. On the **Add Advanced Settings** dialog box, enter the following **Keys** and respective values:

Table 7-121 Add Advanced Settings Key and Value

Key	Default Value	Description
DIAMETER.Cleanup.OverrideCleanupAudit	True	This parameter is used along with `maxTTL` flag. If true along with `maxTTL` is also true, deletes the Gx and Rx stale sessions and no notification is sent to PGW. If false, notification is sent to PGW and stale sessions are not deleted.
DIAMETER.ENF.DUPLICATE.UPDATE.MESSAGE.HANDLING	false	Specifies if the duplicate message handling feature should be enabled or disabled.
DIAMETER.MsgBufferThreadCount	60	Specifies the number of threads to process read-diameter-messages.
DIAMETER.MsgBufferQueueSize	8192	Specifies the size of the queue for holding pending read-diameter-messages.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-121 (Cont.) Add Advanced Settings Key and Value

Key	Default Value	Description
DIAMETER.AF.MaxAFReportHandler	The minimum valid value for this parameter is 1. The maximum valid value of this setting is defined according to the following criteria: • For an Rx session with 2 media components (Audio, video) and 2 media sub components for each media component, the maximum value allowed is 2. • For an Rx session with 1 media component (Audio) and 2 media sub components, the maximum value allowed is 4. **Note** To enable the feature flag, Enter the value as *true* in the **Value** field.	Specifies the number of the Rx session to establish. **Note**: These minimum and maximum values are only valid with data compression disabled.
DIAMETER.ENF.AFDirectReply	True **Note:** Allowed value True or False	If true, PCRF responds immediately to AAR request with AAA answer to AF, and at the same time RAR request is sent to PGW. If false, PCRF awaits until RAA is received from PGW and then responds with AAA answer to AF.
DIAMETER.AF.SessionBindingAltKeys	NONE	Comma separated list that determines alternate keys and their order to look for if a Rx session lookup results in multiple matches (use when message contains IPv4 address). The available identifiers that can be used are: • NONE • IMSI • NAI • E164 • APN • IP • IPD

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-121 (Cont.) Add Advanced Settings Key and Value

Key	Default Value	Description
DIAMETER.AF.MaxWaitForInfoOnTermination	3000 milliseconds **Note:** Allowed value 0 - 10000 milliseconds.	The PCRF maximum wait time in milliseconds to receive the information from PCEF before responding to the AF with STR request. On not receiving the awaited information within the configured waiting period, PCRF responds to AF with successful STA answer without the requested information.
DIAMETER.AF.IgnorePartialCodec	false	It specifies whether to ignore QoS calculation if the uplink and downlink codec values are received in separate Rx messages. For example, uplink codec data in AAR-I and downlink codec data in AAR-U.
POLICYDS_REQUEST_TIMEOUT	3000 milliseconds **Note:** Allowed value 0 - 10000 milliseconds.	The PCRF maximum wait time for receiving response from PDS. On not receiving the awaited information from PDS within the configured waiting period, PCRF times out.
DB.GX.DATA.ENCODING.Enabled	false	When the value of this key is set to `true`, PCRF Core Gx session data is encoded. The JSON parameters are encoded based on the version indicated by `DB.GX.ENCODING.MAP.Version` value. If `DB.GX.ENCODING.MAP.Version` is not configured, its default version will be "gx0" and the parameter is encoded by default mapping. The PCRF Core Gx session data is decoded based version value in the session.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-121 (Cont.) Add Advanced Settings Key and Value

Key	Default Value	Description
DB.RX.DATA.ENCODING.Enabled	false	When the value of this key is set to `true`, PCRF Core Rx session data encoding is enabled. The JSON parameters are encoded based on the version indicated by `DB.RX.ENCODING.MAP.Version` value. If `DB.RX.ENCODING.MAP.Version` is not configured, its default version will be "rx0" and the parameter is encoded by default mapping. The PCRF Core Rx session data is decoded based version value in the session.
DB.SD.DATA.ENCODING.Enabled	false	When the value of this key is set to `true`, PCRF Core Sd session data is encoded. The JSON parameters are encoded based on the version indicated by `DB.SD.ENCODING.MAP.Version` value. If `DB.SD.ENCODING.MAP.Version` is not configured, its default version will be "sd0" and the parameter is encoded by default mapping. The PCRF Core Sd session data is decoded based version value in the session.
DB.GX.ENCODING.MAP.Version	0	Indicates the mapping version name for Gx session encoding. To set this use a "unique string" such as "gx0". The encoding version is used for decoding. When value of this key is set to "0", or this key is not configured, the encoding/ decoding uses default map.
DB.RX.ENCODING.MAP.Version	0	Indicates the mapping version name for Rx session encoding. To set this use a "unique string" such as "rx0". The encoding version is used for decoding. When value of this key is set to "0", or this key is not configured, the encoding/ decoding uses default map.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-121 (Cont.) Add Advanced Settings Key and Value

Key	Default Value	Description
DB.SD.ENCODING.MAP.Version	0	Indicates the mapping version name for Sd session encoding. To set this use a "unique string" such as "sd0". The encoding version is used for decoding. When value of this key is set to "0", or this key is not configured, the encoding/ decoding uses default map.
DB.ENCODING.MAP.LIST	0	Indicates the mapping list keyMap and valueMap in JSON format. When this value is set to "0" the default map is referred for encoding and decoding. To set this to customized map in the form of JSON format containing keyMap and valueMap.
enable.late.arrival	Disabled	Indicates whether the stale request cleanup functionality for PCRF Core is enabled or disabled. **Default value**: false
skip.late.processing.for.terminate	false	When enabled, PCRF-Core will not check if Terminate requests have gone stale.
USER.Notification.EnableRetryOnSessionNotFound	false	When enabled, the request will wait for the configured time and try again if Gx session is not found on user data change notification from PDS.
USER.Notification.RetryAttemptsOnSessionNotFound	1	Specifies the number of retry attempts allowed.
USER.Notification.RetryWaitTimeOnSessionNotFound	100	Specifies the wait time between retries in milliseconds.

c. Click **Save**.
This saves the advanced settings and the details get listed on **Edit Settings** page under **Advanced Settings**.

10. Click **Save**.
The page saves the PCRF Core service settings.

7.3.9.2 Serving Gateway

This procedure provides information about how to create and manage serving gateways.

The **Serving Gateway** page allows you to create new and manage existing serving gateways. The page displays the list of defined serving gateways and provides the options to import, export, or add gateways.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure serving gateway:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **PCRF Core**, and then select **Serving Gateway**.
   This opens the **Serving Gateway** page. The page lists the existing gateway details. You can add or import new serving gateways using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Service Gateway** page.
3. On the **Create Service Gateway** page, enter the following information:

   Table 7-122 Create Service Gateway

Field Name	Description
Name	The customized name for serving gateway
Description	The customized description for serving gateway
MCC-MNC	The Mobile country code (3-digit number) or Mobile network code (2- or 3-digit number)
Serving Gateway IP Address/Subnet	IP address or subnet for the serving gateway

4. Click **Save**.
   The serving gateway gets listed on the **Serving Gateway** page.

   > **Note**
   >
   > Use or available under the **Actions** column to update or delete the serving gateway.

Importing Serving Gateway

To import Serving Gateway:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.9.3 Network Element

This section describes how to configure network elements.

To access network elements configurations from CNC Console home page, under **Policy**, navigate to **Service Configurations**, click **PCRF Core**, and then select **Network Elements**.

On clicking PCRF Core, you can select to customize any of the following network elements:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- PGW (PDN Gateway)
- GGSN (GPRS Support Node)

7.3.9.3.1 PGW

This procedure provides information about how to create and manage PDN Gateway (PGW) network element.

The **PGW** page allows you to create new and manage existing PGWs. The page displays the list of defined PGWs with the options to import, export, or add profiles.

To configure PGW:

1. From the navigation menu under **Network Elements**, select **PGW**.
   This opens the **PGW** page. The page lists the existing PGWs. You can add or import new PGWs using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create PGW** page.
3. On the **Create PGW** page, enter the following information:

Table 7-123 Create PGW

Field Name	Description
Name	Use this field to add a customized name for PGW.
Description/Location	Use this field to add a customized description or location for network element.
Backup Host Name/IP Address	Registered domain name, or IP address in IPv4 or IPv6 format, assigned to the network element.
Host Name/IP Address	Alternate address that is used if communication between the CNC Policy and the primary address for the network element fails.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-123 (Cont.) Create PGW

Field Name	Description
Capability	Specifies the capability for the network element. PGW network elements are compatible with usage_report event trigger value 26. **Note** The **Capability** field is now restricted to **Usage_Report-26** or **Empty** only. Prior to 3GPP specification 29.212 Release 9, Revision 4, the value for usage_report was 26. However, starting from Release 9, Revision 4, this value is updated to 33 for usage_report. If this capability is provided, the PCRF will override the default value of 33 with 26 when arming the Usage Report trigger in the CCA message.
Capacity	Specifies the bandwidth allocated to the network element.
IP Domain ID	Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks.
Diameter Realm	Specifies the realm to be sent in the diameter message.
MIP6 Host Identity	Specifies the Mobile IPv6 (MIPv6) host.
Diameter Identity	Specifies the fully qualified domain name (FQDN) of the network element

4. Click **Save**.
   The PGW gets listed on the **PGW** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the PGW.

Importing PGW

To import PGW:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.9.3.2 GGSN

This procedure provides information about how to create and manage PDN Gateway (GGSN) network element.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The **GGSN** page allows you to create new and manage existing GGSNs. The page displays the list of defined GGSNs with the options to import, export, or add profiles.

To configure GGSN:

1. From the navigation menu under **Network Elements**, select **GGSN**.
   This opens the **GGSN** page. The page lists the existing GGSNs. You can add or import new GGSNs using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create GGSN** page.
3. On the **Create GGSN** page, enter the following information:

Table 7-124 Create GGSN

Field Name	Description
Name	Use this field to add a customized name for GGSN
Description/Location	Use this field to add a customized description or location for network element
Backup Host Name/IP Address	Registered domain name, or IP address in IPv4 or IPv6 format, assigned to the network element
Host Name/IP Address	Alternate address that is used if communication between the CNC Policy and the primary address for the network element fails
Capability	Specifies the capability for the network element. Usually, GGSN network elements are compatible with usage_report event trigger value 26. **Note** The **Capability** field is now restricted to **Usage_Report-26** or **Empty** only. Prior to 3GPP specification 29.212 Release 9, Revision 4, the value for usage_report was 26. However, starting from Release 9, Revision 4, this value is updated to 33 for usage_report. If this capability is provided, the PCRF will override the default value of 33 with 26 when arming the Usage Report trigger in the CCA message.
Capacity	Specifies the bandwidth allocated to the network element

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-124 (Cont.) Create GGSN

Field Name	Description
IP Domain ID	Specifies the IPv4 domain identity. This value uniquely identifies the network element if the same IPv4 address is assigned in multiple networks
Diameter Realm	Specifies the realm to be sent in the diameter message
Diameter Identity	Specifies the fully qualified domain name (FQDN) of the network element

4. Click **Save**.
   The GGSN gets listed on the **GGSN** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the GGSN.

Importing GGSN

To import GGSN:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.10 Audit Service

This procedure provides information about configuring the Audit Service.

The **Audit Service** page displays the Audit Service configurations. The page allows you to edit the configurations.

To configure Audit service:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, and select **Audit Service**.
   This opens the **Audit Service** page. The page displays the existing configurations.
2. Click Edit .
   This opens the **Edit Audit Service** page.
3. Make sure that the value of the **Audit Enabled** switch is enabled.
   This field determines if auditing must be enabled for all the registered Policy services. By default, this switch remains disabled.
4. Expand the **Forced Deletion** group and configure the **Minimum Audit Attempts** parameter.

   Minimum Audit Attempts specifies the minimum number of audit attempts until ForceTTL is reached.

   If ForceTTL is reached and audit_attempts >= Minimum Audit Attempts of ForceTTL, then Audit service deletes the identified stale records from its respective database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

For example, it deletes the stale SM sessions from SMPolicyAssociation table.

The default value of this parameter is 0 and the value can range between 0 to 255.

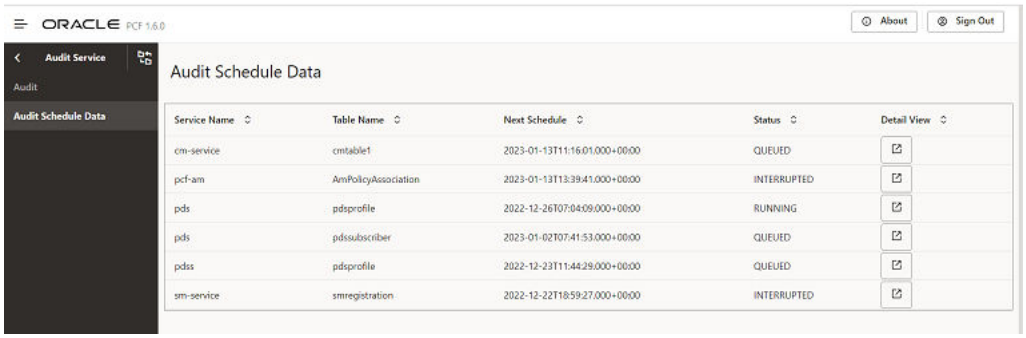
5. Click **Save**.
The page saves the Audit service configurations.

> **Note**
>
> - Perform the Audit configurations at the individual service level (SM service and Binding service), for Audit service and notifications to work appropriately.
>
> **Important considerations during Audit configurations**:
>
> In situations where the number of stale records (records that are eligible to be audited) at any given point of time in the system (for a given microservice database) is expected to be high (for example, > 1M), then the **Policy Session Age** and/or the **Notification Rate** parameters should be set appropriately such that at least 2 audit cycles can be finished before the records that were assessed by the first cycle fall stale again. The Audit procedure having a **Policy Association Age** less than this recommendation, may not be able to assess all stale records as the already assessed ones will be stale again too soon. It is recommended to keep a minimum of 24 hours for the **Policy Association Age** and a minimum of 48 hours for **Max Policy Association Age**.
>
> The time taken to complete an Audit Cycle and begin the next one can be calculated as below:
>
> Audit Cycle Time = S / (N*60) + I minutes, where,
>
> S = expected number of stale sessions at any given time,
>
> N = notification rate (per second),
>
> I = minimum Audit Interval
> - When table slicing feature is enabled, and audit is running on a set of sliced tables, the audit notification rate would be expected to reach no of sliced tables * configured notification rate if audit is running for some/all the sliced tables concurrently.

Audit Schedule Data

Audit service supports multiple pod, using the Audit Schedule and Audit TaskScheduler. Audit schedule has list of registerd services that needs audit service with all the scheduled details. Audit TaskScheduler polls for all those audit jobs in the QUEUED status.

Figure 7-18 Audit Scheduled Service List Data



Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-125 Audit Schedule Data Fields

Field Name	Description
Service Name	Name of the service that had registerd for audit service.
Table Name	Name of the database table that has requested for the audit service
Next Schedule	Next schedule availability time
Status	Scheduler job status
Start Time	Audit start time of pod.
End Time	Audit end time of pod.
Last Polled Time	Pod and associated scheduler details.
Schedular Details	Last time at which pod updated this table.
Is Service Dependent	If this is true, notification will be triggered for one table in the service, for all table's in the service, notifications will be sent parallelly based on the notificationRate set for each table.
Priority	Priority set by customer to audit certain records or group of records in some order
Version	For JPA optimization

Audit Schedule task can be in one of the state described below:

Figure 7-19 Audit Schedule Job Work Flow

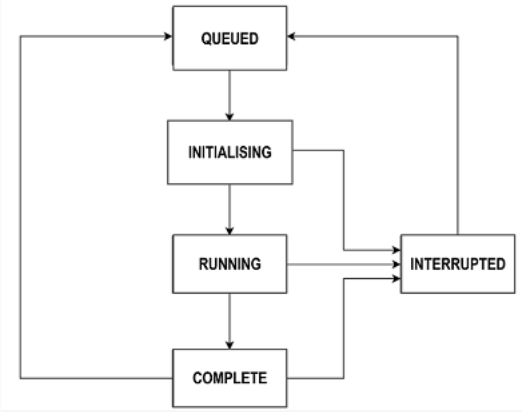


Table 7-126 Audit Schedule Job Status

Status	Description
QUEUED	When a registered request is received it is added to the schedule table, the job status is set to Queued.
INITIALISING	When polling task is complete and is initialising for AuditTaskManager to audit, the job status is set to Initialising.
RUNNING	When Audit task manager starts the task, the job status is set to Running.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-126 (Cont.) Audit Schedule Job Status

Status	Description
COMPLETE	When Audit TaskManager completes the Audit, the status is set to Complete.
INTERRUPTED	When the audit process is paused from GUI, then the job status is set to Interrupted. When resumed from GUI, job status is set to Queued When deregistered, the job data will be removed from the table. when a service is register, it is set to Queued.
DEREGISTERED	When deregistered, the job status is set to Deregistered for Initialising or Running and the entry will be deleted for any other status(except Initialising or Running). In case the a service register request is received before AuditTaskManager deletes the table entry for deregistered job statuses, the status would be moved to Queued.

For more information on Audit Service and Audit Schedule REST API details, see the section *Audit Service* in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

7.3.11 Configuring Notifier Service

This section provides information on how to configure Notifier service.

7.3.11.1 Notifier Configurations

This procedure provides information about managing Notifier Service Settings.

The Notifier Service Settings page allows you to edit Advanced Settings for Notifier service.

To configure, perform the following steps:

1. From the navigation menu, under **Policy**, click **Service Configurations**, click **Notifier**, and then select **Notifier Configurations**.
   This opens the Notifier Service Settings page.
2. Click **Edit**.

   This opens the Edit Notifier Service Settings page.
3. Edit the **SMPP Configuration**:

Table 7-127 SMPP Configuration

Attribute Name	Description
Enable SMPP	Enables the Subscriber Notification using SMPP Protocol. **Default Value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-127 (Cont.) SMPP Configuration

Attribute Name	Description
Default SMS Gateway Group	All the SMS Gateways that are created in SMS GATEWAY CONFIGURATION page.
ESME Source Address	External Short Messaging Entity (ESME) Source Address is a mandatory field and can accept IPV4/IPV6 address. This field is empty by default.
ESME Source Address TON	Indicates the ESME Source address type of number: • UNKNOWN • INTERNATIONAL • NATIONAL • NETWORK_SPECIFIC • SUBSCRIBER_NUMBER • ALPHANUMERIC • ABBREVIATED **Default Value**: UNKNOWN
ESME Source Address NPI	ESME Source Address Number Plan Indicator: • UNKNOWN • ISDN (E163/E164) • DATA (X, 121) • TELEX • LAND_MOBILE • NATIONAL • PRIVATE • ERMES • INTERNET • WAP **Default Value**: UNKNOWN
Connection Timeout (in milliseconds)	Indicates the SMS Gateway Connection Timeout in milliseconds. **Range**: 1-60000 **Default Value**: 30000
Response Timeout (in milliseconds)	Indicates the timeout (in milliseconds) for the response going towards SMS Gateway. **Range**: 1-60000 **Default Value**: 10000

4. Click **Add** to add the advanced settings.

Table 7-128 Advanced Settings

Key	Value
smpp.bindType	Bind type of the SMPP server. Allowed values: • BIND_TX • BIND_RX • BIND_TRX **Default value**: BIND_TRX

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-128 (Cont.) Advanced Settings

Key	Value
smpp.systemType	System type. This key can accept null values.
smpp.addrTon	Address type of number of the SMPP server. Allowed values: • UNKNOWN • INTERNATIONAL • NATIONAL • NETWORK_SPECIFIC • SUBSCRIBER_NUMBER • ALPHANUMERIC • ABBREVIATED **Default value**: UNKNOWN
smpp.addrNpi	Address Number Plan Indicator: • UNKNOWN • ISDN (E163/E164) • DATA (X, 121) • TELEX • LAND_MOBILE • NATIONAL • PRIVATE • ERMES • INTERNET • WAP **Default value**: UNKNOWN
smpp.addrRange	Set of SME addresses. Address range can accept null values.
smpp.serviceType	Service type can be either null or CMT.
smpp.encodingScheme	SMPP Encoding Scheme. **Default value**: UTF-8
smpp.destAddrTon	Destination address type of number: • UNKNOWN • INTERNATIONAL • NATIONAL • NETWORK_SPECIFIC • SUBSCRIBER_NUMBER • ALPHANUMERIC • ABBREVIATED **Default value**: UNKNOWN

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-128 (Cont.) Advanced Settings

Key	Value
smpp.destAddrNpi	Destination Address Number Plan Indicator: • UNKNOWN • ISDN (E163/E164) • DATA (X, 121) • TELEX • LAND_MOBILE • NATIONAL • PRIVATE • ERMES • INTERNET • WAP **Default value**: ISDN
smpp.validatePeriodInDays	Validity period of the SMS (in days) **Default value**: 3 days
smpp.esmClassValue	The message mode and type, indicating any special message attributes associated with the SMS. **Default value**: 0
smpp.reconnectMinDelayMillis	Minimum delay in milliseconds after the consumer/producer tries to reconnect to the SMSC, after the connection was lost. **Default value**: 500
smpp.reconnectMaxDelayMillis	Maximum delay in milliseconds after the consumer/producer tries to reconnect to the SMSC, after the connection was lost. **Default value**: 10000
smpp.smDefaultMsgId	Short message default message identifier. **Default value**: 0
smpp.protocolId	Protocol ID. **Default value**: 0
smpp.priorityFlag	Priority Flag. **Default value**: 0
smpp.packedGSM7Encoding	Indicates whether to apply GSM-7 character encoding. **Default value**: false
smpp.sarSegmentSize	SMS Segment size. **Default value**: 134

Table 7-129 Advanced Settings for Congestion Control

Key	Value
NOTIFIER.NOTIFY.PRIORITY	Update Subscriber Notification API: /v1/notify **Allowed Values**: 0-31 **Default Value**: 20

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-129 (Cont.) Advanced Settings for Congestion Control

Key	Value
CONGESTION_RESPONSE_CODE	Configure the response code of any rejected requests by Notifier service due to congestion state. By default, the service sends 503 as response code. If configured then it shall be 5xx only.

5. Click **Save** to save the advanced settings.
   To discard the changes, click **Cancel**
6. Click **Save** to save the Notifier Service Settings.
   To discard the changes, click **Cancel**

7.3.11.2 Notification Server

7.3.11.2.1 HTTP Server

This procedure provides information on how to add and manage HTTP Server.

The HTTP Server page allows you to add and edit HTTP servers.

To configure, perform the following steps:

1. From the navigation menu, under **Policy**, click **Service Configurations**, click **Notifier**, click **Notification Server**, and then select **HTTP Server**.
   This opens the HTTP Server page.
2. Click **Add**.

   This opens the Add HTTP Server page.
3. Enter values for the following input fields, as described in the following table:

Table 7-130 Add HTTP Server

Field Name	Description
Name	Enter the name of the HTTP server. The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).
Description/Location	Free-form text that identifies the HTTP server within the network. Enter up to 250 characters.
Scheme	Select the scheme. The available values are: • HTTP • HTTPS

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-130 (Cont.) Add HTTP Server

Field Name	Description
Host	Enter the Host Name of the HTTP server. **Note** Enter IPv6 values in square brackets to avoid ambiguity and parsing issues. Host field format rules (HttpServer Host and Alt Host): • IPv4 and FQDN: – You may enter with or without port. – Examples: * 10.20.30.40 * 10.20.30.40:8080 * api.example.com * api.example.com:8443 • IPv6: – You must use square brackets around the IPv6 host. – Supported formats: * [host] * [host]:port – Examples: * [2001:db8::10] * [2001:db8::10]:443 • Do not enter IPv6 without brackets when a port is present. – Example to avoid: * 2001:db8::10:443

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-130 (Cont.) Add HTTP Server

Field Name	Description
Alt Host	Enter the Alternate Host Name of the HTTP server. **Note** Enter IPv6 values in square brackets to avoid ambiguity and parsing issues. Host field format rules (HttpServer Host and Alt Host): • IPv4 and FQDN: – You may enter with or without port. – Examples: * 10.20.30.40 * 10.20.30.40:8080 * api.example.com * api.example.com:8443 • IPv6: – You must use square brackets around the IPv6 host. – Supported formats: * [host] * [host]:port – Examples: * [2001:db8::10] * [2001:db8::10]:443 • Do not enter IPv6 without brackets when a port is present. – Example to avoid: * 2001:db8::10:443
URI Path	Enter the URI path.
HTTP Version	Select the HTTP version. The available values are: • 1.1 • 2
HTTP Header	Provide HTTP Header details:
Header Key	Enter the header key.
Header Value	Enter the value for the header key.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Backward compatibility for older bulk exports:
>
> - Some legacy bulk-export files may contain host and port together in a single unbracketed value.
> - During import, the value may be interpreted by splitting at the last colon, treating the final segment as port and the remaining part as host.
> - To avoid ambiguity and incorrect parsing, always use bracketed IPv6 format: [host] or [host]:port.

4. Click **Save**. The HTTP server is displayed on the HTTP Server page.
   To discard the changes, click **Cancel**

Use pencil icon or trash bin icon available in the next column to edit or update the created HTTP server.

7.3.11.2.2 SMS Gateway Group

The SMS Gateway Group page allows you to configure the SME Gateways.

1. From the navigation menu, under **Policy**, click **Service Configurations**, click **Notifier**, click **Notification Server**, and then select **SMS Gateway Group**.
   This opens the SMS Gateway Group page.
2. Click **Add**.

   This opens the Add SMS Gateway Group page.
3. Enter values for the following input fields, as described in the following table:

Table 7-131 Add SMS Gateway Group

Field Name	Description
Name	Enter the name of the SMS Gateway server. The name can be Maximum 40 characters consisting of alphabets, numbers, period, hyphen and underscore (_). By default, the value is left empty.
Description	Free-form text that identifies the SMS Gateway server within the network. Enter up to 250 characters. By default, the value is left empty.
Primary SMSC Host	Enter the Host Name of the primary SMSC Host server. By default, the value is left empty.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-131 (Cont.) Add SMS Gateway Group

Field Name	Description
Request Delivery Receipt	Specify the mode of delivery receipt. This field accepts the following integer values: • 0 to indicate REQUEST_DELIVERY_RECEIPT_NO • 1 to indicate REQUEST_DELIVERY_RECEIPT_SUCCESS_FAILURE • 2 to indicate REQUEST_DELIVERY_RECEIPT_FAILURE **Default Value**: 0
Maximum Byte Length	Maximum number of bytes allowed for the message. The length of the message can range between 1 to 254 bytes. **Default Value**: 140
Long Message Enabled	Enables the long messages. **Default Value**: true
Long Message maximum Byte Length	Specifies the maximum number of bytes allowed in the long message. Maximum length of the long messages can range between 1 to 999 bytes. **Default Value**: 500 For details on the long message scenarios, see Long Message Scenarios
Long Message Delivery Method	Specify the long message delivery method. It can take the following integer values: • 0 to indicate SEGMENTATION AND REASSEMBLY (SAR) to deliver the long messages in segments • 1 to indicate the MESSAGE_PAYLOAD to deliver the long messages in payload **Default Value**: 0
Truncate Long Messages	Indicates whether to truncate messages longer than the specified length. **Default Value**: false
Fail Max Message Size	Specify the maximum length of the message after which the message fails. **Default Value**: true

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-132 Long Message Scenarios

Scenario	Fail Max Message Size	Long Message Enabled	Truncate Long Messages	Result
Message with 165 charactersLength > 140 and < 254	Enabled	Disabled	Disabled	• Message failed with cause: SmsLengthExceeded • "message":"rejecting message because longMsgEnabled: false, messageLen: 165 > maxBytesLen: 140, failMsgOnMaxMsgSize: true",
Message with 165 charactersLength > 140 and < 254	Disabled	Disabled	Disabled	Message has been successfully sent to the SMSC server without any error.
Message with 260 characters Length > 140 and > 254	Disabled	Disabled	Disabled	• Messaged failed with cause: SmsLengthExceeded • "message":"rejecting message because longMsgEnabled: false, messageLen: 140 > 254, truncateOnLongMsg: false"
Message with 165 characters Length > 140 and < 254	Disabled	Disabled	Enabled	Message has been truncated to 140 characters and sent to the SMSC server without any error.
Message with 260 charactersLength > 140 and > 254	Disabled	Disabled	Enabled	Message has been truncated to 140 characters and sent to the SMSC server without any error.

4. Click **Save**. The SMS Gateway details are displayed on the **SMS Gateway Group** page. To discard the changes, click **Cancel**
5. You can use pencil icon or trash bin icon available in the next column to edit or delete the created SMS Gateway server.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.11.2.3 SMSC Host Info

The SMSC Host Info page allows you to add and edit SMSC host configuration.

To configure, perform the following steps:

1. From the navigation menu, under **Policy**, click **Service Configurations**, click **Notifier**, click **Notification Server**, and then select **SMSC Host Info**.
   This opens the SMSC Host Info page.
2. Click **Add**.

   This opens the Add SMSC Host Info page.
3. Enter values for the following input fields, as described in the following table:

Table 7-133 Add SMSC Host Info

Field Name	Description
Name	Enter the name of the SMSC Host server. The name can be lower case alphanumeric characters, '-' or '.', and must start and end with an alphanumeric character. By default, the value is left empty.
SMSC Host	Enter the Host Name of the SMSC server. The host can be Ipv4, Ipv6 or FQDN with optional port value. By default, the value is left empty.
SMSC Port	Enter the Port number of the SMSC server. Range: 0-65535 By default, the value is left empty.

4. Click **Save**. The SMSC Host server is displayed on the SMSC Host Info page.
   To discard the changes, click **Cancel**

Use pencil icon or trash bin icon available in the next column to edit or delete the SMSC Host details.

7.3.12 PDS

This section includes the Policy Data Service (PDS) configurations.

To access PDS configurations from the CNC Console home page, expand **Policy**, navigate to **Service Configurations** and select **PDS**.

On clicking **PDS**, you can customize the following configurations:

- PDS Settings
- PDS Workflow

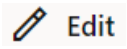
7.3.12.1 PDS Settings

This procedure provides information about configuring the PDS settings.

The **PDS Settings** page under **PDS** displays the PDS settings. The page allows you to edit the configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To edit the PDS settings:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, click **PDS**, and then select **PDS Settings**.
   This opens the **PDS Settings** page. The page displays the existing settings for PDS.
2. Click 

   .
   This opens the **Edit PDS Settings** page.
3. Expand the **Remote Subscriber State Variable Root Path** group.
   Remote Subscriber State Variable Root Path defines the root path of the remote subscriber state variables block corresponding to each datasources. For example, SMPolicyData, AMPolicyData, OperatorSpecificData, UEPolicyData, SpendingLimitData, and so on.

   For information about subscriber state variables block, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*. This information is written back (PATCH Request) to UDR as soon as the values are updated or when the last session of the subscriber terminates.
4. Under the **Remote Subscriber State Variable Root Path** group, enter values for the following parameters:

Table 7-134 Remote Subscriber State Variable Root Path Group Settings

Field Name	Description
Enable End Session SSV Remote to UDR	Determines if the dynamic write should happen at time of policy execution or at the end of the last session for subscriber. **Note:** This field is not applicable for Operator Specific Data (OSD). **Default Value**: false
SM Policy Data	Defines the path of subscriber state variables under SMPolicyData. You can provide multiple paths separated by commas.
UE Policy Set	Defines the path of subscriber state variables under UEPolicyData. You can provide multiple paths separated by commas.
Operator Specific Data	This multiple value input field enables the operator to specify the paths in Operator Specific Data (OSD) that are used for Remote Subscriber State Variables. **Note:** The `Enable End Session SSV Remote to UDR` field is not applicable for Operator Specific Data.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-20 PDS Settings: Remote Subscriber State Variable Root Path

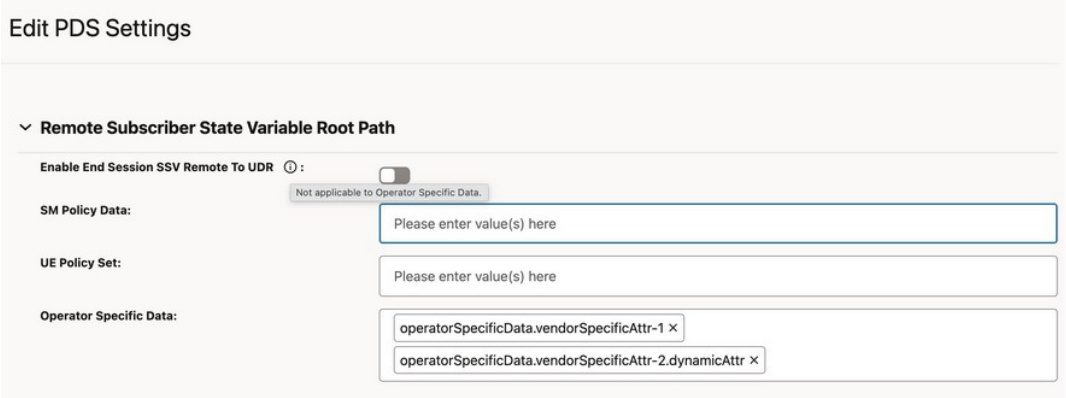
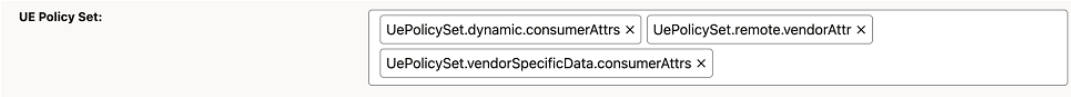


Figure 7-21 Sample UE Policy Set Configured



5. Expand the **Common** group and enter values for the following parameters:

Table 7-135 Common Group Settings

Field Name	Description
Enable HTTP2	If this switch is enabled, the HTTP2 remains enabled. By default, the switch remains disabled.
Global Request Timeout	If PDS Setting is updated then set the timeout as 3000 for the initial flow to succeed.
Enable Configurable Timeout	If this switch is enabled the following interface-level timeouts (optional) are displayed: • UDR Request Timeout • CHF Request Timeout • LDAP Request Timeout • OCS Request Timeout • Bulwark Request Timeout • PRE Request Timeout • Notification Request Timeout • Audit Request Timeout **Note** When the **Enable Configurable Timeout** field is disabled, it defaults to the **Global Request Timeout**. Similarly, if interface-level timeouts are not set, they will also use the **Global Request Timeout** as a fallback.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-135 (Cont.) Common Group Settings

Field Name	Description
Enable Fetch and Resubscribe	If this switch is set to true, PDS re-fetches the data and revalidates the subscription when the number of sessions exceeds the configured limit at PDS. PDS revalidates each subsequent request received after the configured limit. If the revalidation is successful, PDS does not perform any further action. However, if PDS fails to revalidate subscriptions (with error status 404), then it resubscribes with the datasource. By default, the value for this parameter is set to false. For `smPolicyData`, the limit for the number of sessions is defined per SNSSAI:DNN. **Note**: For user data type `smPolicyData`, the attributes **Include Snssai in User Query** and **Include Dnn in User Query** on the PCF Session Management page must be set to false. For `spendingLimitData`, the limit is defined per DNN:SNSSAI.
Data Compression Scheme	Specifies the data compression scheme used by PDS. Following are the allowed values for this field: • Disabled • Application Compressed By default, this value remains disabled.

Note

The **Type of Search** field under **PDS Settings** page is not active. The key preference for PDS search query must be configured using **Type of Search** field on **PDS UE ID Configuration** page. For more information, see PDS UE ID Configuration.

The **Type of Search** (`common.typeOfSearch`) and **Preference Order** (`common.preferenceOrder`) fields are not imported or updated through PDS Settings, either using CNC Console or REST API. These configurations must be updated using PDS UE ID Configuration. For more information, see PDS UE ID Configuration

When the **Enable Fetch and Resubscribe** switch is set to true, you are required to configure the parameters described in this table.

Table 7-136 Session Count per DNN/APN List Settings

Field Name	Description
DNN	Displays the Data Network Name. The allowed expression for DNN is [^[A-Za-z0-9-.]+$] and NA. **Note**: Do not add spaces to this field.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-136 (Cont.) Session Count per DNN/APN List Settings

Field Name	Description
SST	Displays the Slice or Service Type name in the S-NSSAI. You can enter a number from 0 to 255 or NA.
SD	Displays the Slice Differentiators Name. The allowed expression for SD is ^([A-Fa-f0-9]+|NA)$. **Note**: Do not add spaces or any other characters to this field.
Max Sessions Count	Displays the number of sessions after which PDS re fetches and revalidates subscriptions. You can enter a number from 1 to 12.

6. Under the **Audit** group, enter values for the following parameters:

Table 7-137 Configurable Parameters for Audit group

Field Name	Description
Enabled	Determines whether to send registration request to Audit service or not. **Default Value**: false
Notification Rate (per second)	Defines the number of stale records which Audit service notifies to PDS service in one second. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)
Subscriber Session Age (in minutes)	Defines the age of PDS subscriber entry after which a record is considered to be stale on Policy and services (SM, AM, UE, and PCRF Core) are queried for presence of such associations. **Default Value**: 1500
Subscriber Session Max Age (in minutes)	Defines the age of PDS subscriber entry after which a record is purged from the database and no query requests are sent to services for presence of such associations. **Default Value**: 2940
Subscriber Min Audit Pass Interval (in minutes)	Defines the minimum interval between start times of two consecutive audit passes for the pdssubscriber table. **Default Value**: 390
PDS Profile Age (in minutes)	Defines the age of PDS profile (GPSI-SUPI-NAI mapping) after which the profile is considered to be stale in Policy and PDS subscriber table is queried for presence of such associations. **Default Value**: 4500
PDS Profile Max Age (in minutes)	Defines the age of PDS profile (GPSI-SUPI-NAI mapping) after which the profile is purged from the database without sending any queries to PDS subscriber table. **Default Value**: 8820

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-137 (Cont.) Configurable Parameters for Audit group

Field Name	Description
PDS Profile Min Audit Pass Interval (in minutes)	Defines the minimum interval between start times of two consecutive audit passes for the pdssubscriber table. **Default Value**: 1170

> **Note**
>
> At the time of fresh installation, check and save PDS settings configuration even if there is no change to the configuration.
>
> a. Click **Edit**.
> b. Update the values if required.
> c. Click **Save** (even if there is no change to the configuration).
>
> The Audit Service starts auditing with the default/updated configuration.

7. Perform the configurations under **Policy Data Subscription Expiry**

Table 7-138 Policy Data Subscription Configuration

Field Name	Description
Policy Data Subscription Enabled	Determines whether to enable or disable the handling of Policy Data subscription expiry. **Default value**: false
Pre-Expiry Period (in minutes)	Specifies the duration (time in minutes) for which the Re-subscription can be triggered for Policy data. **Default value**: 180 **Range**: 1 to 20160
Policy Data Subscription Expiry Audit Notification Rate (per second)	Specifies the Policy Data Subscription Expiry notification processing rate. **Default value**: 50 **Range**: 20-300
Policy Data Subscription Expiry Max Age (% of Pre-expiry period)	Specifies the Audit window limited to local site. The local site triggers the audit until the Max Age is reached. Once the Max Age expires, the replicated site becomes eligible to perform the audit. **Default value**: 50 **Range**: 1-100
Policy Data Subscription Expiry Min Audit Pass Interval (in minutes)	Specifies the minimum interval between Policy Data Subscription expiry audits. **Default value**: 10 **Range**: 1-1440

8. Perform the following steps to configure **Advanced Settings** that allows PDS to handle concurrent requests:

   a. Click the ⊕ Add

Copyright © 2019, 2026, Oracle and/or its affiliates.

The page opens the **Add Advanced Settings** dialog box.

b. In the dialog box, enter the following **keys** and respective **values**:

Table 7-139 Parameters for Advanced Settings

Keys	Value
NOTIFICATION_DATA_COMPARE_FLAG	When enabled, this flag compares the incoming notification content with existing data in the database for a subscriber. If there is any change identified, PDS notifies the context owner, otherwise notification will not be forwarded to core service (context-owner). **Default Value**: `false`
CONCURRENT_REQUEST_GUARD_TIME	On receiving `resetContext` flag for a resource from core-service, PolicyDS keeps the association per subscriber resource that are within the time period (in milliseconds). Any other associations which are beyond this time period are cleaned up. **Default Value**: 10000 millisecond **Note**: When Usage Monitoring feature is enabled and Concurrency Control is enabled in Usage Monitoring settings, set the value of CONCURRENT_REQUEST_GUARD_TIME=0.
OPTIMISTIC_RETRY_MAX_ATTEMPT	In case of concurrent DB transactions, if DB operation failed then for these many number of times the DB operation can be re-attempted. **Default Value**: 2
POLICYCOUNTER_QUERY_OPTIMIZE	This flag optimizes whether on asynchronous lookup to CHF/OCS, the create/update subscription request goes out or not. Default Value: true • **true**: No lookup is made to CHF/OCS if subscription already exists. • **false**: A lookup is always performed against CHF/OCS, regardless of whether subscription information is already available in the policy. The latest subscription information is fetched and/or updated in CHF/OCS. **Note**: Setting this setting to false may adversely affect performance, particularly when the policy is not configured correctly. In such cases, every asynchronous CHF/OCS lookup blockly action triggers a CHF/OCS call, regardless of whether valid subscription information is already available in the policy. Contact Oracle Support before changing this flag to false.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
ACTION_ON_SSV_REMOTE_IN_REVALIDATION_OR_NOTIFICATION	Used to control the behavior (IGNORE/ OVERRIDE) of Subscriber Remote section during: • revalidation of subscription for N+ sessions • UDR notification This parameter can take the following values: • **OVERRIDE**: To override the Subscriber Remote section if Revalidation limit reached and a new SM data is received. • **IGNORE**: To retain/preserve old Subscriber Remote section even if the Revalidation limit is reached and a new SM data is received. **Default Value**: OVERRIDE
PDS_SEARCH_USING_All_UEIDS	Used when **typeOfSearch** field is set to **Preferential Search**. When set to true, the preference order will be ignored. PDS will use all the UE Ids available in the request as search indexes and use them one by one to search for Pdsprofile record. **Default Value**: false **Note**: When typeOfSearch field is set to **Multi-UE Id search** this configuration is not considered.
CONCURRENCY.BULWARK_ENABLED_FOR_CHF_NOTIFICATION	Determines whether to enable Bulwark service for CHF notification flow. **Default Value**: false
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_CHF_NOTIFICATION	The number of retries when a request to Bulwark service fails for CHF notification flow. **Default Value**: 3
CONCURRENCY.LOCK_LEASE_DURATION_FOR_CHF_NOTIFICATION	Duration in (milliseconds) for which the lock can be held for CHF Notification. **Default Value**: 2000 (ms)
CONCURRENCY.LOCK_WAIT_DURATION_FOR_CHF_NOTIFICATION	Duration in (milliseconds) for which the CHF can wait to acquire a lock once it sends a request to Bulwark service. **Default Value**: 3000 (ms)
CONCURRENCY.LOCK_REQUEST_KEY_TYPE_FOR_CHF_NOTIFICATION	Determines the key value that is used to acquire the lock for CHF Notification. **Default Value**: SUPI
CONCURRENCY.BULWARK_ENABLED_FOR_OCS_NOTIFICATION	Determines whether to enable Bulwark service for OCS notification flow. **Default Value**: false
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_OCS_NOTIFICATION	The number of retries when a request to Bulwark service fails for OCS notification flow. **Default Value**: 3
CONCURRENCY.LOCK_LEASE_DURATION_FOR_OCS_NOTIFICATION	Duration in (milliseconds) for which the lock can be held for OCS Notification. **Default Value**: 2000 (ms)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
CONCURRENCY.LOCK_WAIT_DURATION_FOR_OCS_NOTIFICATION	Duration in (milliseconds) for which the OCS can wait to acquire a lock once it sends a request to Bulwark service. **Default Value**: 3000 (ms)
CONCURRENCY.LOCK_REQUEST_KEY_TYPE_FOR_OCS_NOTIFICATION	Determines the key value that is used to acquire the lock for OCS Notification. **Default Value**: SUPI
CONCURRENCY.BULWARK_ENABLED_FOR_UDR_NOTIFICATION	Determines whether to enable Bulwark service for UDR notification flow. **Default Value**: false
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT_FOR_UDR_NOTIFICATION	The number of retries when a request to Bulwark service fails for UDR notification flow. **Default Value**: 3
CONCURRENCY.LOCK_LEASE_DURATION_FOR_UDR_NOTIFICATION	Duration in (milliseconds) for which the lock can be held for UDR Notification. **Default Value**: 2000 (ms)
CONCURRENCY.LOCK_WAIT_DURATION_FOR_UDR_NOTIFICATION	Duration in (milliseconds) for which the UDR can wait to acquire a lock once it sends a request to Bulwark service. **Default Value**: 3000 (ms)
CONCURRENCY.LOCK_REQUEST_KEY_TYPE_FOR_UDR_NOTIFICATION	Determines the key value that is used to acquire the lock for UDR Notification. **Default Value**: SUPI
CONCURRENCY.LOCK_REQUEST_RETRY_COUNT	The number of retries when a request to Bulwark service fails. **Default Value**: 3
CONCURRENCY.LOCK_LEASE_DURATION	Duration for which lock is held once it is acquired. After this duration, the lock will be released automatically. **Default Value**: 6000 (ms)
CONCURRENCY.LOCK_WAIT_DURATION	Duration for which the Policy service will wait for the response to get a lock. The same duration is used by Bulwark service to poll for the lock if a lock is not available. **Default Value**: 3000 (ms)
BULWARK_ERROR_CODES	Error codes from Bulwark Service for which Notification can be rejected by PDS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
ENABLE_CUSTOM_ATTRIBUTES_IN_UDR_NOTIFICATION	Determines whether to disable customAttributes in UDR-Notification. That is: If the value of the key is `true`, UDR notification with unmapped variables parsed inside **customAttributes** are forwarded to core service. If the value of the key is `false`, UDR notification with unmapped variables are forwarded to core service as it is received from UDR, without **customAttributes**. **Default value**: `true` **Note**: For PCRF Core to forward the custom attributes to Usage Monitoring service, you must set the value of ENABLE_CUSTOM_ATTRIBUTES_IN_UDR_NOTIFICATION flag to `false`. **Note:** For a fresh installation, it is recommended to set the value of ENABLE_CUSTOM_ATTRIBUTES_IN_UDR_NOTIFICATION flag to `false`.
CREATE_PDSPROFILE_ON_REQUESTPC	Determines whether to create a PDS profile if it is not present. If the value is `true`, create request is sent if PDS Profile is empty. If the value is `false`, delete request is sent if PDS Profile is empty. **Default value**: `true`
PDS_ERROR_HANDLER_ENABLED	This flag enables error handling library integration with PDS service. **Default Value**: false
UPDATE_SSV_DATASOURCE_INFO_ON_CHANGE	This flag is used to avoid additional database operations (SEARCH and UPDATE) required to update the latest data source information received in the PATCH response. Possible values: • `true`: PDS updates the latest data source information in the database received in the PATCH response for SSV entry. • `false`: PDS skips updating the latest data source information in the database received in the PATCH response. When the value of this key is set to `true`, this flag updates SSV's subscription information following each PATCH call. The PATCH call returns updated subscription information. **Default value**: `false`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
UDR_RELATED_RESOURCE	When the UDR_USE_RELATED_RESOURCE is enabled, then this list of resources is used to identify to use the GET/POST UDR information. **Default Value**: AmPolicyData,UEPolicySet Possible values: AmPolicyData,SmPolicyData, UEPolicySet,OperatorSpecificData
UDR_FETCH_RELATED_RESOURCE	This flag fetches related UDR resource and forwards to UDR connector. **Default Value**: false
NOTIFY_PCF_SM_ON_SUBSCRIPTION_FAILURE	Indicates whether to notify the SM service if there is a subscription failure. **Default Value**: false
SUBSCRIPTION_FAILURE_NOTIFICATION_DELAY	Indicates the delay for the initial subscription failure notification (in milliseconds). **Default Value**: 3000
SUBSCRIPTION_FAILURE_NOTIFICATION_RETRY_COUNT	Indicates the retry count for subscription failure notification (if value is 3 then maximum 3 calls will be done including first web call). **Default Value**: 3
SUBSCRIPTION_FAILURE_NOTIFICATION_RETRY_DELAY	Indicates the delay between retry of subscription failure notification. **Default Value**: 3000
PDS_NOTIFY_USER_DATA_REQUEST_PRIORITY	Set request priority for Notify user data requests. **Allowed Values**: 0-100 **Default Value**: 18
PDS_GET_USER_DATA_REQUEST_PRIORITY	Set request priority to fetch User data request. **Allowed Values**: 0-100 **Default Value**: 18
PDS_UPDATE_USER_DATA_REQUEST_PRIORITY	Set request priority to update User data for request. **Allowed Values**: 0-100 **Default Value**: 18
PDS_DELETE_USER_DATA_REQUEST_PRIORITY	Set request priority to delete User data request. **Allowed Values**: 0-100 **Default Value**: 16
PDS_AUDIT_NOTIFY_REQUEST_PRIORITY	Set request priority to Audit notify request. **Allowed Values**: 0-100 **Default Value**: 27
CONGESTION_RESPONSE_CODE	Configure the response code of the rejected requests by PDS due to congestion state. By default, PDS sends 503 as response code. The user can configure this parameter with either 1xx, 3xx, 4xx, or 5xx response codes.. **Allowed Values**: 1xx, 3xx, 4xx, or 5xx **Default Value**: 503

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
ENABLE_STACK_TRACE_FOR_DB_OPS	This flag helps to prevent the flooding of stack trace logs in case of Optimistic exception or other DB exceptions. When this flag is enabled, it prints the complete exception stack trace. When this flag is disabled, it prints the exception message rather than the complete stack trace. **Default Value**: false
CONCURRENCY.LOCK_RETRY_MODE	Indicates whether the lock retry must be triggered under PDS. Possible values are: • **CLIENT_ONLY**: lock retry is triggered only in client services. • **SERVER_ONLY**: lock retry is triggered only in bulwark. • **CLIENT_AND_SERVER**: lock retry is triggered by both server and client.(server will retry to acquire the lock till the lockWaitTimeout is expired and client will retry after the configured request backOff timer is expired) • Consumer service's advance settings should be updated with the non-zero lockWaitTimeOut.
PRIMARYKEY_LOOKUP_ENABLED	When this flag is enabled, PDS performs primary key based search in its DB during delete, query on update and query on terminate call flows. Currently, this key is supported for SM, AM, UE and PCRF Core services only. This key is not supported during a multi-dnn scenario. **Note** To understand the limitations of this feature, refer to the note section after this table. **Default Value**: false
CONCURRENCY_DETECTION_CURRENT_FLOW_ENABLED	This flag is used only when `PRIMARYKEY_LOOKUP_ENABLED` flag is enabled. If not then the optimistic merge is performed in the existing call flow. When this flag is enabled, PDS ensures concurrency handling using optimistic merge in the existing call flow. When this flag is disabled, PDS handles the optimistic merge in the subsequent create/notify call flows. **Default Value**: false
USE_SAVE_METHOD_TO_INSERT	When this flag is enabled, JPA uses save instead of saveAll to improve the performance. **Default Value**: `true`
ENABLE_PDS_PROFILE_ENTITY_DELETE	When this flag is disabled, PDS DB profile deletion is not be done when all the sessions are deleted, instead audit service handles its deletion. **Default Value**: `true`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
NOTIFICATION_RETRY_COUNT	The number of tries performed by PDS to respective context owner for PDS location information notification after optimistic merge in case of non 2xx and non 404. **Default Value**: 3
NOTIFICATION_RETRY_DELAY	The delay between the retries performed for PDS location information notification to the context owners. The delay value is provided in milliseconds. **Default Value**: `3000`
CHF_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
UDR_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
AM_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
SM_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
UE_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 0
ENABLE_PDS_DB_HISTOGRAM_METRICS	Indicates whether to enable the following database histogram metrics for PDS: • occnp_db_processing_latency_seconds • occnp_http_in_conn_processing_latency_seconds • occnp_http_out_conn_processing_latency_seconds **Default value**: true **Note**: Enabling ENABLE_PDS_DB_HISTOGRAM_METRICS flag will lead to performance degradation and hence, should not be enabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
DATA_COMPRESSION_CTX_INFO_EX_CHAR_SUPPORT	This setting is used to support extra characters in contextInfo column when PDS compression is enabled. When PDS compression and DATA_COMPRESSION_CTX_INFO_EX_CHAR_SUPPORT are enabled, you can support more contexts. However, if you disable either of these features later, you may lose older contexts in the next call flow for this resource. This will happen unless the uncompressed context information is small enough to fit within the specified CONTEXT_INFO_COLUMN_LIMIT. **Default value**: false
ENABLE_ERROR_HANDLING_FOR_REVALIDATION	Indicates whether to handle the errors for revalidation using error configurations for PDS as described in Error Configurations. This key accepts a Boolean value. If the value of this key is set to `true`, the revalidation errors are handled using error configurations for PDS. **Default value**: false
PDS_ERROR_HANDLER_ENABLED	Indicates whether or not to integrate the error handler library with all the flows to/from PDS. This key accepts a Boolean value. If the value of this key is set to `true`, the error handler library is integrated with the PDS call flows. **Default value**: false
REVALIDATE_GET_SUBSCRIPTION_SMPOLICYDATA_ENABLED	This key determines whether to use UDR GET operation or UDR PUT operation for the revalidation requests for which the subscriber info is `SmpolicyData` type PDS call flows. This key accepts a Boolean value. If the value of this key is set to `true`, GET operation is used for revalidation call flow. If the value of this key is set to `false`, PUT operation is used for revalidation call flow. **Default value**: false
REVALIDATE_GET_SUBSCRIPTION_OPERATORSPECIFICDATA_ENABLED	This key determines whether to use UDR GET operation or UDR PUT operation for the revalidation requests for which the subscriber info is `OperatorSpecificData` type PDS call flows. This key accepts a Boolean value. If the value of this key is set to `true`, GET operation is used for revalidation call flow. If the value of this key is set to `false`, PUT operation is used for revalidation call flow. **Default value**: false

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
REVALIDATE_GET_SUBSCRIPTION_AMPOLICYDATA_ENABLED	This key determines whether to use UDR GET operation or UDR PUT operation for the revalidation requests for which the subscriber info is `AmPolicyData` type PDS call flows. This key accepts a Boolean value. If the value of this key is set to `true`, GET operation is used for revalidation call flow. If the value of this key is set to `false`, PUT operation is used for revalidation call flow. **Default value**: false
REVALIDATE_GET_SUBSCRIPTION_UEPOLICYSET_ENABLED	This key determines whether to use UDR GET operation or UDR PUT operation for the revalidation requests for which the subscriber info is `UePolicySet` type PDS call flows. This key accepts a Boolean value. If the value of this key is set to `true`, GET operation is used for revalidation call flow. If the value of this key is set to `false`, PUT operation is used for revalidation call flow. **Default value**: false
POLICY_DATA_SUBSCRIPTION_EXPIRY_ENABLED	This key is used to control the subscription expiry persistence in PolicyDS database for new / revalidated sessions and the same can be verified in `subscription_expiry` column of pdssubscriber table and `occnp_policy_data_subscription_expiry_status_total` metric. **Default value**: true
ENABLE_OCS_ERROR_HANDLING	This flag controls whether PDS sends a notification to SM when PDS receives an OCS transaction error for SLR requests REQUEST-PC based OCS transactions. When the value is true, PDS sends the notification. **Default value**: false
NF_PEER_INFO_FIND_OPTIMIZE_SRC	When this flag is enabled, `srcServInst` is selected based on the oldest context owner when the saved `srcServInstance` value or the incoming `srcServInstance` value is invalid, especially during notification. **Default value**: true
OPTIMISTIC_RETRY_BACKOFF_TIME_MS	Specifies the initial backoff delay in milliseconds, before retrying a DB operation that fails due to a concurrency-related exception such as OptimisticLockException, StaleStateException, or ConstraintViolationException. The retry count is controlled by `OPTIMISTIC_RETRY_MAX_ATTEMPT`. **Default value**: 10

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-139 (Cont.) Parameters for Advanced Settings

Keys	Value
DBEXCEPTION_RETRY_BACKOFF_TIME_MS	Specifies the initial backoff delay, in milliseconds, before retrying other retryable DB exceptions that are not classified as concurrency-related. The retry count for these exceptions is controlled by DB_RETRY_MAX_ATTEMPT. **Default value**: 0

> **Note**
>
> **Assumptions/Limitations, when PRIMARYKEY_LOOKUP_ENABLED is enabled:**
>
> - When the revalidation fails in the subsequent create requests and if the entry is deleted in the PDSSUBSCRIBER table, the older associations in core services for that user are not updated with latest PDS Location Information.
> - When this flag is enabled, it is suggested to enable Bulwark in the core services to get the better performance and reduce concurrency.
> - SSV-GET and SSV-UPDATE request triggered by N1N2 Notification from UE service does not handle the pds location information header.
> - If parameters, PRIMARYKEY_LOOKUP_ENABLE is enabled and CONCURRENCY_DETECTION_CURRENT_FLOW_ENABLED is disabled, then the concurrency handling/optimistic merge gets triggered in the subsequent CREATE requests and not for REQUEST-PC.

9. Click **Save**.
   The page saves the PDS settings.

7.3.12.2 PDS Workflow

Using the PDS Workflow page, you can alter the behavior of PDS to suit the network requirements where you are deploying Policy. This page displays the call flow, depending on the value you select for Workflow type and the mode of deployment.

On upgrading to Policy, the system comes up with the default workflow.

To change the PDS workflow, perform the following steps:

1. On the PDS Workflow page, click Edit.
2. Select any of the following values from the drop-down list:

Table 7-140 Workflow Type

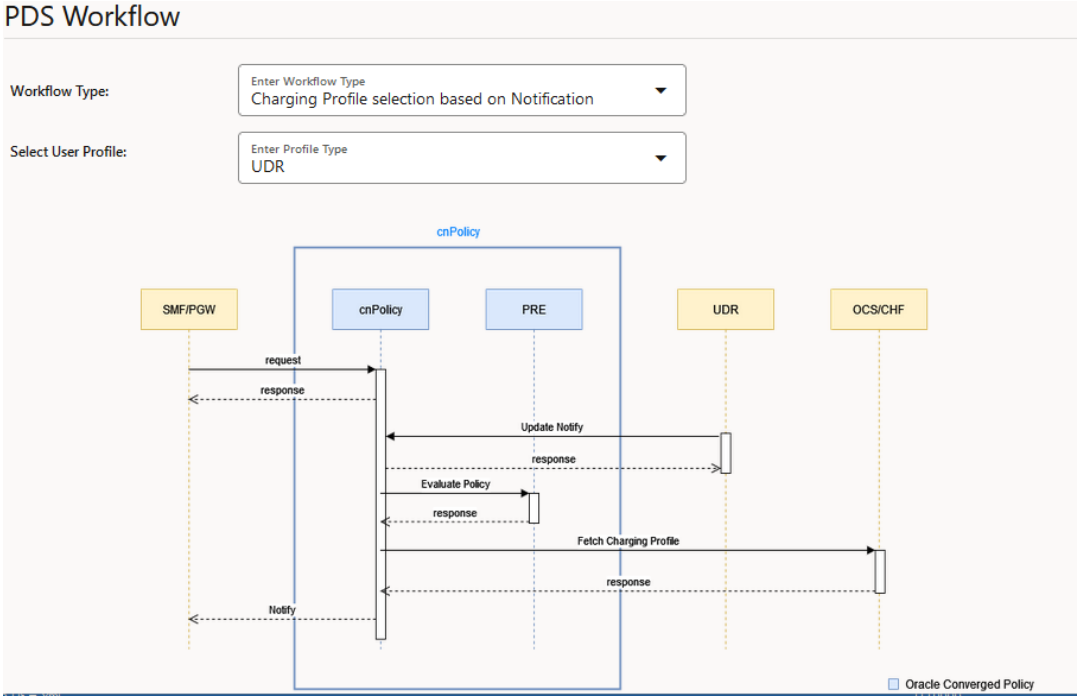
Value	Description
Default	On selecting this option, the default PDS behavior applies.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-140 (Cont.) Workflow Type

Value	Description
Charging Profile selection based on User Profile	On selecting this option, you can configure whether to select user profile from LDAP or UDR. **Note**: For Sy selection per subscriber on the basis of LDAP attribute, select the value LDAP for user profile.
Charging Profile selection based on Notification	On selecting this option, you can configure to select user profile based on Notification from UDR.
Datasource selection based on PRE	On selecting this option, you can configure to select datasource based on PRE.
Custom	For a custom workflow, contact Oracle Policy engineering team and paste the workflow in JSON format provided by the team.

Figure 7-22 PDS Workflow



3. Click **Save** to save your updates.

7.3.12.3 PDS UE ID Configuration

The **PDS UE ID Configuration** page allows to configure the type of query on PolicyDS database.

Policy provides options to query the PolicyDS database based on single UE ID, multiple UE IDs or based on a specific preference.

To configure the type of query on PolicyDS database, perform the following procedure:

1. Navigate to **PDS UE ID Configuration** page under **PDS** for **Service Configurations** in CNC Console.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. On the **PDS UE ID Configuration** page, click **Edit**.
3. Configure the following fields:

Table 7-141 PDS UE ID Configuration

Value	Description
Type Of Search	Indicates the type of query to be performed on the PolicyDS database. This field provides a dropdown list with the following options: • Multi_UE_ID_SEARCH: Specifies a key preference for PDS search query used to look up for a `Pdsprofile` record. When Multi UE ID search is selected the search query uses OR criteria and the search time will be higher. • PREFERENTIAL_SEARCH: When Preferential Search is selected, Preference Order field is displayed. It allows to query based on preferred primary key. • SINGLE_UE_ID_PREFERENTIAL_SEARCH: Specifies a key preference for PDS search query used to look up for a `PDSSubscriber` record.
Subscriber Source Types	Accepts a list of source types supported by PDS for that particular deployment. If it is not provided then by default all source types will be considered. Ideally providing this configuration will limit the source type list to fixed number else unnecessarily all the source types will be considered and DB searches will be made for those source types.
NF Instance ID List	Accepts a list of mated Site IDs for a PCF deployment. In single site setup this configuration might not be required. But in multi-site deployment for single table configuration, all mated site IDs along with self site ID should be provided as a comma separated list.
Primary Key Combination	Specifies the required primary key combination. The primary key can be SUPI,GPSI or a combination of SUPI and GPSI. On selecting the required primary key combination, the requests to PDS is expected to contain that ID. Otherwise, the request is rejected with 400 HTTP error code.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-141 (Cont.) PDS UE ID Configuration

Value	Description
Preference Order	This field must be configured when **Type Of Search** parameter is configured as `PREFERENTIAL_SEARCH`. The value of **Preference Order** parameter specifies the preferred order of keys used for querying the database. • SUPI: Query based on SUPI value. It is mandatory to provide a valid SUPI value. • GPSI: Query based on GPSI value. It is mandatory to provide a valid GPSI value. • SUPI, GPSI: Query on SUPI first and then on GPSI. It is mandatory to provide at least a valid SUPI or GPSI value. • GPSI, SUPI: Query on GPSI first and then on SUPI. It is mandatory to provide at least a valid SUPI or GPSI value.
Migration In Progress	The **Migration In Progress** flag is applicable only when switching between MULTI_UE_ID_SEARCH/ PREFERENTIAL_SEARCH and SINGLE_UE_ID_PREFERENTIAL_SEARCH. This flag is enabled when the records are being migrated from PDSProfile to PDSSubscriber. This flag can be disabled once the migration of all the records are complete. The expectation is that all records must be migrated to updated format. While disabling **Migration In Progress**, Policy console displays the following warning: "Migration should be disabled only when all the records have been migrated. Are you sure you want to disable it?". If **Migration In Progress** flag is disabled while the migration of records is still in progress, the non-migrated records will go stale and can be cleaned up by Audit. **Note** In case of multi-site deployment: • **Migration In Progress** flag can be disabled for a site only if migration is enabled in all the sites with the updated configuration. Otherwise, migration cannot be disabled. • Migration should be disabled in all the sites almost simultaneously to avoid stale subscriptions being left in PDS. • Migration from Single to Single with different Primary Key combinations should be done in all sites almost simultaneously to avoid stale subscription being left in PDS
Migration Status	This section is used to verify the migration status at each site.
Select the site	Allows to list the SiteIDs for a PCF deployment for which the migration status is to be displayed. In case of multi-site deployment, the site IDs must be provided as a comma separated list.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-141 (Cont.) PDS UE ID Configuration

Value	Description
Query Migration Status	Upon clicking this button, Policy console displays the migration status for the specified sites. It includes the number of non-migrated records for configurable time period. The default time period is 1 hour. If clicked later than cache period, the console queries again to fetch the status of latest non-migrated records. **Note**: The query results and the cache period are the same as the ones used for **Query** option available for **Custom Query**. For more information, see Custom Query.

4. Click **Save** to save the configurations.

7.3.13 Binding Service

This procedure provides information about configuring the Binding Service.

The **Binding Service Configuration** page displays the configurations for the Binding Service. You can edit the existing configurations using this page.

To configure the Binding service:

1. From the navigation menu under **Policy**, navigate to **Service Configurations**, and select **Binding Service**.
   This opens the **Binding Service Configuration** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit Binding Service Configuration** page.
3. Check the default configuration for all the fields in all groups and edit as necessary.
   The following table describes the input fields displayed under each group:

Table 7-142 Edit Binding Service Configuration

Field Name	Description
BSF Enabled	Determines if BSF is enabled or disabled. When the value of the **Binding Operation** field is set to false, BSF cannot be enabled.
Binding Use Local Configured Bsf Always	Specifies whether to use local configured BSF without Always discovering. **Default Value**: FALSE
Binding Use Local Configured Bsf When Not Discovered	Whether to use local configured (if having) BSF when not discovered or discover failed. Local configuration can be done using custom yaml. **Default Value**: FALSE
Use HTTP2	Determines if using http/2 to communicate with BSF. Otherwise use http/1.1. **Default Value** : TRUE

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-142 (Cont.) Edit Binding Service Configuration

Field Name	Description
Abort or Terminate Session on BSF Error	Determines if PCF (SM service) should abort terminate session when binding error is received. **Note**: This works for Create, Modify, and Pending Transactions requests only.
Session Limit By User	This parameter can be used to enable or disable user level limiting for bindings at Binding service. Binding service only marks the sessions as stale, and then notifies either SM or PCRF Core to perform the clean-up. The default value for this parameter is true.
Max Session Limit By User	This parameter can be used to specify the maximum session limit for a particular user. The default value for this parameter is 10.
Max Session Limit By APN	Defines the maximum number of concurrent sessions that can be bound to a specific APN for a given subscriber. The default value for this parameter is 2.
Max Session Cleanup Mode	Binding service uses this flag to send request to SM service for either local or remote session clean up. The allowed values for this flag are: • `Local` • `Remote` On choosing the flag to `Local`, PCF deletes the session locally and does not send notify terminate request toward SMF. **Default Value**: Local
Max Session Force Delete On Expiry Of Wait Timer For Remote Cleanup	On `Max Session Cleanup Mode` set to `Remote` this toggle flag appears. It makes `forceDeleteOnExpiryOfWaitTimer` flag to true or false which is used in SM service request for remote cleanup. **Default Value**: false
Max Session Force Delete On Error For Remote Cleanup	On `Max Session Cleanup Mode` set to `Remote` this toggle flag appears. It makes `forceDeleteOnError` flag to true or false which is used in SM service request for remote cleanup. On SM service notify terminate request failure and based on `forceDeleteOnError` flag, the session with 4xx and 5xx response status codes are deleted except for the 404 status code. **Default Value**: false
Apn Filter By Snssai	This parameter can be used to specify the maximum session limit for DNN + SNSSAI + IP domain level. The default value for this parameter is 2.
BSF Retry Profile For Initial Messages	Retry Profile to be used when PCF fails to send a create message to a producer node.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-142 (Cont.) Edit Binding Service Configuration

Field Name	Description
BSF Retry Profile For Subsequent Messages	Retry Profile to be used when PCF fails to send an in-session message to a producer node. **Note:** • If both “Retry Profile for Initial Messages” and “Retry Profile for Subsequent Messages” are not configured (default case) no retry is attempted. • If both “Retry Profile for Initial Messages” and “Retry Profile for Subsequent Messages” are configured, retries is attempted accordingly. • If “Retry Profile for Initial Messages” is configured but “Retry Profile for Subsequent Messages” is not configured then the profile for initial messages is used for subsequent messages. (to be backward compatible with release 1.8.x) • If “Retry Profile for Initial Messages” is not configured but “Retry Profile for Subsequent Messages” is configured then retry is not attempted for initial messages but is attempted for subsequent messages.
BSF Communication Profile	Specifies the NF communication profile used by BSF. For more information about configuring NF communication profiles, see NF Communication Profiles.
Enable Vendor Specific Attribute in Register Request	Determines if PCF sends Vendor-Specific-Attribute in the Binding Create or Register request. By default, the value is set to false.
Vendor ID	**Note**: This field becomes active only when **Enable Vendor Specific Attribute in Register Request** switch is enabled. Specifies the VendorI ID that is mapped to the `vendorId` in the Vendor-Specific-Attribute.
Data Compression Scheme	Specifies the data compression scheme used by Binding Service. Following are the allowed values for this field: • Disabled • Application Compressed By default, this value remains disabled.

4. Expand the **Optimization** section to enable indexing on Binding service database and configure query optimization.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-143 Configuring Optimization of Binding Service

Field	Description
Enable Indexing	Indicates whether data must be migrated to the new format and populated into the index tables. Possible values: • true: `contextBindingId` is made equal to contextId and records are inserted in index-tables. • false: no change to existing call flows, and data migration or indexing is not performed. **Default value**: false
Enable Query Optimization	This field appears only when **Enable Indexing** field is enabled. It indicates if the search needs to be optimized using new approaches: Possible values: • true: search `contextBinding` table using primary key column and also search index table using partition-key, for find context-owner and session limiting features. • false: existing index-key based queries are continued as is. Before enabling **Enable Query Optimization** field, verify on the **Custom Query** page that all records are indexed. **NOTE** • Before enabling the flag, please make sure that the software in all sites are upgraded and all the records are migrated properly to new format. • Unnecessary toggling of this feature flag can create an inconsistent dataset and cause inconsistent behavior in Session Limiting and Rx call flows. **Default value**: false
Preferred Subscriber ID for Session Limit	This field appears only when **Enable Query Optimization** field is enabled. Specifies the preferred subscriber ID used to search bindings during session limiting. Possible values: • SUPI or GPSI • SUPI • GPSI **Default value**: SUPI or GPSI **NOTE**: It is recommended to use the `SUPI` or `GPSI` preference instead of `SUPI or GPSI` for better performance. When a single preference is selected, the binding registration request must include the selected subscriber identifier. Otherwise, the Session Limiting feature might behave inconsistently.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. Expand the **Audit** group.
   This group allows you to edit Audit configurations.
6. Enter the values for the input fields, available under the group.

Table 7-144 Edit Audit Configurations

Field Name	Description
Enabled	Determines whether to send registration request to Audit service or not. **Default Value**: True
Notification Rate (per second)	Defines the number of stale records which Audit service notifies to Binding service in one second. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)
Binding Age (in minutes)	Defines the binding age in minutes, after which the record is considered stale. Audit service notifies Binding service and Binding service validates the record with the owning core service, such as SM or PCRF Core. **Default Value**: 1500
Maximum Binding Age (in minutes)	Defines the maximum binding age in minutes, after which the Binding session record becomes eligible for alternate site audit handling. **Default Value**: 2940
Minimum Audit Attempts	Specifies the minimum number of failed audit attempts required before Audit service sends a maxTTL notification with maxTtlReached=true. When maxTTl is reached, Audit service compares the total attempts stored in auditAttempts with minAuditAttempts. If auditAttempts < minAuditAttempts, the notification is sent with maxTtlReached=false; if auditAttempts >= minAuditAttempts, the notification is sent with maxTtlReached=true. **Range**: 0-255 **Default Value**: 0 **Note**: If forceTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until forceTTL is reached.
Minimum Audit Passes Interval (in minutes)	Specifies the minimum interval in minutes between two consecutive audit passes for Binding audit tables. **Default Value**: 15
Revalidate with BSF	Determines whether to revalidate the binding session details with BSF. When this field is enabled, Binding service sends a request for revalidating the binding session records for valid PDU sessions in BSF. **Default value**: false
BSF Retry Profile For Revalidation Messages	Specifies the retry profile for revalidating the session binding records with BSF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-144 (Cont.) Edit Audit Configurations

Field Name	Description
Message Priority Profile	Select one of the message priority profiles created on **Message Profiles** page that must be applied for Binding Service. When a message profile is selected under **Message Priority Profile** section, support for `3GPP-SBI-Message-Priority` header gets enabled for Binding Service.

7. Click **Save**.
   The page saves the Binding Service configurations.
8. Perform the following steps to configure **Advanced Settings** that sets the key for configuring congestion response code and message priority to various rest API end points:
   a. Click the ⊕ Add
      The page opens the **Add Advanced Settings** dialog box.
   b. In the dialog box, enter the following **key** and respective **value**:

Table 7-145 Parameters for Advanced Settings

Keys	Value
CONGESTION_RESPONSE_CODE	Configure the response code of the any rejected requests by Binding service due to congestion state. By default, Binding service sends 503 as response code. The user can configure this parameter with either 1xx, 3xx, 4xx, or 5xx response codes. **Allowed Values**: 1xx, 3xx, 4xx, or 5xx **Default Value**: 503
AUDIT_MESSAGE_PRIORITY	Set request priority for Audit notification request. **Allowed Values**: 0-100 **Default Value**: 30
BSF_AUDIT_MESSAGE_PRIORITY	Set request priority for BSF Audit request. **Allowed Values**: 0-100 **Default Value**: 27
DEPENDENT_CONTEXT_BINDING_REGISTER_MESSAGE_PRIORITY	Set request priority for registering binding contextbinidng request. **Allowed Values**: 0-100 **Default Value**: 24
DEPENDENT_CONTEXT_BINDING_DEREGISTER_MESSAGE_PRIORITY	Set request priority for deregistering binding contextbinding request. **Allowed Values**: 0-100 **Default Value**: 16
DEPENDENT_CONTEXT_BINDING_FIND_CONTEXT_OWNER_MESSAGE_PRIORITY	Set request priority for finding dependent contextBinding owner request. **Allowed Values**: 0-100 **Default Value**: 16

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-145 (Cont.) Parameters for Advanced Settings

Keys	Value
SESSION_BINDING_REGISTER_MESSAGE_PRIORITY	Set request priority for session binding register request. **Allowed Values**: 0-100 **Default Value**: 24
SESSION_BINDING_UPDATE_MESSAGE_PRIORITY	Set request priority for session binding update request . **Allowed Values**: 0-100 **Default Value**: 20
SESSION_BINDING_DEREGISTER_MESSAGE_PRIORITY	Set request priority for deregistering session binding request. **Allowed Values**: 0-100 **Default Value**: 16
SESSION_BINDING_SEARCH_MESSAGE_PRIORITY	Set request priority for searching session binding request. **Allowed Values**: 0-100 **Default Value**: 30
SESSION_BINDING_FIND_CONTEXT_OWNER_MESSAGE_PRIORITY	Set request priority for finding binding context owner request. **Allowed Values**: 0-100 **Default Value**: 16
SESSION_BINDING_CLEANUP_MESSAGE_PRIORITY	Set request priority for session binding cleanup request. **Allowed Values**: 0-100 **Default Value**: 30
BSF_SESSION_UPDATE_MESSAGE_PRIORITY	Set request priority for binding session update. **Allowed Values**: 0-100 **Default Value**: 20
STALE_SESSION_TRACKER_REFRESH_MESSAGE_PRIORITY	Set request priority for tracking stale session request. **Allowed Values**: 0-100 **Default Value**: 30
ENABLE_LATE_ARRIVAL	Indicates whether to enable or disable validation of the incoming stale requests to Binding service. To enable validation of the incoming stale requests by Binding service, set the value of this key as `true`. **Default value**: `false`
ENABLE_LATE_PROCESSING	Indicates whether to enable or disable validation of the stale requests to Binding service during processing. To enable validation of the stale requests during processing, set the value of this key as `true`. **Default value**: `false`
SESSION_BINDING_REVALIDATION_MESSAGE_PRIORITY	The value of this key specifies the HTTP Header "3gpp-sbi-message-priority" and "oc-message-priority" in the revalidation request. **Default value**: 24

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-145 (Cont.) Parameters for Advanced Settings

Keys	Value
ENABLE_BINDING_DB_HISTOGRAM_METRICS	The value of this key indicates whether to enable or disable the histogram metrics for Binding service database. When the value of this key is set to `true`, histogram metrics for Binding service database is enabled. **Default value**: false
ENABLE_BINDING_HTTP_HISTOGRAM_METRICS	The value of this key indicates whether to enable or disable the histogram metrics for HTTP requests sent towards Binding service. When the value of this key is set to `true`, histogram metrics for HTTP requests sent towards Binding service is enabled. **Default value**: false
BSF_CONNECTOR_TIMEOUT_GUARD	This setting is to configure the timeout guard value for timer handling operations in each request. It takes a numerical value. **Default value**: 20ms
SAVE_SRC_SERV_INST:	This flag indicates whether to save the source service instance in the Binding database. This flag takes effect only when the global flag `ENABLE_NF_PEER_INFO` is enabled. **Default Value**: false

7.3.14 Policy Engine

This section provides information about viewing the Policy service details.

The **Policy Engine** page displays the list of the services available on the Policy deployment.

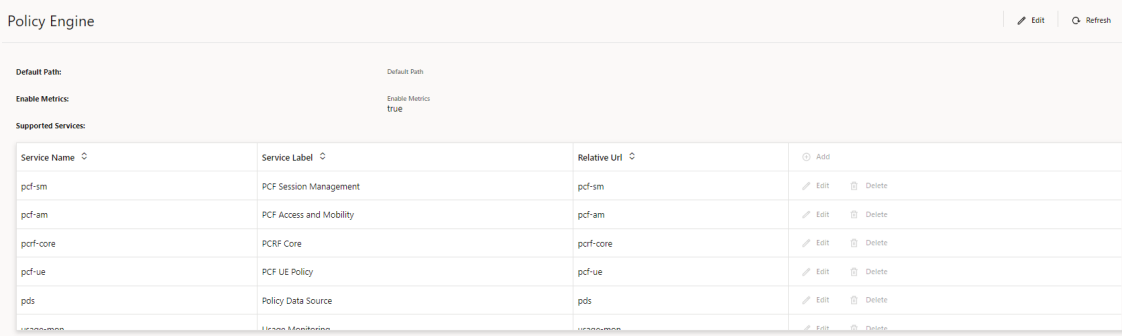
To access **Policy Engine** page from CNC Console home page, expand **Policy**, navigate to **Service Configurations** and select **Policy Engine**.

> **Note**
>
> This page must only be used for adding the Policy Data Source (PDS) service. Rest of the services must not be added or edited using this page.

The following screen capture shows an illustrations of the **Policy Engine** page:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-23 Policy Engine



Configuring PDS Service

To add or configure PDS service:

1. On the **Policy Engine** page, click Edit.
   This opens the **Edit PDS Service** page displaying the supported services in a tabular format, under the **Supported Services** group.
2. Make sure that the Enable Metrics switch is enabled. This field specifies whether to enable the metrics for this functionality. By default, this switch remains disabled.
3. Click Add available in the table.
   The page opens the **Add Supported Services** dialog box.
4. Enter the following information:

Table 7-146 Add Supported Services Configuration

Field Name	Description
Service Name	The name of the service. For PDS, enter the value: `pds`
Service Label	The service label. Enter `Policy Data Source`
Relative Url	Enter `pds`

5. Click **Save** on the dialog box.
   The **pds** service gets listed on the **Edit PDS Service** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the pds service details.

6. On the **Edit PDS Service** page, click **Save**.
   The page saves PDS as the supported service.

7.3.15 Configuring NWDAF Agent

This section provides information on how to configure NWDAF Agent.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.15.1 Settings

This procedure provides information about managing NWDAF Agent Settings

The Settings page allows you to edit Advanced Settings for NWDAF Agent service.

To configure, perform the following steps:

1. From the navigation menu, under **Policy**, click **Service Configurations**, click **NWDAF Agent**, and then select **Settings**.
   This opens the Settings page.
2. Click **Edit**.

   This opens the Edit NWDAF Agent Settings page.
3. Click **Add**.
4. On the **Add Advanced Settings** dialog box, enter values for the following input fields:
   - **Key** - Specify the name of the key.
   - **Value** - Specify the value for the key.
5. Click **Save** to save the advanced settings.
   To discard the changes, click **Cancel**
6. Click **Save** to save the NWDAF Agent Settings.
   To discard the changes, click **Cancel**

7.3.15.2 Slice Load Level

This procedure provides information on how to add and manage Slice Load Level.

The Slice Load Level page allows you to add and edit Slice Load Levels.

To configure, perform the following steps:

1. From the navigation menu, under **Policy**, click **Service Configurations**, click **NWDAF Agent**, click **Autonomous Subscription**, and then select **Slice Load Level**.
   This opens the Slice Load Level Configuration page.
2. Click **Add**.

   This opens the Config Slice Load Level page.
3. Enter values for the following input fields, as described in the following table:

Table 7-147 Config Slice Load Level

Field Name	Description
SNSSAI	Identification of network slice to which the subscription applies.
Threshold	Indication of slice load level in percentage.
ImmRep	Indication of immediate reporting.

4. Click **Save**. The Slice Load Level is displayed on the Slice Load Level Configuration page.
   To discard the changes, click **Cancel**

Importing Slice Load Level

To import Slice Load Level :

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.3.16 NRF Agent

Most of the PCF services discovery requests(On Demand Discovery) towards NRF do not use UE identifiers for NF discovery. Hence the requests do not carry correlation-info header. But On Demand Discovery of UDRs requests have the UE identifiers like SUPI or GPSI. These UDR discovery request with UE identifier toward NRF is updated to support correlation-info header.

Policy supports correlation-info header toward NRF by using the **NRF Agent** page in the CNC Console. The NF communication profiles configured for NRF agent, generates or forwards the correlation-header that is used to for NRF discovery requests. To configure NRF Agent Communication profile, perform the following steps:

1. From the navigation menu under **Policy,** navigate to **Service Configurations**, and then select **NRF Agent**. This opens the **NRF Agent** page.
2. Click Edit. This opens **Edit NRF Agent** page.
3. On the **Edit NRF Agent** page, enter the following information:

Table 7-148 Edit NRF Agent

Field Name	Description
NRF Agent Communication Profile	Specifies the NRF Communication Profile to handle correlation info header toward NRF.
On Demand Discovery Caching	**Provide details about On Demand Discovery Caching**
Enable Caching	Indicates NRF Client to cache the profile data and use it to process the future discovery on demand requests. **Default value**: false
Query Parameters	Accepts the list of parameters that NRF Client uses to fetch the profile data from cache. **Note**: The query parameters in the request from SM service, AM service, UE Policy service must match and must be in the same order as the data received from NRF. Otherwise, NRF Client can not process the request. Supported values: • data-set • target-nf-type • requester-nf-type • target-nf-set-id • service-names • amf-region-id • amf-set-id • GUAMI • target-nf-instance-id • group-id-list

Copyright © 2019, 2026, Oracle and/or its affiliates.

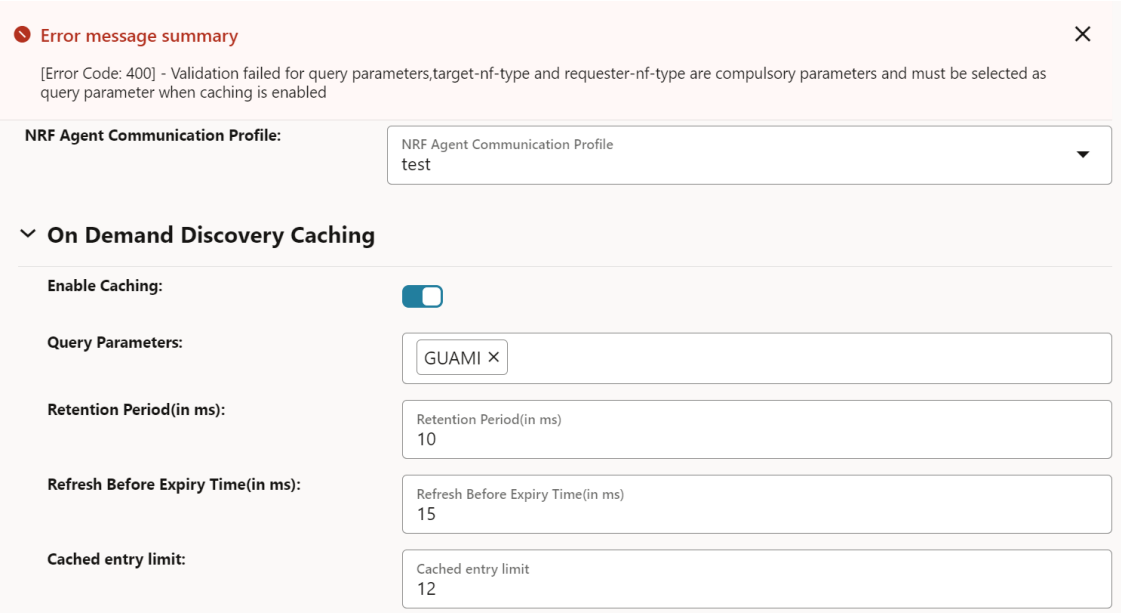
Table 7-148 (Cont.) Edit NRF Agent

Field Name	Description
Retention Period (in ms)	Indicates the time a record is allowed to stay in database after expiry and before any clean process is executed. **Default value**: 864000000
Refresh Before Expiry Time (in ms)	Indicates the time in milliseconds before expiration when a rediscovery must be performed for the requested discovery parameters. **Default value**: 4500
Cached entry limit	Parameter to set the upper bound of cache registries allowed to be retained. **Default value**: 2000
Auditor Scheduler Interval (in ms)	Parameter to set time in milliseconds to activate the Discovery Cache auditor service to clean stale records. **Default value**: 1800000
Auditor Purge Percentage	Parameter to set the percentage of the cached discovery requests that will be pruned once the threshold has been passed. **Default value:** 20

4. Click **Save** to save the changes

When selecting the query parameters to perform on demand discovery by enabling NRF caching, ensure that `target-nf-type` and `requester-nf-type` parameters are selected along with other query parameters. If they are not selected then the configurations are not saved and error message is displayed on the **NRF Agent** page.

Figure 7-24 NRF Agent Error Message



Copyright © 2019, 2026, Oracle and/or its affiliates.

7.3.17 IGW

1. From the navigation menu under **Policy,** navigate to **Service Configurations**, and then select **IGW**. This opens the **Error Code Series List** page.
2. Click Edit on the Error Code Series List.

   This opens **Edit Error Code Series List** page.
3. Click **Add** to add the error code series.

   The **Add Error Code Series** page is displayed.
4. Configure the fields in the **Add Error Code Series** page as mentioned in Table 7-149.
5. Click **Add** in the **Error Code Series** section.

   The **Add Error Code Series** page is displayed.
6. Configure the fields in the **Add Error Code Series** page as mentioned in Table 7-150.
7. Click **Save** on the **Add Error Code Series** page to save the details. Click **Cancel** to discard your progress and go back to **Create Error Code Series** page.
8. Click **Save** on the **Create Error Code Series**page to save the details. Click **Cancel** to discard your progress and go back to **Error Code Series** page.

> **Note**
>
> Use the **Edit** icon or **Delete** available in the next column of the specific entry to update or delete the error code series information.

Table 7-149 Error Code Series

Field Name	Description
Profile	Specifies the name for error code series list profile.
Error Code Series	Lists the error codes for a specific service.

Table 7-150 Error Code Series Configuration

Field Name	Description
Error Set	Possible values for "errorSet" attribute: 5xx, 4xx, 3xx, 2xx, 1xx
Error Codes	Possible values include all error codes in the respective HttpSeries value assigned for "errorSet". **Note**: Use single value of "-1" if all error codes in that HttpSeries are to be considered.

7.3.18 Bulwark

This section describes how to configure Bulwark service.

7.3.18.1 Bulwark Settings

This procedure provides information about managing Bulwark service settings.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure, perform the following steps:

1. From the navigation menu, under **Policy**, click **Service Configurations**, click **Bulwark**, and then select **Settings**.
   This opens the Bulwark Settings page.
2. Click **Edit**.

   This opens the Edit Bulwark Settings page.
3. Under **Server Retry On Already Locked Keys** section, configure the following fields:

Table 7-151 Server Retry On Already Locked Keys

Field	Description
Enable	Indicates whether to enable or disable server retry on already locked keys. To enable the feature, set the value of this field to `true`. **Default value**: `false`
Maximum Pending Lock Requests allowed per Key	Indicates the maximum number of pending lock requests allowed per key. **Default value**: 5

4. Click **Save** to save the settings.
   To discard the changes, click **Cancel**
5. Perform the following steps to configure **Advanced Settings** that sets the key for configuring congestion response code:
   a. Click the Add
      The page opens the **Add Advanced Settings** dialog box.
   b. In the dialog box, enter the following **key** and respective **value**:

Table 7-152 Parameters for Advanced Settings

Keys	Value
CONGESTION_RESPONSE_CODE	Configure the response code of the any rejected requests by Bulwark service due to congestion state. By default, Bulwark service sends 503 as response code. If configured then it shall be 1xx, 3xx, 4xx or 5xx status code. **Default Value**: 503

7.3.19 Diameter Connector

The **Diameter Connector** page allows to configure Diameter Connector.

To edit settings:

1. From the navigation menu, under **Policy**, click **Service Configurations** and select **Diameter Connector**.
   This opens the **Diameter Connector** page. The page displays the existing configurations.
2. Click Edit .

Copyright © 2019, 2026, Oracle and/or its affiliates.

This opens the **Edit Diameter Connector** page.

3. Enter the following information under the respective groups:

Table 7-153 General

Field Name	Description
Redcap Support for Rx Interface	When this field is enabled and if the RAT Type in the PDU session is NR_REDCAP, PCF sends the RATType AVP with value NR_REDCAP to P-CSCF in AAA and RAR messages. When this field is disabled and Rx session is established for the RedCap devices for which the RAT Type of the PDU session is NR_REDCAP: • Policy accepts the session and sends AAA and RAR messages to P-CCSCF without RATType AVP. • Policy increments diam_avp_dropped metric. **Default value**: false

Table 7-154 Stale Request Cleanup

Field Name	Description
Enable Late Arrival	Indicates whether to validate an incoming request if it is stale during arrival. Enable this field to stop processing the incoming requests to Diameter Connector if it already stale. **Default value**: false
Enable Late Processing	Indicates whether to validate a request at Diameter Connector if it is stale during processing. Enable this field to stop processing the requests at Diameter Connector if it becomes stale during processing. **Default value**: false
Skip Late Processing For Terminate	Indicates whether to skip validating requests of type DELETE if the request becomes stale during arrival and processing. **Default value**: false
SBI Timer Enabled	Indicates whether to handle HTTP SBI headers that are attached to incoming request. **Default value**: false

4. Configure the Advanced Settings keys for Diameter Connector:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-155 Advanced Settings for Diameter Connector

Key	Description
ENABLE_REL18_ENCODING_FOR_NCGI	Specifies whether to enable PCF to encode NCGI field value as per 3GPP-User-Location-Info as specified in Rel18 29061 v10. When the value of this key is set to `true`, the NCGI and 5GS TAI And NCGI Geographic Location Filed values are encoded starting from left side placing the first 4 bits as spare bits just after the PLMN Identity and these spare bits are set to zero and next 36 bits set to the NCGI and 5GS TAI And NCGI field values. When the value of this key is set to `false`, in Geographic Location field both 5GS TAI and NCGI shall be encoded one after another and the spare bits are set to zero. **Default value**: false

5. Click **Save** to save the configuration.

7.4 Policy Data Configurations

This section describes how to create the manageable objects (MOs) in Policy, using the **Policy Data Configurations** pages.

7.4.1 Common

This section includes the common services configurations for Policy services.

To access Common Data functionality from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations** and select **Common**.

The common configurations include:

- Policy Table
- Dropdown Blocks
- PCF Presence Reporting Area
- Policy Counter ID
- Match List
- Schemas

7.4.1.1 Policy Table

Policy Tables are the independent objects that can be used to capture differences in policy structures.

Most of the policies are very similar with small differences between them. A policy table abstracts the differences between related policies. Instead of creating many similar policies, using a policy table makes the tasks of adding new policies, modifying existing sets of policies, and checking consistency among related policies simpler and less prone to error.

A Policy table resembles the database tables and consists of the following elements:

- Table name

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Table description
- Column definitions
  Every column has a definition that contains a name, data type, and indication if the column is a key column. Every entry in the column is of the same data type as the column. Every policy table must have at least one key column.
- Data
  The contents of the table cells. Blank cells are not allowed in a policy table.

Each row in a policy table can be thought of as a scenario. Substitutions in policy condition and action parameters can include the values in a specified policy table.

> **Note**
>
> CNC Policy supports Policy Table for the following services:
>
> - SM
> - AM
> - UE Policy
> - PCRF Core
> - Usage Monitoring

You can manage multiple policies with small differences by abstracting the differences into tables. This makes the process of modifying the policies, or creating new or similar policies a matter of modifying the policy table, which is simpler and less prone to error.

Managing Policy Tables

This section describes how to create, modify, delete, and view policy tables.

To access Policy Table configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations** and select **Policy Table**.

The **Policy Table** page allows you to perform the following tasks:

- Configure Policy Table
- Associating a Policy Table with a Policy

7.4.1.1.1 Configure Policy Table

This procedure provides information on how to create and manage Policy Tables.

The **Policy Tables** page allows you to create new and manage existing policy tables. The page displays the list of available policy tables and provides the options to create, configure, import, export, clone, modify, or delete the tables.

> **Important**
>
> When you define a policy table, it must contain at least one key column and one row, and you must populate every cell in the table.

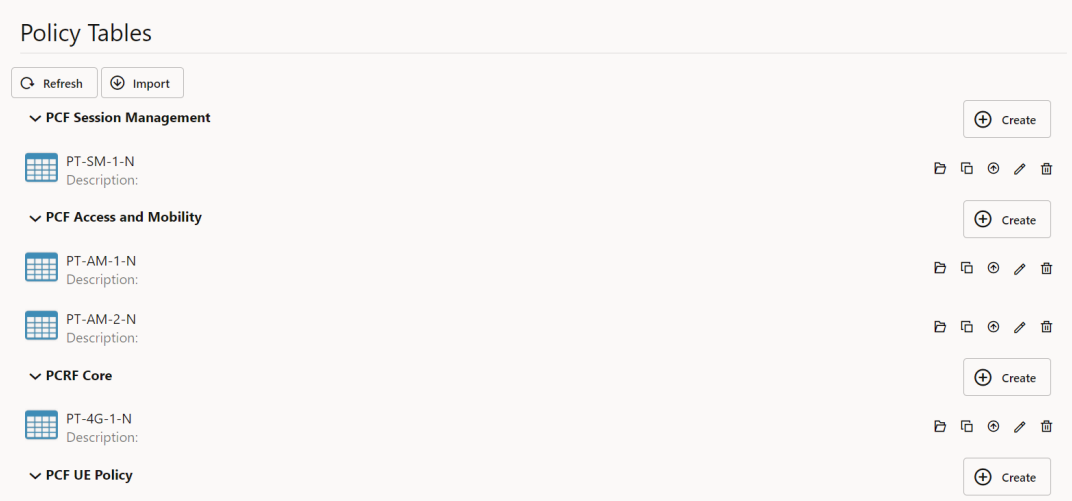
To create and configure a policy table, perform the following steps:

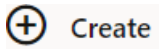
Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the **Policy Management** section of the navigation pane, select **Policy Table**.

   This opens the **Policy Tables** page, displaying the existing policy tables for the respective policy service.
   The following screen capture shows an illustration of the **Policy Tables** page:

Figure 7-25 Policy Tables



2. Click  for the service group, for which the policy table is to be created.

   The page opens the **Create Policy Table** dialog box.

3. In the **Create Policy Table** dialog box, enter the following information:

Table 7-156 Create Policy Table

Field Name	Description
Name	The unique name you assign to the policy table. This is a mandatory field. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underscore (_). The maximum length is 32 characters.
Description	Free-form text that identifies the policy table. The maximum length is 255 characters.

> **Note**
>
> Name can not be the substring of any other configured Policy Table Name.

4. Click **Save**.

   This creates the Policy Table. The table gets listed under the respective service name group.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> - You can create maximum 80 tables per service type.
> - The **Policy Table** page allows you to clone policy tables. Use the icon available with the table listing, to clone a policy table. The cloned table contains the data similar to the table from which it is cloned.
> - Use or available with the table listing, to update or delete the policy table.

5. To configure the policy table, click corresponding to the policy table name.

   This opens a new page for the selected policy table. You can configure the table rows and columns using this page.

6. Click Create Column .

   The page opens the **Create Policy Table Column** dialog box.

> **Note**
>
> You must define at least one key column. You can define maximum 15 key columns in a policy table.

Enter the information as appropriate:

Table 7-157 Create Policy Table Column

Field Name	Description
Name	The name you assign to the column. This is a mandatory field. The name can only contain the characters A–Z, a–z, 0–9, space ( ), and underscore (_). The maximum length is 32 characters. **Note:** Column Name must be unique.
Data Type	The data type of cells in the column. This is a mandatory field. You can select the required data type from the drop-down list.
Key	Enable this switch if this is a key column. **Note**: By default, the first column is always the **Key** column.

> **Note**
>
> Name can not be the substring of any other configured Column Name

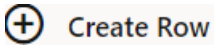
7. Click **Save**.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> You can create maximum 30 columns in a policy table.

This creates the column for the policy table. You can use the  or  to update or delete the columns.

> **Note**
>
> Consider the following points while adding a new column in a policy table:
>
> - The Add, Modify, or Delete operations are allowed for both key and non-key columns, irrespective of the fact whether the policy table contains row(s) or not.
> - A key column can be created for a policy table containing row(s).
> - The row values for the corresponding column and its data type have Empty/ Null Values, you have to manually update the rows, except for boolean data type, which is set to false.
> - While modifying a column, the **Data Type** field remains disabled, if the policy table contain row(s).
> - While editing a column, a warning message is displayed to revisit the policies after editing them. You must agree to it by selecting the checkbox, to enable the **Save** button.
> - A warning is issued to update the policies manually, if the column is deleted.

8. (Optional) You can create rows in the policy table as follows:
   a. Click  .

      The page opens the **Create Policy Table Row** dialog box.
   b. Enter the values corresponding to each column of the policy table. The data in each cell must match with the respective column datatype.
   c. Click **Save**. You can also enter a comma-separated list of values in the **C1** column. Use the data type as array while entering comma-separated values.

   This creates and display the row for the policy table. You can use  or  under the **Action** column to update or delete rows.

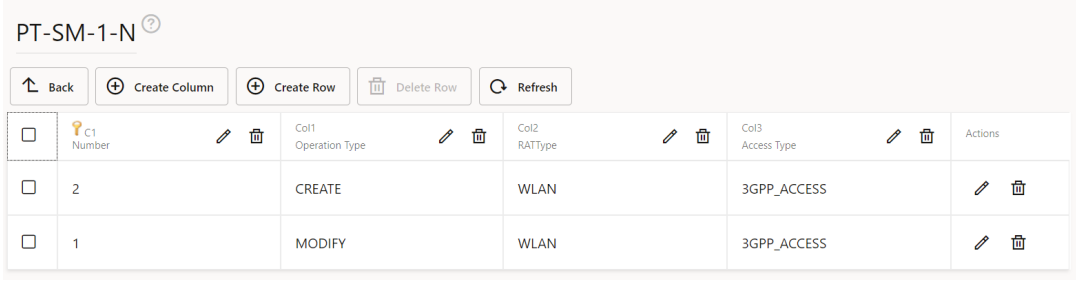
Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> - The policy table loads 100 rows in one fetch. As the user scrolls the page, next set of rows gets loaded and displayed.
> - You can create maximum 3000 rows in a policy table.
> - Make sure that the key column (**C1**) does not hold a combination of duplicate entries, that is, combination of two or more columns in a policy table can be used to uniquely identify each row.
> - One or more wild card values in the key column cell are compared to the values in the policy context data. If there is any match, the row gets matched. The asterisk (*) character represents any number of characters, and the question mark (?) character represents any single character.

The policy table is updated with columns and rows. You can now use the table in a policy.

The following screen capture illustrates an example of a Policy Table with four columns and two rows:

Figure 7-26 Policy Table with Rows and Columns



9. Click Back for returning to the **Policy Tables** page.

> **Note**
>
> he **Policy Table** page allows you to export policy tables. Use the icon available with the table listing, to export the policy table configuration in the JSON file format.

Importing Policy Table

To import a policy table:

> **Note**
>
> The Policy Table Import operation is best suited for smaller policy tables. For policy tables with more than 50 rows, use **Bulk Import**, which is optimized for large datasets to provide better performance, reliability, and a smoother import experience.

10. Click Import .

Copyright © 2019, 2026, Oracle and/or its affiliates.

The page opens the **Upload Policy Table Data** dialog box.

11. Upload the file in JSON format by using the **Drag and Drop** option.
12. After the upload completes for the selected file, choose any of the following values from the **Conflict Resolution Strategy**:

Option	Description
Retain	On selecting the Retain option, no changes are made to the existing Policy Table. No changes are made to the UUIDs and existing policies remain unaffected with this option.
Replace	On selecting the Replace option, the following happens: • No change is made to UUIDs of existing columns. • UUIDs of existing rows is retained if the composite key of the existing row matches with the composite key of incoming row. • New key or non-key columns in the imported file are added to the existing Policy Table with new UUIDs. • Existing rows that are not present in imported file are deleted. **Note**: Column conflict is detected based on the column name and not data type. Using the replace option leads to updates in the Policy Table according to the data present in the import file. For instance, it may result in deletion or addition of key and non-key columns and their respective rows, and change in dataType. Thus, it is recommended to revisit the policies and update wherever required.
Merge	**Note**: Merge option is not allowed and results in an error in the following scenarios: • Change in Key Column: It includes scenarios when user adds a new column, removes an existing key column, or changes data type of existing key column. • Change in datatype of existing non-key column On selecting the Merge option, the following options are enabled: • **Retain**: In case of no conflict, new rows from the import file are created. However, in the case of conflict, no

Copyright © 2019, 2026, Oracle and/or its affiliates.

Option	Description
	change is made to the cell values of the existing rows. In this option, new non-key columns are also added with their corresponding cell values. • **Replace**: In case of no conflict, new rows from the import file are created. However, in the case of conflict, existing cell values are replaced with the cell values of Policy Table in the import file. No change is made to the UUIDs of existing rows. In this option, new non-key columns are also added with their corresponding cell values. **Note**: Two rows are considered to be in conflict when they have same values for the Key columns. If the import file does not contain any existing non-key column, then that column is not removed from the existing Policy table during merge.

13. Click **Import**.

7.4.1.1.2 Associating a Policy Table with a Policy

This procedure provides information on how to associate a policy table with a new or existing policy.

To associate a policy table with a policy, the policy table must already be configured. For information about configuring Policy Tables, see Configure Policy Table.

> **Note**
>
> When a user creates or updates a Policy Table through CNC Console or REST API, it may take up to 30 seconds for the changes to reflect in the policy rule associated with that Policy Table.

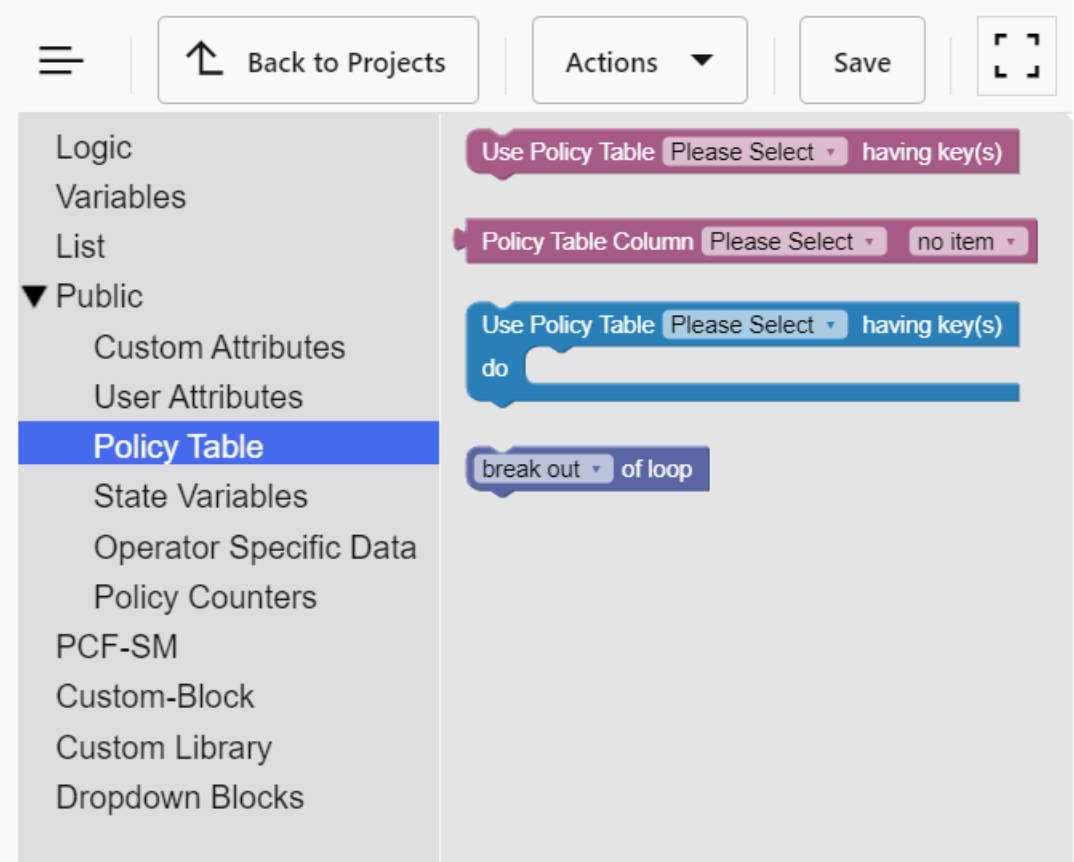
To associate a policy table with a policy rule:

1. From the navigation menu, under **Policy Management**, click **Policy Projects**.
   This opens the **Policy Projects** page displaying all the existing policies.
2. Click  corresponding to the policy to be associated.
   This opens a new page for the selected policy.
3. On the policy page, expand **Public**, and select **Policy Table**.
   This provides you the access to the Policy Table blocks.

   The following screen capture shows an example of Policy Table blocks for a **PCF Session Management** policy:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-27 Example of Policy Table Blocks for SM Policy

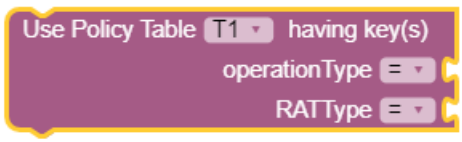


4. In the first block, select the policy table from the **Policy Table** drop-down list.
   The corresponding key columns are displayed in **key(s)**.

   The following screen capture shows an example in which Policy Table **T1** is selected and the **OperationType** and **RatType** are the corresponding key columns in the table **T1**:

> **Note**
>
> This block is being deprecated. Use the third block on the **Policy Tables** page to achieve the functionality of the deprecated block. For more information, see Step 7.

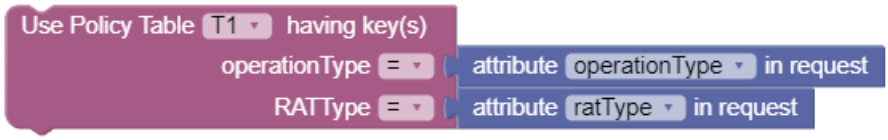
Figure 7-28 Example of Policy Table First Block



5. Select the operator from the operator drop-down list and associate the value or policy condition with the key column. You can select the value or policy condition from **Public** and **PCF-SM** topics. .
   The following screen capture shows an example of associating policy conditions with the key columns, **OperationType** and **RatType**:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-29 Example of Associating Policy Conditions with Key Columns



If all the values associated with the key columns match its column data from the policy table based on the used operator ("="), then it returns the complete row data.

> **Note**
>
> This block can return only single row.

6. In the second block, select the policy table from the **Policy Table Column** drop-down and the corresponding non-key columns are displayed in **no item** drop-down list.
The following screen capture shows an example in which policy table **T1** is selected and the non-key column, **pccRule** is displayed in the drop-down list:

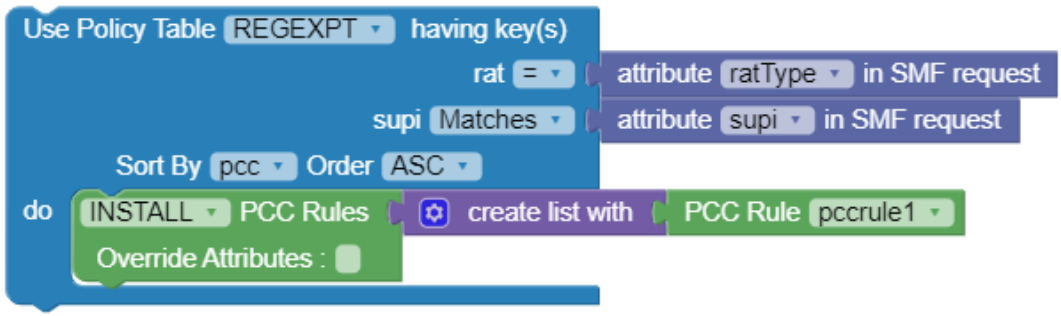
Figure 7-30 Example of Policy Table with non-key Column



This block returns the value of the non-key column selected by taking row data as input from the first block.

7. In the third block, select the policy table from the **Policy Table** drop-down list and the corresponding key and non-key columns are displayed in **key(s)**.
The following screen capture shows an example in which Policy Table **REGEXPT** has been selected and the **rat** and **supi** are the corresponding columns in the table **REGEXPT**.

Figure 7-31 Example of Policy Table with Corresponding Columns



Select the operator from the operator drop-down and associate the value or policy condition with the columns. You can select the value or policy condition from **Public** and

Copyright © 2019, 2026, Oracle and/or its affiliates.

PCF-SM topics. The following screen capture shows an example of associating policy conditions with the columns, **RAT** and **SUPI**.

If all the values associated with the columns match its column data from policy table based on the operator used ("=") and Matches, then it returns the complete row data.

> **Note**
>
> - This block can return multiple rows.
> - For this block, "=", "!=", Matches, and Ignore operators are supported.

8. Click **Save**.

The selected policy tables get associated with this policy rule.

7.4.1.2 Dropdown Blocks

This procedure provides information about how to create and manage dropdown blocks for policy projects.

The **Dropdown Blocks** page allows you to create new and manage existing blocks. The page displays the list of defined dropdown blocks with the options to import, export, or add blocks.

To configure the Dropdown blocks:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **Common**, and select **Dropdown Blocks**.
   This opens the **Dropdown Blocks** page. The page lists the existing dropdown blocks. You can add or import new dropdown block using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Dropdown Blocks** page.
3. On the **Create Dropdown Blocks** page, enter the following information:

Table 7-158 Create Dropdown Blocks

Field Name	Description
Attribute Name	Name of the attribute
Description	Description of the attribute
Type	Select from the following values: • static • dynamic

4. Expand the **Block Options** group.
   This group allows you to add multiple block options.
5. To add block options:

Copyright © 2019, 2026, Oracle and/or its affiliates.

a. Click Add .
The page opens the **Add Block Options** dialog box.

b. On the dialog box, enter the following values:

Table 7-159 Add Block Options

Field Name	Description
Label Name	Name of the block
Value	Specify the value for the block option.

c. Click **Save**.
The block option gets listed under the **Block Option** group on the **Create DropDown Blocks** page.

6. On the **Create DropDown Blocks** page, click **Save**.
The page lists the dropdown block.

> **Note**
>
> Use or available under the **Actions** column to update or delete the dropdown block.

Importing Dropdown Blocks

To import Dropdown Blocks:

1. Click Import .
The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.1.3 PCF Presence Reporting Area

This procedure provides information about how to create and manage PCF Presence Reporting Area (PRA).

The **PCF Presence Reporting Area** page allows you to create new and manage existing PRAs. The page displays the list of defined PRAs and provides the options to import, export, or add PRAs.

To configure PRAs:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **Common**, and then select **PCF Presence Reporting Area**.
This opens the **PCF Presence Reporting Area** page. The page lists the existing PRAs listed in a tabular format. You can add or import new PRAs using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Click Add .
   This opens the **Create PCF Presence Reporting Area** page.
3. On the **Create PCF Presence Reporting Area** page, enter the following information:

Table 7-160 Create PCF Presence Reporting Area

Field Name	Description
Pra Id	The unique identifying number of the PRA list. This field is present if the area of interest subscribed or reported is a Presence Reporting Area. Pra Id can be alphanumeric. It can exceed 3 octets in length. The defined PRA ID ranges (for example, 0–8,388,607 for UE-dedicated and 8,388,608–16,777,215 for Core Network-defined PRAs) are not mandatory constraints, but rather suggested guidelines for classification purposes.
Name	The unique name assigned to the PRA.

4. Expand the **Tracking Area List** group.
   This group allows you to add multiple Tracking Area List
5. To add the Tracking Area Lists:
   a. Click Add .
      The page opens the **Add Tracking Area List** dialog box.
   b. On the dialog box, enter the following values:

Table 7-161 Add Tracking Area List

Field Name	Description
PLMN Id	**Provide the PLMN Id details.**
MNC	Defines the Mobile Network Code. It can be two or three digit number.
MCC	Defines the Mobile Country Code. It should be a 3-digit number.
TAC	28-bit string identifying an E-UTRAN Cell Id as specified, in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents 4 bits. The most significant character representing the 4 most significant bits of the Cell Id appears first in the string, and the character representing the 4 least significant bit of the Cell Id appears last in the string. Pattern: '^[A-Fa-f0-9]{7}$' Example: An E-UTRAN Cell Id 0x5BD6007 be encoded as "5BD6007".

   c. Click **Save**.
      The TAC gets listed under the **Tracking Area List** group on the **Create PCF Presence Reporting Area** page.
6. On the **Create PCF Presence Reporting Area** page, expand the **ECGI List** group.
   This group allows you to add multiple ECGI Lists.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7. To add the ECGI Lists:
   a. Click Add .
      The page opens the **Add ECGI List** dialog box.
   b. On the dialog box, enter the following values:

Table 7-162 ECGI List

Field Name	Description
MNC	Defines the Mobile Network Code of the PLMN. It can be two or three digit number.
MCC	Defines the Mobile Country Code of the PLMN. It should be a 3-digit number.
Eutra Cell Id	28-bit string identifying an E-UTRA Cell Id as specified in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents 4 bits. The most significant character representing the 4 most significant bits of the Cell Id appears first in the string, and the character representing the 4 least significant bit of the Cell Id appears last in the string. Pattern: '^[A-Fa-f0-9]{7}$' Example: An E-UTRA Cell Id 0x5BD6007 be encoded as "5BD6007".

   c. Click **Save**.
      The ECGI List gets listed under the **ECGI List** group on the **Create PCF Presence Reporting Area** page.
8. On the **Create PCF Presence Reporting Area** page, expand the **NCGI List** group. This group allows you to add multiple NCGI Lists.
9. To add the NCGI Lists:
   a. Click Add .
      The page opens the **Add NCGI List** dialog box.
   b. On the dialog box, enter the following values:

Table 7-163 NCGI List

Field Name	Description
MNC	Defines the Mobile Network Code of the PLMN. It can be two or three digit number.
MCC	Defines the Mobile Country Code of the PLMN. It should be a 3-digit number.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-163 (Cont.) NCGI List

Field Name	Description
NR Cell Id	36-bit string identifying an NR Cell Id as specified in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents 4 bits. The most significant character representing the 4 most significant bits of the Cell Id appears first in the string, and the character representing the 4 least significant bit of the Cell Id appears last in the string. Pattern: '^[A-Fa-f0-9]{9}$' Example: An NR Cell Id 0x225BD6007 is encoded as "225BD6007".

c. Click **Save**.
The NCGI List gets listed under the **NCGI List** group on the **Create PCF Presence Reporting Area** page.

10. On the **Create PCF Presence Reporting Area** page, expand the **Global RAN NodeId List** group.
This group allows you to add multiple RAN Node ID Lists.
11. To add the Global RAN NodeId Lists:

a. Click Add .
The page opens the **Add Global RAN NodeId List** dialog box.

b. On the dialog box, enter the following values:

Table 7-164 Global RAN NodeId List

Field Name	Description
PLMN Id	**Provide the PLMN Id details.**
MNC	Defines the Mobile Network Code of the PLMN. It can be a 2- or 3-digit number.
MCC	Defines the Mobile Country Code of the PLMN. It should be a 3-digit number.
N3 Iwf Id	This field is included if the RAN node belongs to non 3GPP access (i.e a N3IWF). It contains the FQDN of the N3IWF.
gNb Id	**Provide the gNb Id details.**
Bit Length	Unsigned integer representing the bit length of the gNB ID within the range 22 to 32.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-164 (Cont.) Global RAN NodeId List

Field Name	Description
gNb Value	Specifies the gNb identifier. The value of the gNB ID is encoded in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents 4 bits. The most significant character representing the 4 most significant bits of the gNB ID appears first in the string, and the character representing the 4 least significant bit of the gNB ID appears last in the string. The string is formatted with following pattern: '^[A-Fa-f0-9]{6,8}$' Example: "382A3F47" indicates a gNB ID with value 0x382A3F47
Nge Nb Id	This field is included if the RAN Node Id represents a NG-eNB. It contains the identifier of an NG-eNB.

c. Click **Save**.
The Global RAN NodeId List gets listed under the **Global RAN NodeId List** group on the **Create PCF Presence Reporting Area** page.

12. On the **Create PCF Presence Reporting Area** page, click **Save**.
The PRA gets listed on the **PCF Presence Reporting Area** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the PRA.

Importing PCF Presence Reporting Area

To import PRA:

1. Click Import .
The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.1.4 Policy Counter Id

This procedure provides information about how to create and manage Policy Counter Ids.

The **Policy Counter Id** page allows you to create new and manage existing IDs. The page displays the list of defined Policy Counter Ids and provides the options to import, export, or add new IDs.

To configure the Policy Counter Id:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **Common**, and then select **Policy Counter Id**.

Copyright © 2019, 2026, Oracle and/or its affiliates.

This opens the **Policy Counter Id** page. The page lists the existing policy counter IDs listed in a tabular format. You can add or import new IDs using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Policy Counter Id** page.
3. On the **Create Policy Counter Id** page, enter values for the following input fields:
   The following table describes the fields:

Table 7-165 Create Policy Counter Id

Field Name	Description
Policy Counter Id	Policy Counter Id's Name.
Name	The unique name of the counter ID. **Note**: Don't use dot (".") or slash ("/") in the while naming the policy counter id. Because, this can lead to parsing or lookup errors in real deployments. However, if you want some sort of separator in the policy counter id name, use dash ("-") or underscore ("_").
Description	Policy Counter Id's description.
Default Status	Checks if provided counter Id in the condition has same default status.

4. Click **Save**.
   The policy counter ID gets listed on the **Policy Counter Id** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the counter ID.

Importing Policy Counter Id Data

To import Policy Counter Ids:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.1.5 Match Lists

In a wireless network, a match list is a set of values in various categories, including Access Point Names (APNs), subscriber IMSIs, Location Area Codes (LACs), Service Area Codes (SACs), Internet addresses, and user equipment identities. Match lists provide allow list (listing

Copyright © 2019, 2026, Oracle and/or its affiliates.

items to be included) and blacklist (listing items to be excluded) functions in policy rules. Match lists support wildcards. Using wild cards, a range of values can be specified compactly.

By using a match list, you can apply a policy to all subscribers in a set of LACs, block access to a list of Internet addresses known to be high risk, and so on.

This procedure provides information about how to create and manage Match Lists.

The **Match List** page allows you to create new and manage existing lists. The page displays the list of defined match lists and provides the options to import, export, or add lists.

To configure match lists:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **Common**, and then select **Match List**.
   This opens the **Match List** page. The page lists the existing match lists. You can add or import new lists using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Match List** page.
3. Enter values for the input fields available on the page:
   The following table describes the fields:

Table 7-166 Create Match List

Field Name	Description
ID	The ID assigned to the match list.
Name	The name assigned to the match list. The name can only contain the characters A-Z, a-z, 0-9, period (.), hyphen (-), and underline (_). The maximum length is 40 characters.
Description	Free-form text
Type	Select from the following: • **String** (default) - The list consists of strings. • **Wildcard String** - The list consists of wildcard match patterns that use an asterisk (*) to match zero or more characters or a question mark (?) to match exactly one character. • **IPv4 Subnet** - IP address in IPv4 subnet. • **IPv6 Subnet** - IP address in IPv6 subnet. • **Regular Expression** - Regular Expression to match the IP address.
Items	Item list to either include or exclude.

4. Click **Save**.
   The match list gets listed on the **Match List** page. It is defined in the database and can now be used in a policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the match list.

Importing the Match Lists

To import match lists:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.1.6 Schemas

Schemas enable operators to accept data in custom format instead of the standard format. This data can then be used to construct conditions and actions.

This section describes how to configure Schemas for Policy.

To access Schemas configurations from CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations**, click **Common**, and select **Schemas**.

On clicking **Schemas**, you can select to customize any of the following configurations:

- Yaml Schemas
- Diameter Schemas

7.4.1.6.1 Yaml Schema

This procedure provides information about how to view, import, and configure the custom schema.

The **Yaml Schema** page allows you to import and manage existing Yaml Schema. The page displays the list of defined Yaml schema and provides the options to import, export, update, or delete the schema.

> **Note**
>
> Any pre-existing data will not be included in the bulk export operation. Therefore, this data should not be deleted unless you are absolutely certain or a backup has been created using the "Export" option provided for the specific row action. In case of modification of pre-existing data, the individual row data must be exported and modified. The modified data then can be imported using the  option.

This section describes how to import a custom schema Yaml file in the CNC Console.

> **Note**
>
> Custom schema yaml file must follow Open API standards.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To import a custom Yaml schema:

1. From the navigation menu under **Schema**, select **Yaml Schema**.
   This opens the **Yaml Schema** page.

   The page lists the details including schema name, Schema Tag, and Actions for the following provisioned schema yaml files:

   - `AmPolicyData`
   - `SmPolicyData`
   - `UePolicyData`

2. Click Import .
   The page opens the **File Upload** dialog box.
3. Upload the file in JSON format by using the **Drag and Drop** button.
4. Select the tags to tag the schema in the selected files. The page supports only **User** tag.
5. Click **Import**.

On successful import, the yaml file gets listed on the **Yaml Schema** page.

- To update any existing schema, click Export , make changes to the exported yaml file, and save it on your system. Then, import the file again.
- To delete any existing service area restriction, click the under the **Action** column.

When a schema is tagged as **User** during import, CNC Policy allows you to access and configure the schema using the **User Attributes** blocks, available under the Public category. When a schema is not tagged, you may access and configure it using the **Custom Attributes** blocks, available under the Public category. For more information, see *Oracle Communications Cloud Native Core Policy Design Guide*.

Sample Yaml Schema

The following is a sample yaml schema:

```
openapi: 3.0.0
info:
  description: Customer
  version: 0.0.1
  title: Customer
paths:
  /:
    get:
      operationId: get
      summary: get
      tags:
        - get
      responses:
        '200':
          description: OK
          content:
            application/json:
              schema:
                $ref: '#/components/schemas/Customer'
components:
  schemas:
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
Customer:
  type: object
  properties:
    phones:
      type: array
      items:
         type: string
    name:
      type: string
    address:
      $ref: '#/components/schemas/Address'
Address:
  type: object
  properties:
    house:
      type: string
    street:
      type: string
    city:
      type: string
```

7.4.1.6.2 Diameter Schemas

This section describes the diameter schemas for user data configurations.

To access Schemas configurations under **Schemas**, select **Diameter Schemas**.

On clicking **Diameter Schemas**, you can select to customize any of the following configurations:

- Custom AVP
- Custom Vendor

7.4.1.6.2.1 Custom AVP

An attribute-value pair (AVP) is used to encapsulate protocol specific information supported by CNC Policy. Diameter messages, such as RAA, CCA, CCR, and RAR are supported by third-party AVP policy conditions. The supported outgoing Diameter messages set or remove the third-party AVPs. For more information, see Custom AVP to Support Third-Party Vendor Specific AVPs.

To create a custom AVP:

1. From the navigation menu, under **Diameter Schemas**, select **Custom AVP**.
   This opens the **Custom AVP** page. The page lists the existing AVPs. You can add or import new AVPs using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Custom AVP** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Enter values for the input fields available on the page:
The following table describes the fields:

Table 7-167 Create Custom AVP

Field Name	Description
AVP Name	The name you assign to the AVP. This is a mandatory field. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Description	Free-form text that identifies the AVP. Enter up to 250 characters.
AVP Code	A unique numeric value assigned to the new AVP. This is a mandatory field.
Vendor	Select a vendor from the vendor list. To add a vendor to the list, see Custom Vendor.
Mandatory Flag	When checked, specifies that is a mandatory attribute. By default this is disabled.
Protect Flag	When checked, specifies the protected AVP values.
May Encrypt Flag	The AVP is encrypted if the checkbox is specified.
Vendor Specific Flag	The AVP is encrypted if the checkbox is specified.
AVP Type	Select the data type from the list: • **address** • **enumerated** • **float32** • **float64** • **grouped** • **id** • **int32** • **int64** • **ipFilterRule** • **octetString** • **time** • **uint32** • **uint64** • **uri** • **utf8String**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-167 (Cont.) Create Custom AVP

Field Name	Description
Parent AVP	If the AVP is a member of a grouped AVP, then the parent AVP must be specified. Select one of the following from the list: • **ADC-Rule-Definition:10415** • **ADC-Rule-Install:10415** • **ADC-Rule-Remove:10415** • **ADC-Rule-Report:10415** • **AF-Correlation-Information:10415** • **Acceptable-Service-Info:10415** • **Access-Network-Charging-Identifier-Gx:10415** • **Access-Network-Charging-Identifier:10415** • **Access-Network-Physical-Access-ID:10415** • **Allocation-Retention-Priority:10415** • **Application-Detection-Information:10415** • **CC-Money** • **Charging-Information:10415** • **Charging-Rule-Definition-3GPP2:5535** • **Charging-Rule-Definition:10415** • **Charging-Rule-Event-Cisco:9** • **Charging-Rule-Event-Trigger-Cisco:9** • **Charging-Rule-Install-3GPP2:5535** • **Charging-Rule-Install:10415** • **Charging-Rule-Remove:10415** • **Charging-Rule-Report-3GPP2:5535** • **Charging-Rule-Report:10415** • **Codec-Data-Tmp:10415**

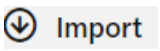
4. Click **Save**.
5. If the AVP name matches the name of a standard AVP, a confirmation message displays. Click **OK** to overwrite the existing AVP.

The Custom AVP gets listed on the **Custom AVP** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the AVP.

Importing Custom AVP

To import the custom AVP:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.4.1.6.2.2 Custom Vendor

A custom vendor is used to define a vendor in the PCRF system. This dictionary includes vendor IDs and text descriptions. You can define custom vendors and add them to the dictionary.

To configure Custom Vendor:

1. From the navigation menu, under **Diameter Schemas**, select **Custom Vendor**.
   This opens the **Custom Vendor** page. The page lists the existing vendors. You can add or import new vendors using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Custom Vendor** page.
3. Enter values for the input fields available on the page:
   The following table describes the fields:

   Table 7-168 Create Custom Vendor

Field Name	Description
Vendor Name	The name you assign to the vendor. This is a mandatory field. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Description	Free-form text that identifies the vendor. Enter up to 250 characters.
Vendor Code	A unique numeric value assigned to the new vendor. This is a mandatory field.

4. Click **Save**.
   The Custom Vendor gets listed on the **Custom Vendor** page.

   > **Note**
   >
   > Use or available under the **Actions** column to update or delete the vendor.

Importing Custom Vendor

To import custom vendor:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Click **Import**.

7.4.2 PCF Session Management

This section includes the configurations for PCF Session Management service.

To access PCF Session Management configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations** and select **PCF Session Management**.

The PCF Session Management configurations includes:

- Session Rule
- Session Rule Profile
- QoS Information
- PCC Rule
- PCC Rule Profile
- QoS Data
- Charging Data
- Traffic Control Data
- Condition Data

7.4.2.1 Session Rule

This procedure provides information about how to create and manage the session rules in CNC Policy.

The **Session Rule** page allows you to create new and manage existing session rule configurations. The page displays the list of defined rules and provides the options to import, export, or add data.

To configure the session rules:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **Session Rule**.
   This opens the **Session Rule** page. The page lists the existing session rules data. You can add or import new rules using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Session Rule** page.
3. On the **Create Session Rule** page, enter the information common to all the groups available on the page.
   The following table describes the common input fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-169 Create Session Rule

Field Name	Description
Session Rule ID	Specifies the Session Rule ID.
Name	Specifies the name assigned to the session rule.
Description	Free-form text that identifies the session rule.

4. Expand the **Authorized Session AMBR** group.
   This group allows you to add authorized session AMBR information.
5. Enter the values for the input fields, available under the **Authorized Session AMBR** group.
   The following table describes the fields:

Table 7-170 Authorized Session AMBR

Field Name	Description
Uplink Bandwidth	Specifies the bandwidth in uplink.
Downlink Bandwidth	Specifies the bandwidth in downlink.

> **Note**
>
> Click the **Remove** button to remove the Authorized Session AMBR details from the page.

6. Select value for **Condition Data** from the drop-down list.
7. Select value for **Authorize Default Qos** from the drop-down list.

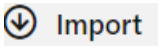
> **Note**
>
> The drop-down list data is configured from the QoS Information. For more information about QoS Data configuration, see QoS Data.

8. Click **Save**.
   The session rule data gets listed on the **Session Rule** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the session rule data configurations.

Importing Session Rules

To import session rules:

1. Click 

   .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.4.2.2 Session Rule Profile

This procedure provides information about how to create and manage the session rule profiles that can be assigned to session rule profiles.

The **Session Rule Profile** page allows you to create new and manage existing session rule profile configurations. The page displays the list of defined rules and provides the options to import, export, or add data.

To configure the session rule profiles:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **Session Rule Profile**.
   This opens the **Session Rule Profile** page. The page lists the existing session rule profiles. You can add or import new profiles using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Session Rule Profile** page.
3. On the **Create Session Rule Profile** page, enter the information common to all the groups available on the page.
   The following table describes the common input fields:

Table 7-171 Create Session Rule Profile

Field Name	Description
Session Rule Profile NAME	Specifies the name assigned to the session rule profile.
Description	Free-form text that identifies the session rule profile.

4. Expand the **Authorized Session AMBR** group.
   This group allows you to add authorized session AMBR information.
5. Enter the values for the input fields, available under the **Authorized Session AMBR** group.
   The following table describes the fields:

Table 7-172 Authorized Session AMBR

Field Name	Description
Uplink Bandwidth	Specifies the bandwidth in uplink.
Downlink Bandwidth	Specifies the bandwidth in downlink.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Click the **Remove** button to remove the Authorized Session AMBR details from the page.

6. Select value for **Condition Data** from the drop-down list.
7. Select value for **Authorize Default Qos** from the drop-down list.

> **Note**
>
> The drop-down list data is configured from the QoS Information. For more information about QoS Data configuration, see QoS Data.

8. Click **Save**.
   The profile data gets listed on the **Session Rule Profile** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the session rule profile configurations.

Importing the Session Rule Profiles

To import session rule profiles:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.2.3 QoS Information

This procedure provides information about how to create and manage the Quality of Service (QoS) information in CNC Policy.

The **QoS Information** page allows you to create new and manage existing information related to QoS configurations. The page displays the list of defined QoS identifiers and provides the options to import, export, or add data.

To configure QoS Information data:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **QoS Information**.
   This opens the **QoS Information** page. The page lists the existing session QoS data. You can add or import new data using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Click Add .
This opens the **Create QoS Information** page.
3. On the **Create QoS Information** page, enter values for the input fields common to all the groups available on the page.
The following table describes the fields:

Table 7-173 Common Configuration on Create QoS Information

Field Name	Description
Name	Specifies the name assigned to the QOS information.
Description	Free-form text that identifies the QOS information.
Default 5G QoS Identifier	Identifier for the authorized QoS parameters for the service data flow. It is included when the QoS information decision is initially provisioned.
Priority Level	Unsigned integer indicating the 5QI Priority Level, within a range of 1 to 127.
Average Window	Represents the duration over which the guaranteed and maximum bitrate is calculated. **Minimum Value**: 1 **Maximum Value**: 4095
Max DataBurstVol	Denotes the largest amount of data that is required to be transferred within a period of 5GAN PDB. **Minimum Value**: 1 **Maximum Value**: 4095

4. Expand the **ARP** group.
This group allows you to add Allocation and Retention Priority (ARP) information.
5. Enter the values for the input fields, available under the **ARP** group.
The following table describes the fields:

Table 7-174 ARP group

Field Name	Description
Priority Level	Unsigned integer indicating the ARP Priority Level, within the range 1 to 15.
Preemption Capability	Defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level. Possible values are: • NOT_PREEMPT : Does not trigger pre-emption. • MAY_PREEMPT : May trigger pre-emption.
Preemption Vulnerability	Defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level. Possible values are: • NOT_PREEMPTABLE : Does not be pre-empted. • PREEMPTABLE : May be pre-empted.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Click the **Remove** button to remove the ARP fields from the page.

6. Click **Save**.
   The QoS information data gets listed on the **QoS Information** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the QoS information.

Importing the QoS Information

To import the QoS Information:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.2.4 PCC Rule

This procedure provides information about how to create and manage the PCC Rules in Policy.

The **PCC Rule** page allows you to create new and manage existing PCC Rule configurations. The page displays the list of defined rules and provides the options to import, export, or add rules.

To configure the PCC rule:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **PCC Rule**.
   This opens the **PCC Rule** page. The page lists the existing session PCC rules data. You can add or import new rules using this page.

> **Note**
>
> Click  to download the available listings in the JSON file format on your system.

2. Click  .
   This opens the **Create PCC Rule** page.
3. On the **Create PCC Rule** page, enter values for the available input fields.
   The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-175 Create PCC Rule

Field Name	Description
PCC Rule Id	Specifies the PCC Rule ID.
Name	Specifies the name assigned to the PCC rule.
Description	Free-form text that identifies the PCC rule.
Type	Select the required type. Possible values are: • Predefined PCC Rule • Dynamic PCC Rule If you have selected Dynamic PCC Rule, then perform Step 4 else, perform Step 5.
Use Custom QoS Class Identifier	When this flag is enabled, you can use the custom QCI values. Default Value: Disabled
QoS Class Identifier (1-254)	When Use Custom QoS Class Identifier flag is enabled, you can use a custom value for this parameter. The value ranges between 1 and 254. When Use Custom QoS Class Identifier flag is disabled, you can select one of the QCIs from the dropdown list box: • 4=Streaming • 5-Interactive with Priority 1 Signaling • 6=Interactive with Priority 1 • 7=Interactive with Priority 2 • 8=Interactive with Priority 3 • 9=Background • 65=MC-PTT Voice • 66-PTT Voice

> **Note**
>
> The name of PCC Rule and PCC Profile must not be same. It is recommended to use unique PCC Rule and PCC Profile names.

4. Expand the **Flow Information** group.
The expanded group displays the available flow information and allows you to add new information.

   To add flow information:

   a. Click ⊕ Add .
   The page opens the **Add Flow Information** dialog box.

   b. On the dialog box, enter values for the following input fields:

Table 7-176 Add Flow Information

Field Name	Description
Name	Indicates the name for the flow.
Pack Filt Id	An identifier of packet filter.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-176 (Cont.) Add Flow Information

Field Name	Description
Packet Filter Usage	The packet is sent to the UE. The default value "FALSE" applies, if the attribute is not present and has not been supplied previously.
Tos Traffic Class	Contains the IPv4 Type-of-Service and mask field or the IPv6 Traffic-Class field and mask field.
Spi	The security parameter index of the IPSec packet.
Flow Label	The IPv6 flow label header field.

c. Click **Save**.
The Flow Information gets listed under the **Flow Information** group on the **Create PCC Rule** page.

5. On the **Create PCC Rule** page, enter the values for the following input fields:

Table 7-177 Create PCC Profile Common Configurations

Field Name	Description
App Id	A reference to the application detection filter configured at the UPF.
Content Version	Indicates the content version of the PCC rule.
Precedence	Determines the order in which this PCC rule is applied relative to other PCC rules within the same PDU session. It is included if the "flowInfos" attribute is included or may be included if the "appId" attribute is included when the PCF initially provisions the PCC rule.
AF Signalling Protocol	Indicates the protocol used for signaling between the UE and the AF. The default value "NO_INFORMATION" applies, if the attribute is not present and has not been supplied previously.
--QoS Flow Usage	Indicates the QoS flow usage. The default value is not applicable for this field. Users can select GENERAL or IMS_SIG from the drop down list as per the requirement.
Application Relocation	Indication of application relocation possibility. The default value "NO_INFORMATION" is applicable, if the attribute is not present and has not been supplied previously.
Qos Data	A reference to the QoSData policy type decision type.
Traffic Control Data	A reference to the TrafficControlData policy decision type.
Charging Data	A reference to the ChargingData policy decision type.
Usage Monitoring Data	A reference to UsageMonitoringData policy decision type.
Condition Data	A reference to the condition data.

6. On the **Create PCC Rule** page, click **Save**.
The PCC profile data gets listed on the **PCC Rule** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the rule data.

Importing the PCC Rules

To import the pcc rules:

1. Click **Import**.
   The **File Upload** window appears on the screen.
2. Upload the files in required format by clicking **Drop Files here or click to upload**.

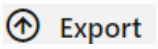
7.4.2.5 PCC Rule Profile

This procedure provides information about how to create and manage the PCC Rule Profiles in Policy.

The **PCC Rule Profile** page allows you to create new and manage existing PCC Rule Profile configurations. The page displays the list of defined profiles and provides the options to import, export, or add profiles.

To configure PCC Rule Profile:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **PCC Rule Profile**.
   This opens the **PCC Rule Profile** page. The page lists the existing session PCC rule profile data. You can add or import new profiles using this page.

   > **Note**
   >
   > Click  to download the available listings in the JSON file format on your system.

2. Click  .
   This opens the **Create PCC Rule Profile** page.
3. On the **Create PCC Rule Profile** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-178 Create PCC Rule Profile

Field Name	Description
Name	Specifies the name assigned to the PCC rule profile.
Description	Free-form text that identifies the PCC rule profile.
Type	Select the required type. Possible Values are: • Predefined PCC Rule • Dynamic PCC Rule If you have selected Dynamic PCC Rule, then perform Step 4 else, perform Step 5.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-178 (Cont.) Create PCC Rule Profile

Field Name	Description
Use Custom QoS Class Identifier	When this flag is enabled, you can use the custom QCI values. Default Value: Disabled
QoS Class Identifier (1-254)	When Use Custom QoS Class Identifier flag is enabled, you can use a custom value for this parameter. The value ranges between 1 and 254. When Use Custom QoS Class Identifier flag is disabled, you can select one of the QCIs from the dropdown list box: • 4=Streaming • 5-Interactive with Priority 1 Signaling • 6=Interactive with Priority 1 • 7=Interactive with Priority 2 • 8=Interactive with Priority 3 • 9=Background • 65=MC-PTT Voice • 66-PTT Voice

4. Expand the **Flow Information** group.
The expanded group displays the available flow information and allows you to add new information.

   To add flow information:

   a. Click ⊕ Add .
   The page opens the **Add Flow Information** dialog box.

   b. On the dialog box, enter values for the following input fields:

   Table 7-179 Add Flow Information

Field Name	Description
Name	Indicates the name for the flow.
Pack Filt Id	An identifier of packet filter.
Packet Filter Usage	The packet is sent to the UE. The default value "FALSE" is applicable, if the attribute is not present and has not been supplied previously.
Tos Traffic Class	Contains the IPv4 Type-of-Service and mask field or the IPv6 Traffic-Class field and mask field.
Spi	The security parameter index of the IPSec packet.
Flow Label	The IPv6 flow label header field.

   c. Click **Save**.
   The Flow Information gets listed under the **Flow Information** group on the **Create PCC Rule Profile** page.

5. On the **Create PCC Rule Profile** page, enter the values for the following input fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-180 Create PCC Rule Profile Common Configurations

Field Name	Description
App Id	A reference to the application detection filter configured at the UPF.
Content Version	Indicates the content version of the PCC rule.
Precedence	Determines the order in which this PCC rule is applied relative to other PCC rules within the same PDU session. It is included if the "flowInfos" attribute is included or may be included if the "appId" attribute is included when the PCF initially provisions the PCC rule.
AF Signaling Protocol	Indicates the protocol used for signaling between the UE and the AF. The default value "NO_INFORMATION" is applicable, if the attribute is not present and has not been supplied previously.
--QoS Flow Usage	Indicates the QoS flow usage. The default value is not applicable for this field. Users can select GENERAL or IMS_SIG from the drop down list as per the requirement.
Application Relocation	Indication of application relocation possibility. The default value "NO_INFORMATION" is applicable, if the attribute is not present and has not been supplied previously.
Qos Data	A reference to the QoS Data policy type decision type.
Traffic Control Data	A reference to the TrafficControlData policy decision type.
Charging Data	A reference to the ChargingData policy decision type.
Usage Monitoring Data	A reference to UsageMonitoringData policy decision type.
Condition Data	A reference to the condition data.

6. On the **Create PCC Rule Profile** page, click **Save**.
   The PCC profile data gets listed on the **PCC Rule Profile** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the profile data.

Importing PCC Rule Profiles

To import PCC Rule Profiles:

1. Click 
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.2.6 QoS Data

This procedure provides information about how to create and manage the QoS data in Policy.

The **QoS Data** page allows you to create new and manage existing data related to QoS configurations. The page displays the list of defined QoS details and provides the options to import, export, or add data.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure QoS data:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **QoS Data**.
   This opens the **QoS Data** page. The page lists the existing session QoS data. You can add or import new data using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create QoS Data** page.
3. On the **Create QoS Data** page, enter values for the input fields common to all the groups available on the page.
   The following table describes the fields:

Table 7-181 Create QoS Data Common Configurations

Field Name	Description
QoS ID	Specifies the QoS ID.
Name	Specifies the name assigned to the QOS data.
Description	Free-form text that identifies the QOS data.
Default 5G QoS Identifier	Identifier for the authorized QoS parameters of the service data flow. It is included when the QoS data decision is initially provisioned.
Maximum Bit Rate UL	Indicates the max bandwidth in uplink.
Maximum Bit Rate DL	Indicates the max bandwidth in downlink.
Guaranteed Bit Rate UL	Indicates the guaranteed bandwidth in uplink
Guaranteed Bit Rate DL	Indicates the guaranteed bandwidth in downlink.
QoS Notification Control	Indicates whether notifications are requested from 3GPP NG-RAN when the GFBR can no longer (or again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow. Default value "FALSE" is used, if not present and has not been supplied previously.
Reflective QoS	Indicates whether the QoS information is reflective for the corresponding service data flow. Default value is "FALSE", if not present and has not been supplied previously.
Sharing Key Ul	Indicates, by containing the same value, what PCC rules may share resource in uplink direction.
Sharing Key Dl	Indicates, by containing the same value, what PCC rules may share resource in downlink direction.
Priority Level	Defines the relative importance of a resource request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-181 (Cont.) Create QoS Data Common Configurations

Field Name	Description
Averaging Window	Represents the duration over which the guaranteed and maximum bitrate is calculated (NOTE).
Maximum Data Burst Volume	Denotes the largest amount of data that is required to be transferred within a period of 5GAN PDB (NOTE).
Maximum Packet Loss Rate Dl	Indicates the uplink maximum rate for lost packets that can be tolerated for the service data flow.
Max Packet Loss Rate Ul	Indicates the uplink maximum rate for lost packets that can be tolerated for the service data flow.
Default QoS Flow Indication	Indicates that the dynamic PCC rule always have its binding with the QoS Flow associated with the default QoS rule. Default value is "FALSE", if not present and has not been supplied previously.

4. Expand the **ARP** group.
   This group allows you to add Allocation and Retention Priority (ARP) information.
5. Enter the values for the input fields, available under the **ARP** group.
   The following table describes the fields:

Table 7-182 ARP Configurations

Field Name	Description
Priority Level	Defines the relative importance of a resource request.
Preemption Capability	Defines whether a service data flow may get resources that were already assigned to another service data flow with a lower priority level. Possible values are: • NOT_PREEMPT • MAY_PREEMPT
Preemption Vulnerability	Defines whether a service data flow may lose the resources assigned to it in order to admit a service data flow with higher priority level. Possible values are: • NOT_PREEMPTABLE • PREEMPTABLE

6. Click **Save**.
   The QoS data gets listed on the **QoS Data** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the QoS data.

Importing QoS Data

To import QoS data:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.2.7 Traffic Profile

This section describes how to configure Traffic Profiles for PCF.

To access Traffic Profile configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and select **Traffic Profile**.

The Traffic Profile configuration includes the following:

- ADC Rule
- Predefined ADC Rule
- Predefined ADC Rule Base

7.4.2.7.1 ADC Rule

This procedure provides information about how to define and manage ADC Rules under Traffic Profiles in PCF.

The **ADC Rule** page allows you to create new and manage existing ADC Rules. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure ADC Rule:

1. From the navigation menu under **Traffic Profile**, select **ADC Rule**.
   This opens the **ADC Rule** page.
2. Click Add .
   This opens the **Create ADC Rule** page.
3. On the **Create ADC Rule** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-183 Create ADC Rule Configurations

Field Name	Description
Name	Name of the Traffic Profile.
Rule Name	Uniquely identifies the ADC rule. Used to reference an ADC rule in communication between the CNC Policy and a PCEF within one IP-CAN session.
Description	Description of the profile.
Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network). Provide a valid numerical value.
Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment). Provide a valid numerical value.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-183 (Cont.) Create ADC Rule Configurations

Field Name	Description
Monitoring Key	Monitoring key that may apply to the ADC rule.
Flow Status	Indicates whether the application traffic is enabled or disabled in either the uplink or downlink direction. Select from the following: • ENABLED_UPLINK • ENABLED_DOWNLINK • ENABLED • DISABLED
TDF Application Identifier	Identifies the traffic that belongs to the application to which the rule applies.
TDF Redirect Support	Indicates whether the application traffic should be redirected to another controlled address. Select from the following: • REDIRECTION_DISABLED • REDIRECTION_ENABLED
TDF Redirect Address Type	Specifies the format for the redirect address. Select from the following: • IPv4 • IPv6 • URL • SIP_URI
TDF Redirect Server Address	The address of the TDF redirect server in the specified address type.
Mute Notification	Notification to disable application detection notifications from the TDF device. Select **MUTE_REQUIRED** from the drop-down list. By default, mute remains disabled.
Service Identifier	Credit-control service identifier associated with the traffic defined by this rule. Only applicable if online charging is enabled. Provide a valid numerical value.
Rating Group	Credit-control rating group associated with the traffic defined by this profile. Only applicable if online charging is enabled. Provide a valid numerical value.
Reporting Level	Select from the following: • SERVICE_IDENTIFIER_LEVEL • RATING_GROUP_LEVEL
Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • DISABLE_ONLINE • ENABLE_ONLINE
Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following:: • DISABLE_OFFLINE • ENABLE_OFFLINE
Metering Method	Defines how service data-flow traffic is metered for offline charging. Select from the following: • DURATION • VOLUME • DURATION_VOLUME • EVENT

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-183 (Cont.) Create ADC Rule Configurations

Field Name	Description
Precedence	Precedence value of the profile. The lower the precedence, the higher the priority. Provide a valid numerical value.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **ADC Rule** page. Use or available in the next column to update or delete the listing.

7.4.2.7.2 Predefined ADC Rule

This procedure provides information about how to define and manage Predefined ADC Rules under Traffic Profiles in PCF.

The **Predefined ADC Rule** page allows you to create new and manage existing Predefined ADC Rules. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure Predefined ADC Rule:

1. From the navigation menu under **Traffic Profile**, select **Predefined ADC Rule**. This opens the **Predefined ADC Rule** page.
2. Click Add .

   This opens the **Create Predefined ADC Rule** page.
3. On the **Create Predefined ADC Rule** page, enter values for the available input fields. The following table describes the fields:

Table 7-184 Create Predefined ADC Rule Configurations

Field Name	Description
Name	Name of the Predefined ADC Rule.
Rule Name	Uniquely identifies the Predefined ADC Rule. Used to reference an Predefined ADC Rule in communication between the CNC Policy and a PCEF within one IP-CAN session.
Description	Description of the ADC Rule.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The value gets listed on the **Predefined ADC Rule** page. Use or available in the next column to update or delete the listing.

7.4.2.7.3 Predefined ADC Rule Base

This procedure provides information about how to define and manage Predefined ADC Rule Bases under Traffic Profiles in PCF.

The **Predefined ADC Rule Base** page allows you to create new and manage existing Predefined ADC Rule Bases. The page displays the list of defined configurations and provides the options to add, edit or delete data.

To configure Predefined ADC Rule Base:

1. From the navigation menu under Traffic Profile, select Predefined ADC Rule Base.
   This opens the **Predefined ADC Rule Base** page.
2. Click Add .
   This opens the **Create Predefined ADC Rule Base** page.
3. On the **Create Predefined ADC Rule Base** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-185 Create Predefined ADC Rule Base Configurations

Field Name	Description
Name	Name of the Predefined ADC Rule Base.
Rule-Base Name:	Uniquely identifies the Predefined ADC Rule Base. Used to reference an Predefined ADC Rule Base in communication between the CNC Policy and a PCEF within one IP-CAN session.
Description	Description of the Predefined ADC Rule Base.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Predefined ADC Rule Base** page. Use or available in the next column to update or delete the listing.

7.4.2.8 Charging Data

This procedure provides information about how to create and manage the charging data in Policy.

The **Charging Data** page allows you to create new and manage existing charging data configurations. The page displays the list of defined charging details and provides the options to import, export, or add data.

To configure charging data:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **Charging Data**.
   This opens the **Charging Data** page. The page lists the existing charging data. You can add or import new data using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Charging Data** page.
3. On the **Create Charging Data** page, enter values for the following input fields:
   :

Table 7-186 Create Charging Data Configurations

Field Name	Description
Charging id	Specifies the charging ID
Name	A unique of the Charging data
Description	Brief description of the Charging data
Metering Method	The following options are available • DURATION • VOLUME • DURATION_VOLUME • EVENT Defines. which parameters must be metered for offline charging. If the attribute is not present, but it has been supplied previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but it is set to NULL, the metering method preconfigured at the SMF is applicable as the default metering method.
Offline	Indicates that offline charging is applicable to the PDU session or PCC rule. The default value is `false`, if the attribute is not present and it has not been supplied previously.
Online	Indicates that online charging is applicable to the PDU session or PCC rule. The default value is `false`, if the attribute is not present and it has not been supplied previously.
Rating Group	The charging key for the PCC rule used for rating purposes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-186 (Cont.) Create Charging Data Configurations

Field Name	Description
Reporting Level	The following options are available: • SER_ID_LEVEL • RAT_GR_LEVEL • SPON_CON_LEVEL Defines, on which level the SMF reports the usage for the related PCC rule. If the attribute is not present but it has been provided previously, the previous information remains valid. If the attribute is not present and it has not been supplied previously or the attribute has been supplied previously but it is set to NULL, the reporting level preconfigured at the SMF is applicable as the default reporting level.
Service Id	Indicates the identifier of the service or the service component in the service data flow of a PCC rule.
Sponsor Id	Indicates the sponsor identity.
App Svc Prov Id	Indicates the application service provider identity.
Af Charging Identifier	Identifies the charging control policy data within a PDU session.
sdfHandl	`sdfHandl` attribute send to SMF to indicate whether the service data flow is allowed to start, while the SMF is waiting for the response of the credit request from CHF.

4. Click **Save**.
   The Charging data gets listed on the **Charging Data** page.

> **Note**
>
> Use ✎ or 🗑 available under the **Actions** column to update or delete the charging data.

Importing Charging Data

To import charging data:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.2.9 Traffic Control Data

This procedure provides information about how to create and manage the Traffic Control data in Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The **Traffic Control Data** page allows you to create new and manage existing traffic control configurations. The page displays the list of defined traffic control configurations and provides the options to import, export, or add data.

To configure traffic control data:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **Traffic Control Data**.
   This opens the **Traffic Control Data** page. The page lists the existing traffic control data. You can add or import new data using this page.

   > **Note**
   >
   > Click  to download the available listings in the JSON file format on your system.

2. Click  .
   This opens the **Create Traffic Control Data** page.
3. On the **Create Traffic Control Data** page, enter the information common to all the groups available on the page.
   The following table describes the common input fields:

Table 7-187 Create Traffic Control Data Common Input Fields

Field Name	Description
Traffic Control id	Specifies the traffic control policy data id
Name	The name of the Traffic Control policy data
Description	The description of the Traffic Control policy data
Flow Status	The following options are available: • ENABLED-UPLINK • ENABLED-DOWNLINK • ENABLED • DISABLED • REMOVED Enum determining what action to perform on traffic. Possible values are: [enable, disable, enable_uplink, enable_downlink] . The default value "ENABLED" is applicable, if the attribute is not present and has not been supplied previously.

4. Expand the **Redirect Information** group.
   This group allows you to add traffic redirect information.
5. Enter the values for the input fields, available under **Redirect Information** group.
   The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-188 Redirect Information

Field Name	Description
Redirect Enabled	Indicates the redirect is enabled. This is an optional field.
Redirect Address Type	This string provides forward-compatibility with future extensions to the enumeration but is not used to encode content defined in the present version of this API.
Redirect Server Address	Indicates the address of the redirect server.

> **Note**
>
> Click the **Remove** button to remove the Redirect Information details from the page.

6. Enter the values for the following input fields:

Table 7-189 Create Traffic Control Data Common Input Fields

Field Name	Description
Mute Notification	Indicates whether application's start or stop notification is to be muted. The default value "FALSE" is applicable, if the attribute is not present and has not been supplied previously.
Traffic Steering Pol Id Dl	Reference to a preconfigured traffic steering policy for downlink traffic at the SMF.
Traffic Steering Pol Id Ul	Reference to a preconfigured traffic steering policy for uplink traffic at the SMF.

7. Expand the **Route To Locs** group.
The expanded group displays the available routes and allows you to create new routes.

   To create new routes:

   a. Click ⊕ Add .
   The page opens the **Add Route to Locs** dialog box.

   b. Enter the value for the **DNAI**.
   The DNAI value identifies the location of the application.

   c. Expand the **Route Information** group.
   This group allows you to add the traffic routing information.

   d. Enter the values for the input fields, available under **Route Information** group.
   The following table describes the fields:

Table 7-190 Redirect Information

Field Name	Description
Ipv6 Addr	Ipv6 address of the tunnel end point in the data network.
Port Number	UDP port number of the tunnel end point in the data network.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-190 (Cont.) Redirect Information

Field Name	Description
Ipv4 Addr	Ipv4 address of the tunnel end point in the data network.

> **Note**
>
> Click the **Remove** button to remove the Route Information details from the dialog box.

e. Enter the value for **Route Profile Id**.
This value identifies the routing profile Id.

f. Click **Save**.
The Route Information gets listed under the **Route to Locs** group on the **Create Traffic Control Data** page.

8. On the **Create Traffic Control Data** page, expand the **Up Path Chg Event** group.

9. Enter the values for the input fields, available under **Up Path Chg Event** group.
The following table describes the fields:

Table 7-191 Up Path Chg Event

Field Name	Description
Notification Uri	Defines the notification Uri sent by the SMF.
Notification Correlation Id	It is used to set the value of Notification Correlation ID in the notification sent by the SMF.
Dnai Change Type	The following options are available: • EARLY • EARLY_LATE • LATE Possible values are EARLY: Early notification of UP path reconfiguration. - EARLY_LATE: Early and late notification of UP path reconfiguration. This value is present in the subscription to the DNAI change event. LATE: Late notification of UP path reconfiguration. This string provides forward compatibility with future extensions to the enumeration but is not used to encode content defined in the present version of this API.

> **Note**
>
> Click the **Remove** button to remove the Redirect Information details from the page.

10. On the **Create Traffic Control Data** page, click **Save**.
The traffic control data gets listed on the **Traffic Control Data** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the traffic control data configurations.

Importing Traffic Control Data

To import the traffic control data:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

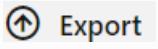
7.4.2.10 Condition Data

This procedure provides information about how to create and manage the Condition data in Policy.

The **Condition Data** page allows you to create new and manage existing conditions that can be applied for Policy services. The page displays the list of defined conditions and provides the options to import, export, or add data.

To configure condition data:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Session Management**, and then, select **Condition Data**.
   This opens the **Condition Data** page. The page lists the existing conditions. You can add or import new data using this page.

   > **Note**
   >
   > Click  to download the available listings in the JSON file format on your system.

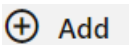
2. Click  .
   This opens the **Create Condition Data** page.
3. On the **Create Condition Data** page, enter values for the following input fields:
   :

Table 7-192 Create Condition Data Configurations

Field Name	Description
Condition id	Specifies the condition data policy data id.
Name	The name of the Condition Data policy data.
Description	The description of the Condition Data policy data.
Activation Time	The time when the decision data is activated.
Deactivation Time	The time when the decision data is deactivated.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. Click **Save**.
   The condition gets listed on the **Condition Data** page.

> **Note**
>
> Use ✎ or 🗑 available under the **Actions** column to update or delete the condition data.

Importing Condition Data

To import condition data:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.3 PCF Access and Mobility

This section includes the configurations for PCF Access and Mobility service.

To access PCF Access and Mobility configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations** and select **PCF Access and Mobility**.

The PCF Access and Mobility configuration includes Managing Service Area Restriction.

7.4.3.1 Service Area Restriction

This procedure provides information about how to create and manage the Service Area Restriction (SAR) in Policy.

The **Service Area Restriction** page allows you to create new and manage existing restrictions. The page displays the list of defined rules and provides the options to import, export, or add data.

To configure service area restrictions:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF Access and Mobility**, and then, select **Service Area Restriction**.
   This opens the **Service Area Restriction** page. The page lists the details of existing service area restrictions including their name and restriction type in a tabular format. You can add or import new data using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Service Area Restriction** page.
3. On the **Create Service Area Restriction** page, enter the information common to all the groups available on the page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The following table describes the common input fields:

Table 7-193 Create Service Area Restriction Configurations

Field Name	Description
Name	Use this field to add a customized name for service area restriction.
Description	Use this field to add a customized description for service area restriction.
Restriction Type	Use this field to specify the restriction type. Possible values are: • ALLOWED_AREAS • NOT_ALLOWED_AREAS **Note:** Set a restriction type for service area restriction only when **Areas** attribute is available.

4. Expand the **Areas** group.
   This group lists the existing area details and allows you to configure new areas.
5. To add new areas:
   a. Click Add .
      The page opens the **Add Areas** dialog box.
   b. Enter the value for the following fields:

      Table 7-194 Add Areas Configurations

Field Name	Description
Tacs	The value for Type Allocation Codes (Tacs) can be defined as a hexa decimal number between 0 and 65535.
Area Codes	Enter the value of area codes.

   c. Click **Save**.
      The areas gets listed under the **Areas** group on the **Create Service Area Restriction** page.
6. Enter value for the **Max Number of TAs** field.
7. Click **Save**.
   The SAR data gets listed on the **Service Area Restriction** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the SAR data.

Importing Service Area Restrictions

To import the Service Area Restrictions:

1. Click Import .
   The page opens the **File Upload** dialog box.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.4 PCF UE Policy

This section includes the configurations for PCF UE Policy service.

To access PCF UE Policy configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations** and select **PCF UE Policy**.

The PCF UE Policy configurations includes:

- URSP Rule
- UPSI Rule

7.4.4.1 URSP Rule

This procedure provides information about how to create and manage the UE Route Selection Policy (URSP) Rules in Policy.

The **URSP Rule** page allows you to create new and manage existing rules. The page displays the list of defined URSP rule configurations and provides the options to import, export, or add rules.

To configure URSP Rules:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF UE Policy**, and then, select **URSP Rule**.
   This opens the **URSP Rule** page. The page lists the existing URSP rules data. You can add or import new rules using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create URSP Rule** page.
3. On the **Create URSP Rule** page, enter the information common to all the groups available on the page.
   The following table describes the common input fields:

Table 7-195 Create URSP Rule Configurations

Field Name	Description
Name	Name of the URSP rule. **Note:** Name can not be the sub string of any other configured URSP rule Name.
Precedence	Precedence value of the URSP rule. **Note:** The value of *precedence* must be unique. If we attempt to import a record with a duplicate *precedence*, it will result in an error stating that the value already exists in the database.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**

4. Expand the **Traffic Descriptor** group.
   The expanded group allows you to create new descriptors.

   To create new traffic descriptors:

   a. Click Add .
      The page opens the **Add Traffic Descriptor** dialog box.

   b. Select a value from the **Type** drop-down list and then, enter corresponding values, if applicable. The following table lists the traffic descriptor types and their corresponding values:

Table 7-196 Traffic Descriptor Type and Values

Traffic Descriptor Type	Value
MATCH_ALL	NA
OS_ID_OS_APP_ID	• OS ID • OS APP ID
IPV4_REMOTE_ADDRESS	• IPv4 Address • Subnet Mask
IPV6_REMOTE_ADDRESS	• IPv6 Address • IPv6 Prefix Length
PROTOCOL_IDENTIFIER	Protocol Number
SINGLE_REMOTE_PORT	Remote Port
REMOTE_PORT_RANGE	• Start Port • End Port
SECURITY_PARAMETER_INDEX	IPSec Security Parameter Index
TYPE_OF_SERVICE_CLASS	• Type of Service • Mask
FLOW_LABEL	IPv6 Flow Label
DESTINATION_MAC_ADDRESS	MAC Address
T_802_1Q_C_TAG_VID	Customer VLAN ID
T_802_1Q_S_TAG_VID	Service VLAN ID
T_802_1Q_C_TAG_PCP_DEI	• Priority Code Point (PCP) • Drop Eligible Indicator (DEI)
T_802_1Q_S_TAG_PCP_DEI	• Priority Code Point (PCP) • Drop Eligible Indicator (DEI)
ETHERTYPE	Ether type
DNN	DNN
CONNECTION_CAPABILITIES	Connection Capabilities
DESTINATION_FQDN	FQDN
OS_APP_ID	OS APP ID

   c. Click **Save**.
      The Route Information gets listed under the **Traffic Descriptor** group on the **Create URSP Rule** page.

Traffic Descriptors List Constraints

Copyright © 2019, 2026, Oracle and/or its affiliates.

- The *Traffic Descriptors List* must not be null or empty.
- If the list includes a MATCH_ALL descriptor, it should not contain any other descriptors.

5. Expand the **Route Selection Descriptor List** group.
   The expanded group allows you to create new descriptors.

   To create new route selection descriptors:

   a. Click ⊕ Add .
      The page opens the **Add Route Selection Descriptor List** dialog box.
   b. Enter the value in the **Precedence** field.
   c. Expand **Route Selection Descriptor Components** group.
      The expanded group allows you to create new descriptors components.
   d. To add new components:

      i. Click ⊕ Add .
         The page opens the **Add Route Selection Descriptor Components** dialog box.
      ii. Select a value from the **Type** drop-down list and then, enter corresponding values, if applicable. The following table lists the route selection descriptor component types and their corresponding values:

Table 7-197 Route Selection Descriptor Components Configurations

Type	Value
SSC_MODE	Select any of the following values for SSC Mode: • SSC Mode 1 • SSC Mode 2 • SSC Mode 3
SNSSAI	Enter the values for the following fields: • SST • SD Accepts a string value of 6 characters containing either numbers from 0 to 9, alphabets from a to f, or A to F. • Mapped SST • Mapped SD Accepts a string value of 6 characters containing either numbers from 0 to 9, alphabets from a to f, or A to F.
DNN	Enter the value of DNN in the provided field.
PDU_SESSION_TYPE	Select any of the following values for PDU Session Type: • IPV4 • IPV6 • IPV4V6 • Unstructured • Ethernet
PREFERRED_ACCESS_TYPE	Select any of the following values for Preferred Access Type: • 3GPP Access • Non 3GPP Access

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-197 (Cont.) Route Selection Descriptor Components Configurations

Type	Value
NON_SEAMLESS_NON_3GPP_OFFLOAD_INDICATION	NA

iii. Click **Save** on the **Add Route Selection Descriptor Components** dialog box.

e. Click **Save** on the on the **Add Route Selection Descriptor Lists** dialog box.

Route Selection Descriptor List Constraints:

- If the list contains a NON_SEAMLESS_NON_3GPP_OFFLOAD_INDICATION descriptor, it must be sole descriptor in the list.
- The following descriptors are not allowed to appear more than once in the list:
  - SSC_MODE
  - PDU_SESSION_TYPE
  - PREFERRED_ACCESS_TYPE
- The following descriptors are allowed to appear multiple times, but each occurrence must have a unique value:
  - SNSSAI
  - DNN

6. On the **Create URSP Rule** page, click **Save**.
   The URSP rule data gets listed on the **URSP Rule** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the URSP rule configurations.

Importing URSP Rule

To import the URSP rules:

1. Click 

   .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.4.2 UPSI

This procedure provides information about how to create and manage the UE Policy Section Identifier (UPSI) in Policy.

The **UPSI** page allows you to create new and manage existing UPSI configurations. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure UPSI:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCF UE Policy**, and then, select **UPSI**.
   This opens the **UPSI** page. The page lists the existing UPSI data. You can add or import new data using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create UPSI** page.
3. On the **Create UPSI** page, enter values for the input fields common to all the groups available on the page.
   The following table describes the fields:

Table 7-198 Create UPSI Configurations

Field Name	Description
Name	Name of the UPSI.
UPSC	Defines UE Policy Section Code. Enter a number between 0 and 65,535.
URSP Rules	Defines URSP rules.

> **Note**
>
> Name can not be the substring of any other configured URSP rule Name.

4. Expand the **PLMN** group.
   This group allows you to add PLMN information.

   The following table describes the fields:

Table 7-199 PLMN Configurations

Field Name	Description
MCC	Defines the Mobile Country Code. Enter a number between 0 and 999.
MNC	Defines the Mobile Network Code. Enter a number between 0 and 999.

5. Click **Save**.
   The UPSI data gets listed on the **UPSI** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the session UPSI configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Importing UPSI

To import UPSIs:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5 PCRF Core

This section includes the configurations for PCRF Core.

To access PCRF Core configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations** and select **PCRF Core**.

The PCRF Core configuration includes the following:

- Charging Server
- Media Profile
- Presence Reporting Area
- Time Periods
- Retry Profile
- Traffic Profile

7.4.5.1 Charging Server

This procedure provides information about how to define and manage charging servers within the PCRF Core in Policy. A charging server is an application that calculates billing charges.

The **Charging Server** page allows you to create new and manage existing charging server configurations. The page displays the list of defined configurations and provides the options to import, export, or add data.

To define a charging server:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCRF Core**, and then, select **Charging Server**.

   This opens the **Charging Server** page. The page lists the existing charging server data. You can add or import new data using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create Charging Server** page.

3. On the **Create Charging Server** page, enter the following information in the available input fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-200 Create Charging Server Configurations

Field Name	Description
Name	The unique name you assign to the charging server. This is a mandatory field. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_).
Description/Location	Free-form text that identifies the charging server within the network. Enter up to 250 characters.
Host Name	The FQDN (fully qualified domain name assigned) to the charging server. This is a mandatory field.
Port	The port number on which the charging server is listening for messages. The default value is 3868.
Transport	Select the transport protocol used to communicate with the charging server. The available options include: • **tcp** Transmission Control Protocol (used with TACACS+) • **udp** User Datagram Protocol (used with RADIUS) **Note:** If you configure the Transport protocol as **udp**, you cannot configure the AAA Protocol as **diameter**.
Protocol	Select the Authentication, Authorization, and Accounting (AAA) Protocol used to communicate with the charging server. The available options include: • **diameter** • **radius** **Note:** If you configure the Transport protocol as **udp**, you can not configure the AAA Protocol as **diameter**. Moreover, you can not set both **Transport** and **Protocol** fields as null.
Security	Select if the transport security is used to communicate with the charging server. By default, the slider option remains unselected.

4. Click **Save**.

   The charging server gets listed on the **Charging Server** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the charging server configurations.

Importing Charging Server

To import charging server:

5. Click  .

   The page opens the **File Upload** dialog box.

6. Upload the file in JSON format by using the **Drag and Drop** button.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7. Click **Import**.

7.4.5.2 Media Profile

This procedure provides information about how to define and manage media profiles under PCRF Core in Policy. A media profile describes a CODEC supported for Rx-to-PCMM translation in a cable network.

> **Note**
>
> Media Profiles is a function that is applicable to Cable mode only.

The **Media Profile** page allows you to create new and manage existing media profile configurations. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure media profile:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCRF Core**, and then, select **Media Profile**.

   This opens the **Media Profile** page. The page lists the existing profiles. You can add or import new profiles using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create Media Profile** page.

3. On the **Create Media Profile** page, enter the following information in the available input fields:

Table 7-201 Create Media Profile Configurations

Field Name	Description
ID	The unique ID assigned to the media profile. This is a mandatory field.
Name	Unique name assigned to the media profile. This is a mandatory field.
Description	Brief description of the media profile.
Codec Name	Unique media subtype assigned to the media profile. This is defined in the IANA MIME registration for the CODEC. Enter a string of up to 255 characters. This is a mandatory field.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-201 (Cont.) Create Media Profile Configurations

Field Name	Description
Transport Type	Transport type. Select any of the following values from the drop-down list: • **RTP/AVP** (default) — RTP audio-video profile. • **RTP/SAVP** — RTP secure audio-video profile. • **RTP/AVPF** — RTP extended audio-video profile with feedback.
Payload Number	The payload number. Valid payload numbers range from 97 through 127. Enter -1 to indicate an unknown payload number. **Note:** You cannot add a CODEC that is predefined with a payload number in the range of 0 to 96. This is a mandatory field.
Sample Rate (kHz)	The sampling rate of the CODEC in KHz. The valid range is an integer from 1 through 100 KHz. This is a mandatory field.
Frame Size in Milliseconds	The size of one audio frame in milliseconds. This is the length of time represented by one audio frame. A single RTP packet may contain multiple audio frames. The bitrate is calculated using the frame size in milliseconds, the frame size in bytes, and the packetization time. The valid range is 0 through 100 ms. This is a mandatory field.
Frame Size in Bytes	The size of one audio frame size in bytes. This is the size represented by one audio frame. A single RTP packet may contain multiple audio frames. The bitrate is calculated using the frame size in milliseconds, the frame size in bytes, and the packetization time. The valid range is 1 through 1,500 bytes. This is a mandatory field.
Packetization Time	The length of time, in milliseconds, represented by the media in a packet. The bitrate is calculated using the frame size in milliseconds, the frame size in bytes, and the packetization time. The valid range is 1 through 100. This is a mandatory field.
Always Use Default Ptime	Select to always use the default packetization time, ignoring the value received in the SDP message. By default the slider option remains unselected. This is a mandatory field.

Importing Media Profile

To import media profile:

4. Click Import .

   The page opens the **File Upload** dialog box.
5. Upload the file in JSON format by using the **Drag and Drop** button.
6. Click **Import**.
7. Click **Save**.

   The media profile gets listed on the **Media Profile** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the profiles.

7.4.5.3 Presence Reporting Area

This procedure provides information about how to define and manage Presence Reporting Area (PRA) under PCRF Core in Policy.

The **Presence Reporting Area** page allows you to create new and manage existing PRA configurations. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure PCRF PRA:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCRF Core**, and then, select **Presence Reporting Area**.
   This opens the **Presence Reporting Area** page. The page lists the existing PRAs. You can add or import new PRAs using this page.

   > **Note**
   >
   > Click  to download the available listings in the JSON file format on your system.

2. Click  .
   This opens the **Create Presence Reporting Area** page.
3. On the **Create Presence Reporting Area** page, enter values for the input fields common to all the groups available on the page.
   The following table describes the fields:

Table 7-202 Create Presence Reporting Area Configurations

Field Name	Description
ID	The unique identifying number of the PRA list. The ID must be a number between 0 and 16777125. This field is present if the Area of Interest subscribed or reported is a Presence Reporting Area.
Name	The unique name assigned to the PRA.
Description	Description of the PRA.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-202 (Cont.) Create Presence Reporting Area Configurations

Field Name	Description
Type	This is a mandatory field. Select the PRA type from the drop-down list. The available options are: • predefined: Select this to create a core network pre-configured PRA. If the **predefined** is selected, then the option to add PRA items must be disabled, as adding PRA items under this type is not recommended. • ue_dedicated: Select this to create a ue dedicated PRA. If the **ue_dedicated** is selected, then the user must be able to add PRA items.

4. Expand the **PRA Items** group.
   The expanded group allows you to add PRA items.
5. To add new items:
   a. Click Add .
      The page opens the **Add PRA Items** dialog box.
   b. Select a value from the **Type** drop-down list and then, enter corresponding values. The available options with value combination are:
      - **TAI**: Tracking Area Identity (MCC,MNC,TAC)
      - **RAI**: Routing Area Identity (MCC,MNC,LAC,RAC)
      - **Macro eNodeB**: (MCC,MNC,MENB)
      - **Home eNodeB**: (MCC,MNC,HENB)
      - **ECGI**: E-UTRAN Cell Global Identifier (MCC,MNC,ECI)
      - **SAI**: Service Area Identity (MCC,MNC,LAC,SAC)
      - **CGI:** Cell Global Identity (MCC,MNC,LAC,CI)

      The input fields differ for each **Type**, based on the components applicable for that PRA item type. The following table describes each field:

Table 7-203 PRA Items Components Based on Type

Field Name	Description
MNC *Applicable for All*	Defines the Mobile Network Code. It can be a 2- or 3-digit number.
MCC *Applicable for All*	Defines the Mobile Country Code. It should be a 3-digit number.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-203 (Cont.) PRA Items Components Based on Type

Field Name	Description
TAC *Applicable for All*	28-bit string identifying an E-UTRAN Cell Id as specified, in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents 4 bits. The most significant character representing the 4 most significant bits of the Cell Id appears first in the string, and the character representing the 4 least significant bit of the Cell Id appears last in the string. Pattern: '^[A-Fa-f0-9]{7}$' Example: An E-UTRAN Cell Id 0x5BD6007 is encoded as "5BD6007".
LAC *Applicable for Type: RAI/SAI/CGI*	16-bit number that forms part of the Local Area Identifier (LAI) which includes the Mobile Country Code (MCC0 the Mobile Network Code (MNC) and the Local area code. Pattern: A decimal number between 0 and 65535.
RAC *Applicable for Type: RAI*	The routing area code for calling and differing of various RAs. Pattern: A decimal number between 0 and 65535.
MENB *Applicable for Type: Macro eNodeB*	Master eNodeB. Pattern: A decimal number between 0 and 268435455.
HENB *Applicable for Type: Macro eNodeB*	Home eNodeB Pattern: A decimal number between 0 and 268435455.
ECI *Applicable for Type: ECGI*	E-UTRAN Cell Identifier Pattern: A decimal number between 0 and 268435455.
SAC *Applicable for Type: SAI*	Service area code Pattern: A decimal number between 0 and 65535.
CI *Applicable for Type: CGI*	Cell identification Pattern: A decimal number between 0 and 65535.

c. Click **Save** on the on the **Add PRA Items** dialog box.

6. On the **Create Presence Reporting Area** page, click **Save**.
The PRA gets listed on the **Presence Reporting Area** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the PRA configurations.

Importing Presence Reporting Area

To import PRA:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.4 Time Periods

This procedure provides information about how to define and manage Time Periods under PCRF Core in Policy.

The **Time Periods** page allows you to view, create, and configure time periods. You can define a library of time periods to specify in policy time-of-day conditions and associate the time periods with multiple policies. Each time period can have one or more times slots defined. A time slot can be:

- Specific time of day
- Different days of the week
- Different days of a month
- Specific years
- Specific day and time in a specific year
- Specific day and time in every year

For example a single time period can have following time slots defined:

- Every Monday at 2 o'clock
- On the last day of the month
- On every Valentines day
- On May 17, 2016
- The first three days of March, July, and September

To configure time period:

1. From the navigation menu under **Policy**, navigate to **Policy Data Configurations**, click **PCRF Core**, and then, select **Time Periods**.
   This opens the **Time Periods** page. The page lists the existing time periods. You can add or import new periods using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Time Period** page.
3. On the **Create Time Period** page, enter values for the input fields common to all the groups available on the page.
   The following table describes the fields:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-204 Create Time Periods Configurations

Field Name	Description
Name	Name of the time period. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_).
Description	A descriptive phrase.
Precedence	A positive integer. The lower the number, the higher the precedence. If time periods overlap, the time period with the highest precedence (lowest number) applies.

4. Expand the **Time Slot** group.
   The expanded group allows you to add time slots.
5. To add time slots:
   a. Click Add .
      The page opens the **Add Time Slot** dialog box.
   b. Enter the values for the following input fields:

Table 7-205 Add Time Slot Configurations

Field Name	Description
Years	Number of years.
Months of year	Number of months of the year.
Days of Month	Days of the month.
Days of Week	Days of the week.
Start Time	Starting time.
End Time	End time.

> **Note**
>
> The fields in the time slot configuration must have certain value. It must not be left empty.

   c. Click **Save** on the **Add Time Slot** dialog box.
6. On the **Create Time Period** page, click **Save**.
   The time period gets listed on the **Time Period** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the time period configurations.

Importing Time Periods

To import time periods:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.5 Retry Profile

This section describes how to configure Retry Profiles for PCRF Core.

To access Retry Profile configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations**, click **PCRF Core**, and select **Retry Profile**.

The Retry Profile configuration includes the following:

- PCC Retry Profile
- ADC Retry Profile

7.4.5.5.1 PCC Retry Profile

This procedure provides information about how to define and manage PCC Retry Profile under PCRF Core in CNC Policy.

The **PCC Retry Profile** page allows you to create new and manage existing profiles. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure PCC Retry Profile:

1. From the navigation menu under **Retry Profile**, select **PCC Retry Profile**.
   This opens the **PCC Retry Profile** page. The page lists the existing PCC Retry Profiles. You can add or import new profiles using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create PCC Retry Profile** page.
3. On the **Create PCC Retry Profile** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-206 Create PCC Retry Profile Configurations

Field Name	Description
Name	Enter the Name for the profile. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Description	Enter the Description/Location. Free-form text describing the profile.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-206 (Cont.) Create PCC Retry Profile Configurations

Field Name	Description
Maximum Retry Attempt (per Retry Cycle)	The maximum number of retry attempts during a retry cycle in the range from 1 to 10. The default is 5.
Initial Retry Interval	Enter the Initial Retry Interval. The length of time to wait, in seconds, after a reported failure or the end of the Back Off Interval before retrying. Enter a value from 0 to 30 seconds. The default is 10 seconds.
Maximum Retry Interval	Enter the Maximum Retry Interval. The maximum wait, in seconds, after a reported failure or the end of the Back Off Interval before retrying during a retry cycle. Enter a value from 1 to 180 seconds. The default is 60 seconds.
Back Off Interval	Enter the Back Off Interval. The interval from 1 to 86400 seconds between successive retry cycles. The default is 300 seconds.
Maximum Retry Cycles	Enter the Maximum Retry Cycles. The number of retry cycles ranging from 1 to 4. The default value is 1 cycle.
Rule Failure Code	Rule Failure Code The upper box lists available rule failure codes. The lower box lists rule failure codes installed in the profile.

4. Click **Save**.
   The PCC Retry Profile gets listed on the **PCC Retry Profile** page.

> **Note**
>
> Use ✎ or 🗑 available under the **Actions** column to update or delete the PCC Retry Profile.

Importing PCC Retry Profile

To import PCC Retry Profile:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.5.2 ADC Retry Profile

This procedure provides information about how to define and manage ADC Retry Profile under PCRF Core in CNC Policy.

The **ADC Retry Profile** page allows you to create new and manage existing profiles. The page displays the list of defined configurations and provides the options to import, export, or add data.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure ADC Retry Profile:

1. From the navigation menu under **Retry Profile**, select **ADC Retry Profile**.
   This opens the **ADC Retry Profile** page. The page lists the existing ADC Retry Profiles. You can add or import new profiles using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create ADC Retry Profile** page.
3. On the **Create ADC Retry Profile** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-207 Create ADC Retry Profile Configurations

Field Name	Description
Name	Enter the Name for the profile. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
Description	Enter the Description/Location. Free-form text describing the profile.
Maximum Retry Attempt (per Retry Cycle)	The maximum number of retry attempts during a retry cycle in the range from 1 to 10. The default is 5.
Initial Retry Interval	Enter the Initial Retry Interval. The length of time to wait, in seconds, after a reported failure or the end of the Back Off Interval before retrying. Enter a value from 0 to 30 seconds. The default is 10 seconds.
Maximum Retry Interval	Enter the Maximum Retry Interval. The maximum wait, in seconds, after a reported failure or the end of the Back Off Interval before retrying during a retry cycle. Enter a value from 1 to 180 seconds. The default is 60 seconds.
Back Off Interval	Enter the Back Off Interval. The interval from 1 to 86400 seconds between successive retry cycles. The default is 300 seconds.
Maximum Retry Cycles	Enter the Maximum Retry Cycles. The number of retry cycles ranging from 1 to 4. The default value is 1 cycle.
Rule Failure Code	Rule Failure Code The upper box lists available rule failure codes. The lower box lists rule failure codes installed in the profile.

4. Click **Save**.
   The ADC Retry Profile gets listed on the **ADC Retry Profile** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the ADC Retry Profile.

Importing ADC Retry Profile

To import ADC Retry Profile:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.6 Traffic Profile

This section describes how to configure Traffic Profiles for PCRF Core.

To access Retry Profile configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations**, click **PCRF Core**, and select **Traffic Profile**.

The Traffic Profile configuration includes the following:

- ADC Rule
- Diameter QoS
- PCC Profile
- PCC Rule
- Predefined ADC Rule
- Predefined ADC Rule Base
- Predefined PCC Rule
- Predefined PCC Rule Base

7.4.5.6.1 ADC Rule

This procedure provides information about how to define and manage ADC Rules under Traffic Profiles in PCRF Core.

The **ADC Rule** page allows you to create new and manage existing ADC Rules. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure ADC Rule:

1. From the navigation menu under **Traffic Profile**, select **ADC Rule**.
   This opens the **ADC Rule** page. The page lists the existing ADC Rules. You can add or import new data using this page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create ADC Rule** page.

3. On the **Create ADC Rule** page, enter values for the available input fields. The following table describes the fields:

Table 7-208 Create ADC Rule Configurations

Field Name	Description
Name	Name of the Profile.
Rule Name	Uniquely identifies the ADC rule. Used to reference an ADC rule in communication between the CNC Policy and a PCEF within one IP-CAN session.
Description	Description of the profile.
Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network).
Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment).
Monitoring Key	Monitoring key that may apply to the ADC rule.
Flow Status	Indicates whether the application traffic is enabled or disabled in either the uplink or downlink direction. Select from the following: • ENABLED_UPLINK • ENABLED_DOWNLINK • ENABLED • DISABLED
TDF Application Identifier	Identifies the traffic that belongs to the application to which the rule applies.
TDF Redirect Support	Indicates whether the application traffic should be redirected to another controlled address. Select from the following: • REDIRECTION_DISABLED • REDIRECTION_ENABLED
TDF Redirect Address Type	Specifies the format for the redirect address. Select from the following: • IPv4 • IPv6 • URL • SIP_URI
TDF Redirect Server Address	The address of the TDF redirect server in the specified address type.
Mute Notification	Notification to disable application detection notifications from the TDF device. Select **MUTE_REQUIRED** from the drop-down list. By default, mute remains disabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-208 (Cont.) Create ADC Rule Configurations

Field Name	Description
Service Identifier	Credit-control service identifier associated with the traffic defined by this rule. Only applicable if online charging is enabled.
Rating Group	Credit-control rating group associated with the traffic defined by this profile. Only applicable if online charging is enabled.
Reporting Level	Select from the following: • SERVICE_IDENTIFIER_LEVEL • RATING_GROUP_LEVEL
Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • DISABLE_ONLINE • ENABLE_ONLINE
Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following:: • DISABLE_OFFLINE • ENABLE_OFFLINE
Metering Method	Defines how service data-flow traffic is metered for offline charging. Select from the following: • DURATION • VOLUME • DURATION_VOLUME • EVENT
Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **ADC Rule** page. Use or available in the next column to update or delete the listing.

Importing ADC Rule

To import ADC Rule:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.6.2 Diameter QoS

This procedure provides information about how to define and manage Diameter QoSs under Traffic Profiles in PCRF Core.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The **Diameter QoS** page allows you to create new and manage existing Diameter QoSs. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure Diameter QoS:

1. From the navigation menu under **Traffic Profile**, select **Diameter QoS**.
   This opens the **Diameter QoS** page. The page lists the existing Diameter QoSs. You can add or import new data using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create Diameter QoS** page.

3. On the **Create Diameter QoS** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-209 Create Diameter QoS Configurations

Field Name	Description
Name	Name of the Profile.
Description	Description of the profile.
QoS Class Identifier (1-254)	Identifies the QoS class. Enter a value between 1 and 254 or select from the following: • 1 = Conversational speech • 2 = Conversational • 3 = Streaming speech • 4 = Streaming • 5 = Interactive with priority 1 signaling • 6 = Interactive with priority 1 • 7 = Interactive with priority 2 • 8 = Interactive with priority 3 • 9 = Background • 65 = MC-PTT Voice • 66 = PTT Voice • 69 = MC-PTT Signaling • 70 = MC Data **Note:** QCI values between 1 and 254 are supported. Values other than 1 through 9, 65, 66, 69, and 70 are undefined.
Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network).
Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment).
Uplink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for uplinks (user equipment to network). Only applicable if the QoS class identifier is between 1 and 4.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-209 (Cont.) Create Diameter QoS Configurations

Field Name	Description
Downlink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for downlinks (network to user equipment). Only applicable if the QoS class identifier is between 1 and 4.
ARP Priority Level	Allocation and Retention Priority level of the service flows associated with this profile. Highest: 1 Lowest: 15
ARP Preemption Capability	Enable or disable the ARP Preemption Capability. Select from the following: • PREEMPTION_CAPABILITY_ENABLED • PREEMPTION_CAPABILITY_DISABLED
ARP Preemption Vulnerability	Enable or disable the ARP Preemption Vulnerability. Select from the following: • PREEMPTION_VULNERABILITY_ENABLED • PREEMPTION_VULNERABILITY_DISABLED
Resource Allocation Notification	Resource Allocation Notification Indicates that the allocation of resources for the related Diameter QoSs are confirmed. Select **ENABLE_NOTIFICATION** to enable.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Diameter QoS** page. Use  or  available in the next column to update or delete the listing.

Importing Diameter QoS

To import Diameter QoS:

1. Click 

.
The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.6.3 PCC Profile

This procedure provides information about how to define and manage PCC Profiles under Traffic Profiles in PCRF Core.

The **PCC Profile** page allows you to create new and manage existing PCC Profiles. The page displays the list of defined configurations and provides the options to import, export, or add data.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure PCC Profile:

1. From the navigation menu under **Traffic Profile**, select **PCC Profile**.
   This opens the **PCC Profile** page. The page lists the existing PCC Profiles. You can add or import new data using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create PCC Profile** page.

3. On the **Create PCC Profile** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-210 Create PCC Profile Configurations

Field Name	Description
Name	Name of the Profile.
Description	Description of the profile.
QoS Class Identifier (1-254)	Identifies the QoS class. Enter a value between 1 and 254 or select from the following: • 1 = Conversational speech • 2 = Conversational • 3 = Streaming speech • 4 = Streaming • 5 = Interactive with priority 1 signalling • 6 = Interactive with priority 1 • 7 = Interactive with priority 2 • 8 = Interactive with priority 3 • 9 = Background • 65 = MC-PTT Voice • 66 = PTT Voice • 69 = MC-PTT Signaling • 70 = MC Data **Note:** QCI values between 1 and 254 are supported. Values other than 1 through 9, 65, 66, 69, and 70 are undefined.
Bearer Usage	Indicates the Bearer usage. The default value is not applicable for this field. Users can select GENERAL or IMS_SIGNALLING from the drop down list as per the requirement.
Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network).
Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment).
Uplink Min Guranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for uplinks (user equipment to network).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-210 (Cont.) Create PCC Profile Configurations

Field Name	Description
Downlink Min Guranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for downlinks (network to user equipment).
ARP Priority Level	Allocation and Retention Priority level of the service flows associated with this profile. Highest: 1 Lowest: 15
ARP Preemption Capability	Enable or disable the ARP Preemption Capability. Select from the following: • PREEMPTION_CAPABILITY_ENABLED • PREEMPTION_CAPABILITY_DISABLED
ARP Preemption Vulnerability	Enable or disable the ARP Preemption Vulnerability. Select from the following: • PREEMPTION_VULNERABILITY_ENABLED • PREEMPTION_VULNERABILITY_DISABLED
Service Identifier	Credit-control service identifier associated with the traffic defined by this rule. Only applicable if online charging is enabled.
Rating Group	Credit-control rating group associated with the traffic defined by this profile. Only applicable if online charging is enabled.
Monitoring Key	Monitoring key that may apply to the PCC Rule.
Reporting Level	The reporting level. Select from the following: • SERVICE_IDENTIFIER_LEVEL • RATING_GROUP_LEVEL • SPONSORED_CONNECTIVITY_LEVEL
Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • DISABLE_ONLINE • ENABLE_ONLINE
Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following:: • DISABLE_OFFLINE • ENABLE_OFFLINE
Metering Method	Defines how service data-flow traffic is metered for offline charging. Select from the following: • DURATION • VOLUME • DURATION_VOLUME • EVENT
Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.
Flow Status	Indicates whether the application traffic is enabled or disabled in either the uplink or downlink direction. Select from the following: • ENABLED_UPLINK • ENABLED_DOWNLINK • ENABLED • DISABLED

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-210 (Cont.) Create PCC Profile Configurations

Field Name	Description
Resource Allocation Notification	Resource Allocation Notification Indicates that the allocation of resources for the related PCC rules are confirmed. Select **ENABLE_NOTIFICATION** to enable.
Required Access Info	Select from the following: • USER_LOCATION — the subscriber's location • MS_TIME_ZONE — the mobile subscriber's time zone • USER_LOCATION and MS_TIME_ZONE — the (mobile) subscriber's location and time zone If this field is not set, the device uses the values sent in AF requests; otherwise, it uses the values set here.
TDF Application Identifier	Identifies the traffic that belongs to the application to which the rule applies.
TDF Redirect Support	Indicates whether the application traffic should be redirected to another controlled address. Select from the following: • REDIRECTION_DISABLED • REDIRECTION_ENABLED
TDF Redirect Address Type	Specifies the format for the redirect address. Select from the following: • IPv4 • IPv6 • URL • SIP_URI
TDF Redirect Server Address	The address of the TDF redirect server in the specified address type.
Mute Notification	Notification to disable application detection notifications from the TDF device. Select **MUTE_REQUIRED** from the drop-down list. By default, mute remains disabled.
Sponsor Identity	Name identifying a connectivity sponsor.
Application Service Provider Identity	Name identifying an application service provider.
Flow Descriptions(s)	IP flows associated with this profile. A comma-separated list of Diameter IP Filter rules following the format specified in RFC 3588 section 4.3. Used in the following cases: • An old traffic profile is imported, and the flow description is not an empty string. • An upgrade from an older version is in process and the existing traffic profile flow description is not an empty string.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The value gets listed on the **PCC Profile** page. Use or available in the next column to update or delete the listing.

Importing PCC Profile

To import PCC Profile:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.6.4 PCC Rule

This procedure provides information about how to define and manage PCC Rules under Traffic Profiles in PCRF Core.

The **PCC Rule** page allows you to create new and manage existing PCC Rules. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure PCC Rule:

1. From the navigation menu under **Traffic Profile**, select **PCC Rule**.
   This opens the **PCC Rule** page. The page lists the existing PCC Rules. You can add or import new data using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create PCC Rule** page.
3. On the **Create PCC Rule** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-211 Create PCC Rule Configurations

Field Name	Description
Name	Name of the Profile.
Rule Name	Uniquely identifies the PCC Rule. Used to reference an PCC Rule in communication between the CNC Policy and a PCEF within one IP-CAN session. **Note**: The ***Name*** and the ***Rule Name*** fields must have the same values. It helps in proper installation of PCC rules.
Description	Description of the profile.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-211 (Cont.) Create PCC Rule Configurations

Field Name	Description
QoS Class Identifier (1-254)	Identifies the QoS class. Enter a value between 1 and 254 or select from the following: • 1 = Conversational speech • 2 = Conversational • 3 = Streaming speech • 4 = Streaming • 5 = Interactive with priority 1 signaling • 6 = Interactive with priority 1 • 7 = Interactive with priority 2 • 8 = Interactive with priority 3 • 9 = Background • 65 = MC-PTT Voice • 66 = PTT Voice • 69 = MC-PTT Signaling • 70 = MC Data **Note:** QCI values between 1 and 254 are supported. Values other than 1 through 9, 65, 66, 69, and 70 are undefined.
Bearer Usage	Indicates the Bearer usage. The default value is not applicable for this field. Users can select GENERAL or IMS_SIGNALLING from the drop down list as per the requirement.
Uplink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for uplinks (user equipment to network).
Downlink Max Authorized Rate (bps)	Maximum authorized bandwidth in bits per second for downlinks (network to user equipment).
Uplink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for uplinks (user equipment to network). Only applicable if the QoS class identifier is between 1 and 4.
Downlink Min Guaranteed Rate (bps)	Minimum guaranteed bandwidth in bits per second for downlinks (network to user equipment). Only applicable if the QoS class identifier is between 1 and 4.
ARP Priority Level	Allocation and Retention Priority level of the service flows associated with this profile. Highest: 1 Lowest: 15
ARP Preemption Capability	Enable or disable the ARP Preemption Capability. Select from the following: • PREEMPTION_CAPABILITY_ENABLED • PREEMPTION_CAPABILITY_DISABLED
ARP Preemption Vulnerability	Enable or disable the ARP Preemption Vulnerability. Select from the following: • PREEMPTION_VULNERABILITY_ENABLED • PREEMPTION_VULNERABILITY_DISABLED
Service Identifier	Credit-control service identifier associated with the traffic defined by this rule. Only applicable if online charging is enabled.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-211 (Cont.) Create PCC Rule Configurations

Field Name	Description
Rating Group	Credit-control rating group associated with the traffic defined by this profile. Only applicable if online charging is enabled.
Reporting Level	The reporting level. Select from the following: • SERVICE_IDENTIFIER_LEVEL • RATING_GROUP_LEVEL • SPONSORED_CONNECTIVITY_LEVEL
Online Charging	Specifies whether or not online charging is enabled in this profile. Select from the following: • DISABLE_ONLINE • ENABLE_ONLINE
Offline Charging	Specifies whether or not offline charging is enabled in this profile. Select from the following:: • DISABLE_OFFLINE • ENABLE_OFFLINE
Metering Method	Defines how service data-flow traffic is metered for offline charging. Select from the following: • DURATION • VOLUME • DURATION_VOLUME • EVENT
Precedence	Precedence value of the profile. The lower the precedence, the higher the priority.
Flow Status	Indicates whether the application traffic is enabled or disabled in either the uplink or downlink direction. Select from the following: • ENABLED_UPLINK • ENABLED_DOWNLINK • ENABLED • DISABLED
Resource Allocation Notification	Resource Allocation Notification Indicates that the allocation of resources for the related PCC rules are confirmed. Select **ENABLE_NOTIFICATION** to enable.
Required Access Info	Select from the following: • USER_LOCATION — the subscriber's location • MS_TIME_ZONE — the mobile subscriber's time zone • USER_LOCATION and MS_TIME_ZONE — the (mobile) subscriber's location and time zone If this field is not set, the device uses the values sent in AF requests; otherwise, it uses the values set here.
TDF Application Identifier	Identifies the traffic that belongs to the application to which the rule applies.
TDF Redirect Support	Indicates whether the application traffic should be redirected to another controlled address. Select from the following: • REDIRECTION_DISABLED • REDIRECTION_ENABLED

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-211 (Cont.) Create PCC Rule Configurations

Field Name	Description
TDF Redirect Address Type	Specifies the format for the redirect address. Select from the following: • IPv4 • IPv6 • URL • SIP_URI
TDF Redirect Server Address	The address of the TDF redirect server in the specified address type.
Mute Notification	Notification to disable application detection notifications from the TDF device. Select **MUTE_REQUIRED** from the drop-down list. By default, mute remains disabled.
Sponsor Identity	Name identifying a connectivity sponsor.
Application Service Provider Identity	Name identifying an application service provider.
PS to CS Session Connectivity	Indicates that the service data flow carries video and allows for packet switch (PS) to circuit switch (CS) session continuity. Select **VIDEO_PS2CS_CONT_CANDIDATE** from the drop-down list.
Flow Descriptions(s)	IP flows associated with this profile. A comma-separated list of Diameter IP Filter rules following the format specified in RFC 3588 section 4.3. Used in the following cases: • An old traffic profile is imported, and the flow description is not an empty string. • An upgrade from an older version is in process and the existing traffic profile flow description is not an empty string.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **PCC Rule** page. Use or available in the next column to update or delete the listing.

Importing PCC Rule

To import PCC Rule:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.4.5.6.5 Predefined ADC Rule

This procedure provides information about how to define and manage Predefined ADC Rules under Traffic Profiles in PCRF Core.

The **Predefined ADC Rule** page allows you to create new and manage existing Predefined ADC Rules. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure Predefined ADC Rule:

1. From the navigation menu under **Traffic Profile**, select **Predefined ADC Rule**.
   This opens the **Predefined ADC Rule** page. The page lists the existing Predefined ADC Rules. You can add or import new data using this page.

   Note

   - Click Export to download the available listings in the JSON file format on your system.
   - Do not configure duplicate or same key name for pre-defined-pcc-rule, pre-defined-base-pcc-rule and pcc-rule. The actual rule name can be same if customer required. For example,
     key : value **

     For

     ```
     Predefined PCC Rule Base==>btuk5000_Base : btuk5000
     ```

     For

     ```
     Predefined PCC Rule ==>btuk5000 : btuk5000
     ```

2. Click Add .

   This opens the **Create Predefined ADC Rule** page.

3. On the **Create Predefined ADC Rule** page, enter values for the available input fields. The following table describes the fields:

   Table 7-212 Create Predefined ADC Rule Configurations

Field Name	Description
Name	Name of the Predefined ADC Rule.
Rule-Base Name	Uniquely identifies the Predefined ADC Rule. Used to reference an Predefined ADC Rule in communication between the CNC Policy and a PCEF within one IP-CAN session.
Description	Description of the ADC Rule.

4. Click **Save** to save the changes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Predefined ADC Rule** page. Use  or  available in the next column to update or delete the listing.

Importing Predefined ADC Rule

To import Predefined ADC Rule:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.6.6 Predefined ADC Rule Base

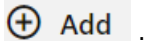
This procedure provides information about how to define and manage Predefined ADC Rule Bases under Traffic Profiles in PCRF Core.

The **Predefined ADC Rule Base** page allows you to create new and manage existing Predefined ADC Rule Bases. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure Predefined ADC Rule Base:

1. From the navigation menu under **Traffic Profile**, select **Predefined ADC Rule Base**.
   This opens the **Predefined ADC Rule Base** page. The page lists the existing Predefined ADC Rule Bases. You can add or import new data using this page.

   > **Note**
   >
   > - Click  to download the available listings in the JSON file format on your system.
   > - Do not configure duplicate or same key name for pre-defined-pcc-rule, pre-defined-base-pcc-rule and pcc-rule. The actual rule name can be same if customer required. For example,
   >   key : value **
   >
   >   For
   >
   >   ```
   >   Predefined PCC Rule Base==>btuk5000_Base : btuk5000
   >   ```
   >
   >   For
   >
   >   ```
   >   Predefined PCC Rule ==>btuk5000 : btuk5000
   >   ```

2. Click  .
   This opens the **Create Predefined ADC Rule Base** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. On the **Create Predefined ADC Rule Base** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-213 Create Predefined ADC Rule Base Configurations

Field Name	Description
Name	Name of the Predefined ADC Rule Base.
Rule-Base Name:	Uniquely identifies the Predefined ADC Rule Base. Used to reference an Predefined ADC Rule Base in communication between the CNC Policy and a PCEF within one IP-CAN session.
Description	Description of the Predefined ADC Rule Base.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Predefined ADC Rule Base** page. Use or available in the next column to update or delete the listing.

Importing Predefined ADC Rule Base

To import Predefined ADC Rule Base:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.6.7 Predefined PCC Rule

This procedure provides information about how to define and manage Predefined PCC Rules under Traffic Profiles in PCRF Core.

The **Predefined PCC Rule** page allows you to create new and manage existing Predefined PCC Rules. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure Predefined PCC Rule:

1. From the navigation menu under **Traffic Profile**, select **Predefined PCC Rule**.
   This opens the **Predefined PCC Rule** page. The page lists the existing Predefined PCC Rules. You can add or import new data using this page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> - Click Export to download the available listings in the JSON file format on your system.
> - Do not configure duplicate or same key name for pre-defined-pcc-rule, pre-defined-base-pcc-rule and pcc-rule. The actual rule name can be same if customer required. For example,
> key : value **
>
> For
>
> `Predefined PCC Rule Base==>btuk5000_Base : btuk5000`
>
> For
>
> `Predefined PCC Rule ==>btuk5000 : btuk5000`

2. Click Add .

   This opens the **Create Predefined PCC Rule** page.

3. On the **Create Predefined PCC Rule** page, enter values for the available input fields. The following table describes the fields:

Table 7-214 Create Predefined PCC Rule Configurations

Field Name	Description
Name	Name of the Predefined PCC Rule.
Rule Name	Uniquely identifies the Predefined Pre-defined PCC Rule. Used to reference an Predefined Predefined PCC Rule in communication between the CNC Policy and a PCEF within one IP-CAN session. **Note**: The ***Name*** and the ***Rule Name*** fields must have the same values. It helps in proper installation of PCC rules.
Description	Description of the Predefined PCC Rule.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Predefined PCC Rule** page. Use or available in the next column to update or delete the listing.

Importing Predefined PCC Rule

To import Predefined PCC Rule:

1. Click Import .
   The page opens the **File Upload** dialog box.

Copyright © 2019, 2026, Oracle and/or its affiliates.

2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.5.6.8 Predefined PCC Rule Base

This procedure provides information about how to define and manage Predefined PCC Rule Bases under Traffic Profiles in PCRF Core.

The **Predefined PCC Rule Base** page allows you to create new and manage existing Predefined PCC Rule Bases. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure Predefined PCC Rule Base:

1. From the navigation menu under **Traffic Profile**, select **Predefined PCC Rule Base**. This opens the **Predefined PCC Rule Base** page. The page lists the existing Predefined PCC Rule Bases. You can add or import new data using this page.

   Note

   - Click Export to download the available listings in the JSON file format on your system.
   - Do not configure duplicate or same key name for pre-defined-pcc-rule, pre-defined-base-pcc-rule and pcc-rule. The actual rule name can be same if customer required. For example,
     key : value **

     For

     ```
     Predefined PCC Rule Base==>btuk5000_Base : btuk5000
     ```

     For

     ```
     Predefined PCC Rule ==>btuk5000 : btuk5000
     ```

2. Click Add .

   This opens the **Create Predefined PCC Rule Base** page.
3. On the **Create Predefined PCC Rule Base** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-215 Create Predefined PCC Rule Base Configurations

Field Name	Description
Name	Name of the Predefined PCC Rule Base.
Rule Name	Uniquely identifies the Predefined PCC Rule Base. Used to reference an Predefined PCC Rule Base in communication between the CNC Policy and a PCEF within one IP-CAN session. **Note**: The ***Name*** and the ***Rule Name*** fields must have the same values. It helps in proper installation of PCC rules.
Description	Description of the Predefined PCC Rule Base.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Predefined PCC Rule Base** page. Use  or  available in the next column to update or delete the listing.

Importing Predefined PCC Rule Base

To import Predefined PCC Rule Base:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.4.6 Usage Monitoring

This section includes the configurations for Usage Monitoring.

To access Usage Monitoring configurations from the CNC Console home page, expand **Policy**, navigate to **Policy Data Configurations**, and select **Usage Monitoring**.

The data configuration for Usage Monitoring includes the following:

- Data Limit Profiles
- Data Limit Selection Profiles
- Data Limit Sorting Profiles
- Data Rollover Profiles

7.4.6.1 Data Limit Profiles

To configure the data limit profiles:

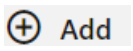
1. Navigate to **Data Limit Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
2. Click  .
   The **Create Data Limit Profile** page appears.
3. On **Create Data Limit Profile** page, add the following details:

Table 7-216 Create Data Limit Profile

Field Name	Description
Profile Name	Uniquely identifies the UM Data Limit Profile by a name. This field is for configuration purpose only and not transmitted over the network.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-216 (Cont.) Create Data Limit Profile

Field Name	Description
Limit Identifier	Specifies the limit identifier. Multiple limit identifiers may have the same priority.
Monitoring Key	Uniquely identifies the UM Data Limit Profile by a Monitoring Key. If its value is not explicitly provided, then the data limit profile's limitId will be used as the monitoring Key of that profile.
Profile Type	Specifies the type of the Data Limit Profile. **Default value**: SUBSCRIBER **Note**: Striked-out entries are for future.
Plan Type	Specifies the type of Plan such as Base, Top-up, and Pass. This helps to determine the priority in selecting the plan over other types. The priority is configurable in service configuration screen. **Default value**: Base
Parent Plan	Identifies a Data Limit Profile as a parent data plan. Any attribute that is not explicitly configured in this plan shall be taken from the parent plan (if present).**Note**: **Parent Plan** cannot be the same as the **Profile Name**.
Priority	A Priority is used to weigh it with other Data Limit Profiles and UDR provisioned Data Limits of the same Plan Type. The priority can be used by Policy or Data Limit Selection Profile for choosing among different candidate profiles. The Plan Type, Priority within that Plan Type and the Selection Order of Plan Types together decide the order of selection of Data Plans.
Validity Duration	Indicates the length of usage time in seconds. **Range**: 3600 - 31536000 (1 Year) **Note**: Validity Duration is applicable only for plans, which has **Periodicity** as NEVER. There is no validity for the recurring plans.
UM Level	Indicates the level of the usage monitoring instance (PDU Session level or per Service). **Default value**: Session Level
Inactivity Time (seconds)	Time interval in seconds after which the PGW or SMF shall stop time measurement for the Monitoring Key, if no packets are received belonging to the corresponding Monitoring Key **Range**: 0 - 604800 (7 Days) **Default value**: 86400 (1 Day)
Data Rollover Profile	A reference to a Data Rollover Profile. If not configured, Data Rollover will be disabled for this Data Plan.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-216 (Cont.) Create Data Limit Profile

Field Name	Description
Allow Excess Usage	Indicates whether or not excess usage is allowed for this Data Limit Profile. When Excess Usage is allowed, Usage Monitoring shall continue to grant and accumulate usage even after consuming 100% of allocated volume/time. The QoS, Charging etc. parameters can be controlled at PCRF Core Policy on account of the consumed usage. **Default value**: False
Usage Limit	Provide Usage Limit details:
Duration	Indicates the length of time in seconds. **Range**: 3600- 2592000
Volume Total	Specifies the total data octets for both downlink and uplink **Range**: 512 - 1000000000000
Volume Uplink	Specifies the uplink data octets. **Range**: 512 - 1000000000000
Volume Downlink	Specifies the downlink data octets. **Range**: 512 - 1000000000000
Reset Period	Provide Reset Period details:
Period	Indicates whether the periodicity is "YEARLY", "MONTHLY", "WEEKLY", "DAILY" , "HOURLY", "NEVER". **Default value**: Monthly
Maximum Number Of Periods	Indicates the maximum number of periods after which the usage monitoring instance does not apply. If omitted, there is no limit in the number of periods.
Billing Day	Provide Billing Day details:
Type	Indicates which day of the period to reset the usage limit. **Default value**: LAST_DAY **Note**: If this configuration is updated, the new configuration shall be applied in the next billing cycle.
Day	Indicates the specific day of the period. Day count starts from 1. If the Day entered is beyond the last day of a period (for example 31 for the month of April), the last day shall be considered. Required when "SPECIFIC_DAY" is selected in the Type field. **Note**: If this configuration is updated, the new configuration shall be applied in the next billing cycle.
Time	Indicates the specific time of day in "HH:MM:SS" **Default value**: "00:00:00" **Note**: If this configuration is updated, the new configuration shall be applied in the next billing cycle.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-216 (Cont.) Create Data Limit Profile

Field Name	Description
Excess Usage Limit	Provide Excess Usage Limit details:
Percentage	Indicates the percentage of base volume/time up to which excess usage is allowed. **Range**: 101-1000 **Note**: If this field is applicable for Excess Usage Limit, the value of the field should not be left empty. Otherwise, excess usage beyond the usage limit duration will not be allowed.
Duration	Indicates the length of time in seconds. This is inclusive of the base duration. That is, the value in this field indicates the total duration to be consumed including base + excess. **Range**: 3600 - 31536000 (1 Year) **Note**: If this field is applicable for Excess Usage Limit, the value of the field should not be left empty. Otherwise, excess usage beyond the usage limit duration will not be allowed.
Volume Total	Specifies the total data octets for both downlink and uplink. This is inclusive of the base total volume. **Range**: 512 - 1073741824000 (1000 GB) **Note**: If this field is applicable for Excess Usage Limit, the value of the field should not be left empty. Otherwise, excess usage limit for both uplink and downlink data octets will not be considered.
Volume Uplink	Uplink data octets. This is inclusive of the base uplink volume. **Range**: 512 - 1073741824000 (1000 GB) **Note**: If this field is applicable for Excess Usage Limit, the value of the field should not be left empty. Otherwise, excess usage limit for uplink data octets will not be considered.
Volume Downlink	Downlink data octets. This is inclusive of the base downlink volume. **Range**: 512 - 1073741824000 (1000 GB) **Note**: If this field is applicable for Excess Usage Limit, the value of the field should not be left empty. Otherwise, excess usage limit for downlink data octets will not be considered.

4. Click **Save** to save the Data Limit Profile.

7.4.6.2 Data Limit Selection Profiles

This page allows you to select, create, and configure Data Limit Selection Profiles.

Data Limit Selection is a set of rules to select one or more Data Limits based on certain conditions.

To create and configure the Data Limit Selection Profiles:

Copyright © 2019, 2026, Oracle and/or its affiliates.

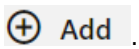
1. Navigate to **Data Limit Selection Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
2. Click 

.
The **Create Data Limit Selection Profile** page appears.
3. Enter the a unique name to identify the Data Limit Selection Profile.
4. Click 

to create new selection rules.
The **Add Selection Rules** dialog box appears.
5. Enter values for the available input fields described in the following table:

Table 7-217 Selection Rules Configurations

Field Name	Description
Priority	Indicates the selection rule priority.
Type	Indicates the selection rules type.
Data Limit Profile Name	This field is displayed when Type is "Data Limit Profile". This field should match the name configured in the Data Limit Profile.
UDR Data Limit Name	This field is displayed when Type is "UDR Data Limit". This field should match the Limit Identifier or the name of the plan if configured in Custom Attribute mapping and present in the UM Data Limit.
Always Match	When this is true, no conditions shall be evaluated. This can be used as a CATCH ALL Selection Rule. **Default value**: false

6. Under **Conditions**, click 

.
The **Add Conditions** dialog box appears.

   Enter values for the available input fields described in the following table:

Table 7-218 Conditions Configurations

Field Name	Description
Parameter Type	Indicates the type of parameter on which the condition will be applied. • Forwarded Attribute - Am attribute forwarded by the core service, for e.g. Serving Gateway MCCMNC / IP Address, APN etc. • Policy Decision Tag - A Tag applied by the policy.
Attribute Name	This field is displayed when Parameter Type is "Forwarded Attribute".
Operator	Accepts the following values: • Equals • Not Equals • Less Than • Greater Than • Matches

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-218 (Cont.) Conditions Configurations

Field Name	Description
Value	Displays the list of configured Match Lists when the Operator is "Matches".

Click **Save** to save the conditions.

7. Click **Save** to save selection rules.

7.4.6.3 Data Limit Sorting Profiles

This page allows you to select, create, and configure Data Limit Sorting Profiles.

Data Limit Sorting Rule is a set of rules to sort Data Limits. If Sorting Rules are configured, Sorting rules are applied after applying Selection Rules and when the output of Selection Rules results in more than one Data Limit.

To configure Selection and/or Sorting Rules to select one Usage Monitoring Data Limit out of many data limits provided by UDR or out of those configured in Data Limit Profiles, perform the following configurations:

1. Navigate to **Data Limit Sorting Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
   The **Create Data Limit Sorting Profile** page appears.
2. Enter a name to uniquely identify the Data Limit Selection Profile in the **Name** field. This is a mandatory field.
3. On the **Create Data Limit Sorting Profile** page:
   a. Under **Sorting Rules**, click ⊕ Add .
      This opens the **Add Sorting Rules** dialog box.
   b. In **Add Sorting Rules** dialog box, perform the following configurations:

Table 7-219 Sorting Rules Configurations

Field Name	Description
Index	Specifies the index. The sorting rules are applied in the order of index.
Parameter Type	Specifies the type of the parameter. Possible values are: • Start Date • End Date • Priority • Periodicity • Data Limit Custom Attributes
Attribute Name	Specifies the name of the attribute. This is a conditional field. It is displayed in GUI only when the value of **Parameter Type** is set to **Data Limit Custom Attributes**.
Order	Specifies the order. Possible values are: • Ascending • Descending

Copyright © 2019, 2026, Oracle and/or its affiliates.

c. Click **Save** to save sorting rules.

4. Click **Save** on the **Create Data Limit Sorting Profile** page to save the Data Limit Sorting Profile.

7.4.6.4 Data Rollover Profiles

To create the data rollover profile:

1. Navigate to **Data Rollover Profiles** page under **Usage Monitoring** in **Policy Data Configurations**.
2. Click 

.
This opens **Create Data Rollover Profile** page.
3. In the **Create Data Rollover Profile** page, add the following configurations:

Table 7-220 Create Data Rollover Profile

Field Name	Description
Profile Name	A unique to identify the Data Rollover Profile.
Data Rollover Enabled	Indicates whether to enable or disable Data Rollover.
Rollover Data Consumption	Indicates when to consume the rollover data. Rollover data to be consumed before or after a base plan. **Note**: As of now, Policy does not support consumption of the rollover data after the parent plan.
Maximum Number of Rollovers	Indicates how many cycles the data plan can rollover. A value of 0 means there is no limit to the number of cycles the left over data can rollover. **Range**: 0 to 24 **Default value**: 0 (No limit)
Data Rollover Percentage	Indicates the percentage of left over data volume/time to rollover to the next cycle. If `Data Rollover Enabled` is enabled, then data rollover percentage must be provided between 1-100. By default, it will take as 0. If the plan contains `timeThreshold`, `totalVolume`, `uplink`, and `downlink`, then all the fields must be provided in maximum and minimum rollover for accurate calculation while creating and allocating rollover data for a plan. **Range**: 1 to 100 **Default value**: 0. **Note**: When Data Rollover Percentage is not defined and the subscriber tries to rollover the data on the basis of maximum rollover threshold / maximum rollover threshold or DATA cap setting, data rollover will not be triggered as the Data Rollover Percentage is taking 0% value.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-220 (Cont.) Create Data Rollover Profile

Field Name	Description
Data Limit Cap Enabled	Indicates whether to enable or disable data limit cap. Data Limit Cap Settings is used to configure the data limit cap, which is applied on until how much of data it must allow rollover across the cycles (rollover). Data Limit Cap has two components: • Base Data Limit, which is fixed. • Rollover, can accumulate over time and reach a value where the capping is applicable. Rollover configuration should be part of Rollover Profile. With different profiles, different capping schemes can be applied. For example, bounded and unbounded rollovers, single period rollover vs. multi-period rollovers. Data Limit Cap checks if the dataLimitCap - baseLimit - additionalRollOVer (which is calculated by adding all the roll-over across the reset cycle happens) > 0, then it allows for rollover. Otherwise, it does not allow the rollover. The maximum cap is applied on the total of base plan volume/time and total accumulated rolled over volume/time.
Maximum Rollover Threshold	To configure the maximum amount of data volume/time that can roll over from one cycle to another.
Base Data Percentage	Indicates the percentage of base plan data volume/time that is allowed as rollover data volume/time. **Range**: 0 to 100
Duration	Indicates the length of time in seconds. **Range**: 3600 - 2592000 (30 Days)
Volume Total	Specifies the total data octets for both downlink and uplink. **Range**: 512 - 107374182400 (100 GB)
Volume Uplink	Specifies the uplink data octets. **Range**: 512 - 107374182400 (100 GB)
Volume Downlink	Specifies the downlink data octets. **Range**: 512 - 107374182400 (100 GB)
Minimum Rollover Threshold	To configure minimum rollover threshold.
Duration	Indicates the length of time in seconds. The remaining duration if applicable shall be rolled over to the next period if it is greater than the threshold value configured here. **Range**: 0 - 2592000 (30 Days)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-220 (Cont.) Create Data Rollover Profile

Field Name	Description
Volume Total	Specifies the total data octets for both downlink and uplink. The remaining total volume if applicable shall be rolled over to the next period if it is greater than the threshold value configured here. **Range**: 0 - 107374182400 (100 GB)
Volume Uplink	Specifies the uplink data octets. The remaining uplink volume if applicable will be rolled over to the next period if it is greater than the threshold value configured here. **Range**: 0 - 107374182400 (100 GB)
Volume Downlink	Specifies the downlink data octets. The remaining downlink volume if applicable will be rolled over to the next period if it is greater than the threshold value configured here. **Range**: 0 - 107374182400 (100 GB)
Data Limit Cap Settings	Data Limit Cap Settings is used to configure the data limit cap, which is applied on until how much of data it must allow rollover across the cycles (rollover).
Duration	Indicates the length of time (duration) in seconds for which the data cap must be imposed. **Range**: 3600 - 2592000 (30 Days)
Volume Total	Indicates the maximum limit on the total volume of data octets for both downlink and uplink. **Range**: 512 - 107374182400 (100 GB)
Volume Uplink	Indicates the maximum volume of data that must be allowed for the uplink data octets. **Range**: 512 - 107374182400 (100 GB)
Volume Downlink	Indicates the maximum volume of data that must be allowed for the downlink data octets. **Range**: 512 - 107374182400 (100 GB)

4. Click **Save** to save the Data Rollover Profile.

7.5 Policy Management

Policy offers a Policy Design editor based on the Blockly interface. You can create and manage a Policy project for each of the following Policy services, based on your deployment:

- Session Management and Policy Authorization
- Access and Mobility Management
- UE Management
- PCRF Core
- Policy Data Source
- Usage Monitoring

This section describes how to create, manage, and deploy policies using the **Policy Management** pages.

Copyright © 2019, 2026, Oracle and/or its affiliates.

The Policy Management configurations includes:

- Policy Projects

The following section describes the configurations on the **Policy Projects** page.

7.5.1 Policy Projects

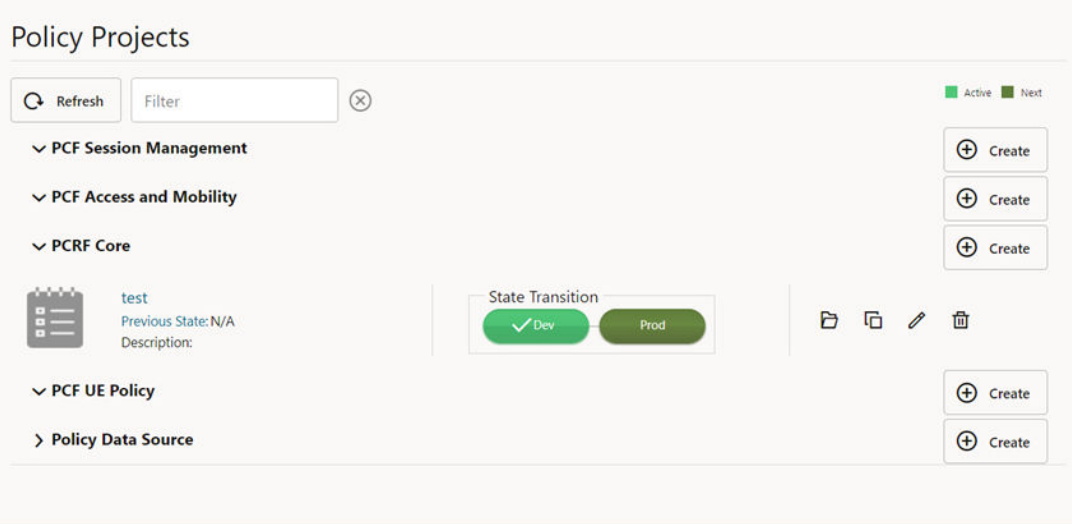
You can create and deploy a Policy project using **Policy Projects** page. There are two possible states for the Policy project, **Prod** and **Dev**.

To create and deploy a Policy project:

1. From the navigation pane under **Policy**, navigate to **Policy Management** and select **Policy Projects**.
   This opens the **Policy Projects** page, displaying the existing Policy projects for the respective Policy service.

   The following screen capture shows an illustration of the **Policy Projects** page:

Figure 7-32 Policy Projects



   You can filter the existing projects based on Project Name and Active State using the Filter box available at the top of the page.

2. To create new project, click ⊕ Create for the service group, for which the Policy project is to be created.
   The page opens the **Create Policy Project** dialog box.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> - Policy supports 10 projects per service type. An error message is displayed on clicking Create, if the number of projects created for a selected service type has reached maximum limit.
> - Release 26.1.200 improves memory utilization in the Policy Runtime service. However, this will not be fully applied to policy projects created prior to this release. In order to use this, you must clone any existing policy project (created prior to Release 26.1.200) and then move it to "prod" state. Cloning recreates projects with optimized references for improved performance. Existing (pre-26.1.200) projects remain usable but are read-only. To make any edits, cloning is required. Non-cloned projects will not benefit from these memory optimizations and can be retired after validating the cloned versions.

3. In the **Create Policy Projects** dialog box, enter the following information:

Table 7-221 Create Policy Projects

Field Name	Description
Name	The unique name you assign to the policy project This is a mandatory field. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underscore (_). The maximum length is 32 characters. **Note:** Name must start with a letter, underscore (_), or $. It cannot start with a digit (0–9), however, it can contain digits after the first character.This Note is also applicable while creating the sub policy under the Policy Project.
Description	Free-form text that identifies the Policy project. The maximum length is 255 characters.

4. Click **Save**.
This creates the Policy Project. The project is listed under the respective service name group.

> **Note**
>
> - Policy allows you to perform unit test for a project. For more information on testing the projects, see `Test Policy Projects` section in the *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.
> - The **Policy Project** page allows you to clone projects. Use the icon available with the Policy project listing to clone the project. The cloned project contains the data similar to the project from which it is cloned.
> - Use or to update or delete the Policy project.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. To configure the Policy project, click  corresponding to the project name.
This opens the Blockly editor. The editor allows you to construct one or more policies using the building blocks provided in the left hand side panel of the editor.

> **Note**
>
> The projects in **Prod** state are not editable. You can only view these projects and the associated policies, but cannot modify them.

For more information on configuring Policy blocks using Blockly editor, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

6. Change the state of a the Policy project, if required.
Policy Projects can have any of the following states:
   - **Dev**: By default, the **Dev** state is assigned to a Policy project. Dev projects do not process any traffic in PRE.
   - **Prod**: The projects in **Prod** state processes traffic in PRE.

   The current state of any project can be identified with a tick mark and light green colored button as displayed at the upper right hand corner of the **Policy Projects** page.

   The following screen capture illustrates the different states of a project.

Figure 7-33 Policy Project States



> **Note**
>
> At any point of time there can be only one project in **Prod** state for a service. If you change the state of the project to **Prod** and there is already a project with the **Prod** state for that service, the **Prod** state for the existing project automatically gets updated to **Dev** state and the project in **Dev** state is updated to **Prod** state.

> **Note**
>
> When a user creates or updates (for example project states) a Policy project through CNC Console or REST API, it may take up to 10 seconds for the changes to reflect in the Policy rule.

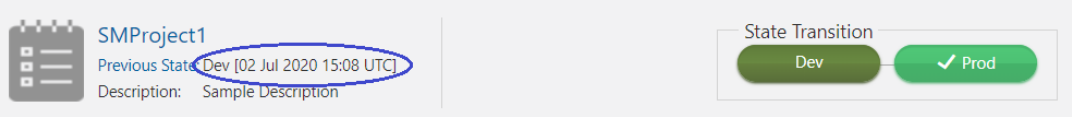
Viewing Policy Project States

The **Policy Projects** page displays the previous states of projects along with the timestamp. The details are described in the following examples:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Example 1:**
  The following screen capture shows an example, displaying a project in **Prod** state:

Figure 7-34 Example 1



The following details are highlighted in the above example:

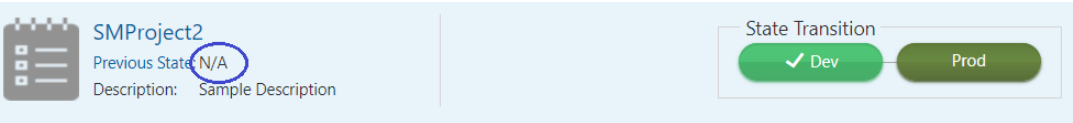
Current State: Prod

Previous State: Dev

Timestamp when the state changed from **Dev** to **Prod**: 02 Jul 2020 15:08 UTC

- **Example 2:**
  The following screen capture shows an example, displaying a newly created project in **Dev** state:

Figure 7-35 Example 2



The following points lists the details highlighted in the above example:

Current State: Dev

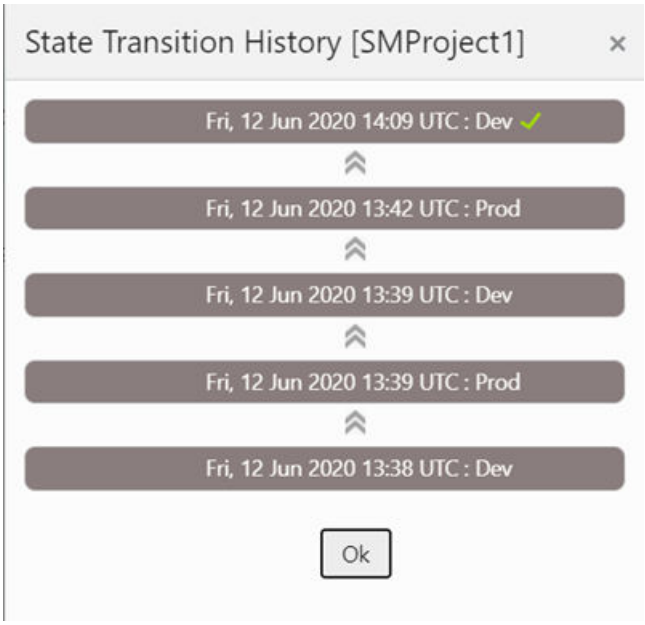
Previous State: N/A

Since it is a new project, there is no previous state.

- **Example 3:**
  The following screen capture shows an example of getting the complete history of the previous states of a Policy project by clicking the **Previous States**:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-36 Example 3



7.6 Diameter Configurations

This section describes how to manage and view the Diameter Configurations in Policy using the **Diameter Configurations** pages.

7.6.1 Settings

The **Settings** page displays the general configurations related to the Diameter node. The page allows you to edit the configurations.

To edit settings:

1. From the navigation menu, under **Policy**, click **Diameter Configurations** and select **Settings**.
   This opens the **Settings** page. The page displays the existing configurations.
2. Click Edit .
   This opens the **Edit Settings** page.
3. Enter the following information under the respective groups:

Table 7-222 Edit Settings

Field Name	Description
Timer	Provide Timer details:
Reconnect Delay (sec)	Enter the time frame to delay before attempting to reconnect after a connection failure in seconds. The default value is 3 seconds.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-222 (Cont.) Edit Settings

Field Name	Description
Response Timeout (ms)	Enter the response timeout interval in milliseconds. The default value is 5000 ms. **Note**: The response timeout interval can have a decimal value. It helps to put the value in milliseconds.
Connection Timeout (sec)	Enter the connection timeout interval in seconds. The default value is 3 seconds.
WatchDog Interval (sec)	Enter the watchdog interval in seconds. The default value is 6 seconds.
Transport	Provide Transport details:
Protocol	The protocol supported is TCP.
Message Priority Profile	Provide Congestion Control details.
Message Priority Profile	Select any of the configured message priority profiles from the drop-down menu. **Note**: The following message priority data that was exported prior to Policy 23.2.0 cannot be imported as the data may be corrupt: • message containing Sd as interface • Sy-SLR as condition message The data with Sd interface or Sy-SLR condition messages that are exported only with Policy 23.2.0 or later versions can be imported.
Overload Control	Provide Overload Control details:
Load Shedding Profile	Select any one of the configured load shedding profiles from the drop-down menu.
Topology Hiding	Provide Topology Hiding details:
Topology Hiding	Enable or disable the topology hiding feature using this switch. When this feature is disabled, no changes are made to the origin-host in the message. On enabling this feature, origin-host is updated in all or specific messages.
Apps to Hide	Specifies the application names for which topology hiding feature needs to be enabled. Users can select one or many values from the following list using the drop-down: • Rx • Gx • Sy • All When Topology Hiding feature is enabled with value `All` for **Apps to Hide** field, origin-host is replaced for all the diameter interface outgoing messages.
Enhanced Timer Configuration	Provide Enhanced Timer Configuration details:
Application Name	Request Timer configuration for applications name like Rx, Gx, Sy, Sd.
Application Response Timeout (milliseconds)	Enter the application response timeout in milliseconds. The range of this value is between 3 seconds to 2147483647.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-222 (Cont.) Edit Settings

Field Name	Description
Command Code Response Timeout	Provide Command Code Response Timeout details:
AAR (milliseconds)	The command code response timeout value for AAR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000
STR (milliseconds)	The command code response timeout value for STR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000
RAR (milliseconds)	The command code response timeout value for RAR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000
ASR (milliseconds)	The command code response timeout value for ASR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000

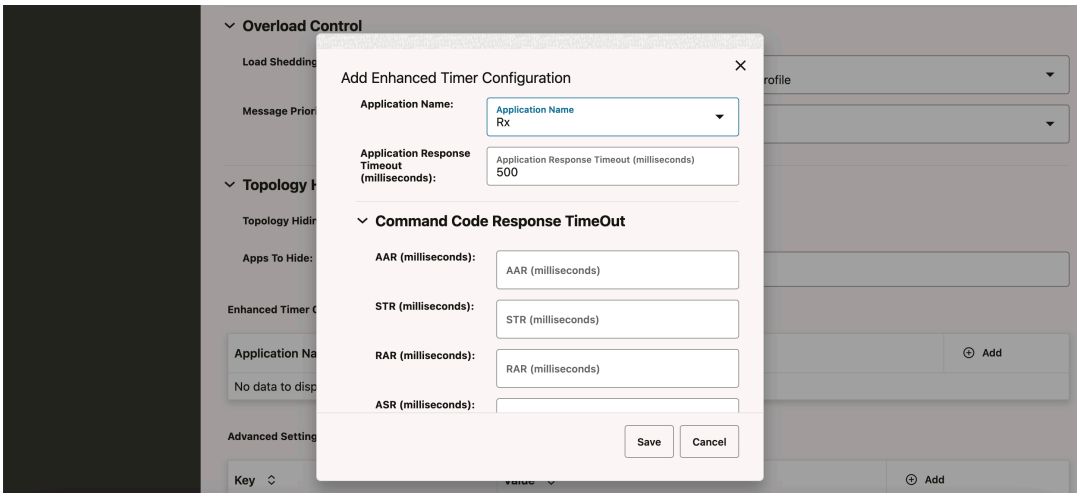
The order of precedence (from highest to lowest) of response timeout configurations is:

a. Command Code Response Timeout (ms) - Message level configurations i.e at AAR, STR etc.

b. Application Response Timeout (ms) - Interface level configuration i.e at Gx, Rx etc.

c. Response Timeout (ms) - General level configuration

Figure 7-37 Add Enhanced Timer Configuration in the edit mode



4. Click **Save** to save the settings.

5. Perform the following steps to configure **Advanced Settings**:

   a. Click the ⊕ Add
   The page opens the **Add Advanced Settings** dialog box.

Copyright © 2019, 2026, Oracle and/or its affiliates.

b. In the dialog box, enter the following **key** and respective **value**:

Table 7-223 Parameters for Advanced Settings

Keys	Value
DIAMETER.ErrorHandler.MaxRetryCount.Rx.RAR	It is used to set the maximum retries that can be performed for failed RAR messages. The retry attempt value can be any positive integer number between 1 to 2147483647. **Note**: If retry attempt value configured is a zero or negative number, then the default retry attempt value shall be considered. **Default Value**: 1
DIAMETER.ErrorHandler.CycleBackRetry.Rx.RAR	It is used to set if peers can be cycled back for retries or not. **Default Value**: false
DIAMETER.ErrorHandler.MaxRetryCount.Rx.ASR	It is used to set the maximum retries that can be performed for failed ASR messages. The retry attempt value can be any positive integer number between 1 to 2147483647. **Note**: If retry attempt value configured is a zero or negative number, then the default retry attempt value shall be considered. **Default Value**: 1
DIAMETER.ErrorHandler.CycleBackRetry.Rx.ASR	It is used to set if peers can be cycled back for retries or not. **Default Value**: false
DIAMETER.ErrorHandler.Enable.UpdateDestinationHost	By default, the cnPolicy Diameter Gateway uses the same `Destination-Host` AVP in the retry message as the one received in the original request message. To update the `Destination-Host` AVP in the retry message with the destination peer selected by the error handling configuration, set `DIAMETER.ErrorHandler.Enable.UpdatedDestinationHost` to `true`. If this parameter is set to `false`, the retry message retains the original Destination-Host AVP. Default value: `false`
DIAMETER.gateway.binding.lookup.failure.forcerouting.enabled	This is used to enable force routing to PCRF Core and/or Diameter Connector on receiving Rx Commands along with Binding error response. **Default Value**: true
DIAMETER.gateway.binding.lookup.failure.forcerouting.service.list	This is used to set the force routing to PCRF Core and/or Diameter Connector. The possible list of values: • PCRF_CORE • DIAMETER_CONNECTOR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-223 (Cont.) Parameters for Advanced Settings

Keys	Value
DIAMETER.gateway.binding.lookup.failure.forcerouting.exceptions	This is used to identify the exceptions for which force routing needs to be set. The possible list of values: • java.net.UnknownHostException • java.net.ConnectException • java.util.concurrent.TimeoutException But any **class exception** can be placed as a value of the list.
DIAMETER.gateway.binding.lookup.failure.forcerouting.responsecodes	This is used to identify the response error codes for which force routing needs to be set. The possible list of values: • 404 • 503 But any **http status code** can be placed as a value of the list.
DIAMETER.Timer.Enabled	Indicates whether to enable or disable the creation of timer AVPs in Diameter Gateway (Orignation-Timestamp, Sender-Timestamp and Max-Response-Time) and forwards them to subsequent services. **Default value**: `false`
CONGESTION_DIAMETER_RESPONSE_CODE	This is to configure the diameter result code for the congestion control discards and data type of value will be numerical. If value is not configured, then default congestion result code will be *3004 (DIAMETER_TOO_BUSY)* **Default Value**: 3004 **Examples**: CONGESTION_DIAMETER_RESPONSE_CODE=5065 CONGESTION_DIAMETER_RESPONSE_CODE=3004
CONGESTION_DIAMETER_VENDOR_ID	This is to configure the diameter vendor id for the congestion control discards and data type of value will be numerical. If value is non-zero, then the *CONGESTION_DIAMETER_RESPONSE_CODE* considered as the experimental result code. If value is zero / not configured, then *CONGESTION_DIAMETER_RESPONSE_CODE*considered as the normal result code. **Examples**: CONGESTION_DIAMETER_VENDOR_ID=10415 CONGESTION_DIAMETER_VENDOR_ID=21274

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-223 (Cont.) Parameters for Advanced Settings

Keys	Value
DIAMETER.UseLegacyBwWhenExtendedBwNotSupported	Indicates whether to enable or disable the extended bandwidth for controlling the AVP. **Default value**: `false`
ENABLE_N7_SESSION_LOOKUP_COOKIE	Determines whether to enable or disable the support for optimizing N7 session lookup for AAR-I messages in Rx callflows at Diameter Gateway service. Possible values are: • true (to enable the feature) • false (to disable the feature) If this key is enabled, when Diameter Gateway receives an AAR-I request, • If BSF is enabled, Diameter Gateway processes the request and forwards `OCNF-SERVICE-COOKIE` AVP to Diameter Connector. • If BSF is disabled, Diameter Gateway interacts with Binding service to retrieve the context owner for the request. Diameter Gateway then forwards the request to Diameter Connector, which extracts the details in the AVP, adds it to the HTTP request of the PA Create request and sends the same to SM service. **Default value**: `false`
DIAMETER.gateway.sd.session.owner.failure.forcerouting.enabled	This is used to enable force routing to PCRF Core and/or Diameter Connector for Sd interface. Allowed values are true or false. **Default Value**: false
DIAMETER.gateway.sd.session.owner.failure.forcerouting.service.list	This is used to set the force routing to PCRF Core and/or Diameter Connector. Default value is a string. Possible values are: • PCRF_CORE • DIAMETER_CONNECTOR
DIAMETER.gateway.sd.session.owner.failure.forcerouting.retry.timeout	This is used to enable force routing retry on the next service if the current selected service is throwing timeout error. Allowed values are true or false. **Default Value**: true
DIAMETER.gateway.sd.session.owner.failure.forcerouting.retry.diameter.unknown.session.id	This is used to enable force routing retry on the next service if the current selected service is throwing `DIAMETER_UNKNOWN_SESSION_ID`. Allowed values are true or false. **Default Value**: true

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-223 (Cont.) Parameters for Advanced Settings

Keys	Value
DIAMETER.gateway.sd.session.owner.failure.forcerouting.retry.error.code.list	Provide the list of diameter error code for which users want to retry force routing. If the diameter error code coming from the current selected service is present in this list then force routing is retried on the next service. Allowed value is a string, and default is empty string. Example: 3004, 5012 **Default Value:** ""
DGW_CONNECTION_REPAVING.MAX_STAGGER_JITTER_MS	Specifies the maximum duration in seconds for stagger window. All pod disconnections are randomly distributed within this time frame. This approach does not depend on the number of pods. **Default value**: 300 **Range**: 300–14400
DGW_CONNECTION_REPAVING.REINVOCATION_DELAY_MIN	Specifies the minimum time between repaving operations. This is the wait between invocations, to prevent the force disconnection from being triggered multiple times in a short period. **Default value**: 10 **Range**: 5–480
DGW_CONNECTION_REPAVING.CONNECTION_DISCONNECT_INTERVAL_MS	The delay in milliseconds that the pod pauses between terminating each target connection. This throttles the process to prevent flooding a peer. **Default value**: 5000 **Range**: 1000–120000
DGW_CONNECTION_REPAVING.DPR_DELAY_MS	Specifies the delay between DPR transmission and forced disconnect. **Default value**: 100 **Range**: 100–200
DGW_CONNECTION_REPAVING.DPR_DISCONNECT_CAUSE	Defines the cause included in DPR. Possible values: • REBOOT • BUSY • DO_NOT_WANT_TO_TALK_TO_YOU

c. Click **Save**.
The page saves the Error Handling configurations.

7.6.2 Peer Nodes

This procedure provides information about how to define and manage Peer Nodes in Diameter Configurations.

The **Peer Nodes** page allows you to create new and manage existing Peer Nodes. The page displays the list of defined configurations and provides the options to import, export, or add data.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure Peer Nodes:

1. From the navigation menu, under **Policy**, click **Diameter Configurations**, and select **Peer Nodes**.
   This opens the **Peer Nodes** page. The page lists the existing Peer Nodes. You can add or import new nodes using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create Peer Node** page.

3. On the **Create Peer Node** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-224 Create Peer Node Configurations

Field Name	Description
Name	Unique name of the peer node. Example value: ocs
Type	Defines which type of diameter service must be selected. The values can be • PCF • Application function (AF) • Backend • Diameter Routing Agent (DRA) • Online Charging System (OCS) • TDF • UDR You can choose a specific type if a particular NF can be directly connected. If NF is behind the DRA, then DRA must be chosen. Backend is a special type used by the engineering team to connect to the backend core services.
Reconnect Limit (sec)	The reconnect limit. This value must be configured as the Diameter peer configuration. Currently, all the Gateway pods reconnect for infinite time for the cloud native environment. Hence, this variable is of no use. This value can be kept as it is.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-224 (Cont.) Create Peer Node Configurations

Field Name	Description
Initiate Connection	Initiate connection has two options: • True: diameter-gateway initiates a connection. **Note:** Each diameter-gateway pod initiates one connection. • False: diamteter-gateway acts as a responder. It waits for other peers to initiate a connection. **Note:** When the diameter gateway is the connection initiator, then each diameter gateway pod would initiate 1 diameter connection with a network peer. For an example, if there are three diameter gateway pods and two external peers, then a mesh would be created with 6 diameter connections.
Port	Enter the port number. Enter a number from 0 to 65535. Example value: `8007`
Transport	Defines the type of transport ways for configuring a peer. The values can be: • TCP • TLSv1.2 • TLSv1.3 • TLSv1.2_OR_TLSv1.3
Host	Enter the host name. Enter a FQDN or IP address available for establishing diameter transport connections to the peer node. **Note:** It is mandatory if *Initiate Connection* is set to true.
Realm	Enter the Realm of the peer to which diameter-gateway needs to be connected. For example,to add the realm detail of the OCS peer, enter `oracle.com` .
Identity	Enter an identity of the peer to which diameter-gateway needs to be connected. For example, to add the identity detail of the OCS peer, provide value enter `ocs`. **Note:** It is mandatory if **Type** is set to *TDF*.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Peer Node** page. Use  or  available in the next column to update or delete the listing.

Importing Peer Node

To import peer node:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.6.3 Routing Table

Configuration allows the routing of Diameter request messages to next hop peer based on `Diameter application-id`, `Destination-Realm`, and `Destination-Host` using Diameter routing table.

When using routing table, there are two ways to configure the next hop route:

1. Host-Based Routing: The destination-host of incoming message is checked in the routing table, and then the message is routed to the top priority of the matching route's peer.
2. Realm-Based Routing: The destination-realm of incoming message is checked in the routing table, and then the message is routed to the top priority of the matching route's peer.

Routing decision at Diameter-Gateway

Diameter gateway follows below steps in the following sequence:

1. If the incoming request message has destination-host and the specified peer is directly connected with the gateway pod, then the message is routed to the peer specified in destination-host.
2. If the incoming request message has destination-host and is not directly connected via any other diameter-gateway pods in cluster, then the message will be inter-pod routed.
3. The routing table is scanned for a matching route:
   - If the host is reachable, message is sent.
   - If the host is not reachable directly, find if it can be reached by another diameter gateway pod, message is sent using inter-pod route.
   - If the host is not reachable directly or indirectly, look up the routing table again for the next priority matching route.

> **Note**
>
> In the routing table, if any peers are not matched then the default route peer will be selected if it is configured.

The **Diameter Routing Table Configurations** page displays the Diameter routing table configurations. The page allows you to edit the configurations.

To configure the diameter routing table:

1. From the navigation menu, under **Policy**, click **Diameter Configurations** and select **Routing Table**.
   This opens the **Diameter Routing Table Configurations** page. The page displays the existing configurations.
2. Click Edit .
   This opens the **Edit Diameter Routing Table Configurations** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Expand the **Diameter Route Table** Table group.
   The expanded group allows you to add route table entries.
4. To add routing table:
   a. Click 

      .
      The page opens the **Add Diameter Route Table** dialog box.
   b. Enter the values for the following input fields:

Table 7-225 Add Diameter Route Table Configuration

Field Name	Description
Priority	Defines the order of use when one or more routes have overlapping criteria. **Note:** If there are more than one routing table entry with same priority, it will consider only first row from multiple rows with same priority. The range is 0-65535. Example value: `1`
Name	Configure Name as the value specified in Server Identifier. Starting with release 1.11.1, for the data sources configured as peer nodes in diameter gateway for Sy interface, the diameter routing table configurations must be added. While configuring, ensure that the given name is same as the value specified in the Server Identifier field.
Type	Route type. The value can be Realm or Host. • When the **Realm** is selected in the **Type** field, **Realms** field is displayed. • When the **Hosts** is selected in the **Type** field, **Hosts** field is displayed.
Realms	The realm detail of the route. Example value: `oracle.com`
Application ID	Select Rx , Gx, Sy, or All. Example value: `Sy`
Server Identifier	Specifies the server to which the message is to be routed. This identity must also be present in the Identity field of the peer node. **Note:** If multiple server identifiers are configured one after the other separated by (,) comma, it considers the first value and ignores the rest of the values which were added with the comma separator.

   c. Click **Save** on the **Add Diameter Routing Table** dialog box.
5. On the **Edit Diameter Routing Table Configurations** page, expand the **Default Route** group.
6. Enter value for the **Server Identifier** drop-down list.
   The server identifier drop-down list shows the list of the configured peer nodes on the **Peer Nodes** configuration page. For more information on configuring Peer Nodes, see Peer Nodes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

On selecting any of the value, ensure that the name is same as the values of server identifier.

> **Note**
>
> * (asterisk) wild card character is allowed in **Hosts**, **Realms**, and **Server Identifier** fields.

7. Click **Save**.
   The configuration gets listed on the **Diameter Routing Table Configurations** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the Diameter Routing Table configurations.

7.6.4 Peer Node Sets

To configure Peer Node Sets:

1. From the navigation menu, under **Policy**, click **Diameter Configurations** and select **Peer Node Sets**.
   This opens the **Peer Node Sets** page. The page lists the existing Peer Node Sets. You can add or import new nodes using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the **Create Peer Node Sets** page.
3. On the **Create Peer Node Sets** page, enter values for the available input fields.
   The following table describes the fields:

Table 7-226 Create Peer Node Sets Configurations

Field Name	Description
Name	Unique name of the peer node. Example value: `ocs`
Description	Description of the Peer node.
Type	Defines which type of diameter service must be selected. The value is: • tdf
Realm	Enter the realm name, that is, FQDNs to all of that computers that transact diameter traffic. For example,to add the realm detail of the OCS peer, enter `oracle.com`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-226 (Cont.) Create Peer Node Sets Configurations

Field Name	Description
Primary Server	The primary server for a TDF client.
Secondary Server	The secondary server for a TDF client.
Tertiary Server	The teritiary server for a TDF client.
Quaternary Server	The quatenary server for a TDF client.

> **Note**
>
> While configuring the Primary, Secondary, Tertiary, or Quaternary Server, you must ensure to configure the **Identity** in the **Create Peer Node** page, if the **Type** is set to **tdf**. This allows the corresponding diameter peer node name to appear as a selectable option in the server drop-down list on the **Create Peer Node Sets** page.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Peer Node Sets** page. Use or available in the next column to update or delete the listing.

7.6.5 Diameter Error Configurations

This section describes how to customize the Diameter error codes according to the network requirements using the Diameter Error Codes page.

The **Diameter Error Codes** page on CNC Console allows users to view and edit conditions defined by default for the Policy network function. This page also provides the options to import and export Diameter error codes.

The following table describes the errors supported by Policy in Rx application ID:

Table 7-227 Error Codes and Responses

Condition ID and Name	Error Message	Diameter Error Code/ Experimental Result Code	Application Error Code
Invalid AVP Value	The request contained an AVP with an invalid value in its data portion.	5004	DIAMETER_INVALID_AVP_VALUE
Missing AVP	The request did not contain an AVP that is required by the Command Code definition.	5005	DIAMETER_MISSING_AVP

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-227 (Cont.) Error Codes and Responses

Condition ID and Name	Error Message	Diameter Error Code/ Experimental Result Code	Application Error Code
Unsupported Command Code	The Request contained a Command-Code that the receiver did not recognize or support.	3001	DIAMETER_COMMAND_UNSUPPORTED
Loop Detected	The Request contained a Command-Code that the receiver did not recognize or support.	3005	DIAMETER_LOOP_DETECTED
Invalid Diameter Error	A request was received whose bits in the Diameter header were either set to an invalid combination, or to a value that is inconsistent with the command code definition. **Note:** Strict parsing must be enabled.	3008	DIAMETER_INVALID_HDR_BITS
Invalid AVP Bits	A request was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the AVP definition. **Note:** Strict parsing must be enabled.	3009	DIAMETER_INVALID_AVP_BITS
Unsupported AVP	The peer received a message that contained an AVP that is not recognized or supported and was marked with the Mandatory bit. **Note:** Strict parsing must be enabled.	5001	DIAMETER_AVP_UNSUPPORTED
AVP Occurs Too Many Times	A message was received that included an AVP that appeared more often than permitted in the message definition. **Note:** Strict parsing must be enabled.	5009	DIAMETER_AVP_OCCURS_TOO_MANY_TIMES
Unsupported Version	A request was received, whose version number is unsupported.	5011	DIAMETER_INVALID_AVP_LENGTH

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-227 (Cont.) Error Codes and Responses

Condition ID and Name	Error Message	Diameter Error Code/ Experimental Result Code	Application Error Code
Invalid AVP Length	The request contained an AVP with an invalid length. **Note:** Strict parsing must be enabled.	5014	DIAMETER_INVALID_AVP_LENGTH
IP-CAN Session Not Available	A request is received without associated PDU session for a binding.	5065	IP-CAN_SESSION_NOT_AVAILABLE
Unknown Session ID	A request is received with unknown session ID.	5002	DIAMETER_UNKNOWN_SESSION_ID
Internal Error	An internal failure occurred.	5012	DIAMETER_UNABLE_TO_COMPLY

The following table describes the errors supported by Policy in CapEx application ID:

Table 7-228 Error Codes and Responses

Condition ID and Name	Error Message	Diameter Error Code	Application Error Code
No common security	CER message is received, and there are no common security mechanisms supported between the peers.	5017	DIAMETER_NO_COMMON_SECURITY
No common security	CER message is received, and there are no common applications supported between the peers.	5010	DIAMETER_NO_COMMON_APPLICATION
No common security	Received the diameter request for unsupported application.	3007	ERROR_COND_APPLICATION_UNSUPPORTED

Editing Diameter Error Codes

To edit any of the defined conditions, perform the following steps:

1. From the navigation menu, click **Policy**, then select **Diameter Configurations**, and click **Diameter Error Codes**.
   This opens the Diameter Error Codes page that lists the **CapEx** and **Rx** application ID.
2. Click **Edit** against the application ID that you need to customize.
   This opens the Edit Diameter Error Codes page for the selected application ID.
3. Update the required values for the fields as described in the following table:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-229 Parameters for Edit Diameter Error Codes

Parameter	Description	Applicable for
Condition Name	Specifies the description for a defined condition. It is recommended to use descriptions that clearly explain the condition.	Rx and CapEx
Result Code	Specifes the Diameter result code for a defined condition. When Use Experimental Result switch is disabled, this field cannot be left blank. **Note:** The value must be a standard diameter result code as defined in the RFC 6733.	Rx and CapEx
Use Experimental Result	Indicates whether to use the Result Code AVP (268) or Experimental Result AVP (297) when an error result is generated by Policy.	
Vendor ID	Specifies the Vendor ID of the operator or governing body that manages the code entered by the user in the **Experimental Result Code** field. When **Use Experimental Result** switch is enabled, this field cannot be left blank.	Rx
Experimental Error Code	Specifies the custom Diameter result code for a defined condition. When Use Experimental Result switch is enabled, this field cannot be left blank. **Note:** The value must be a standard diameter result code, from 3000 to 9999, as defined in the 3GPP Technical Specification 29.230.	Rx
Error Message	A message that explains the nature of the error. This error message is only for user understanding and must not be parsed by network entities.	Rx and CapEx

Use  available under the **Actions** column to update the error code.

4. Click **Save**.

Unsupported Diameter Error Codes

The following table describes the Diameter Error Codes that are not supported while configuring the Diameter Error codes feature:

Table 7-230 Unsupported Diameter Error Codes

Status Code	Description
3006	DIAMETER_REDIRECT_INDICATION
3010	DIAMETER_UNKNOWN_PEER
4001	DIAMETER_AUTHENTICATION_REJECTED
4002	DIAMETER_OUT_OF_SPACE
4003	ELECTION_LOST
5006	DIAMETER_RESOURCES_EXCEEDED
5007	DIAMETER_CONTRADICTING_AVPS
5013	DIAMETER_INVALID_BIT_IN_HEADER
5015	DIAMETER_INVALID_MESSAGE_LENGTH
5016	DIAMETER_INVALID_AVP_BIT_COMBO
5061	INVALID_SERVICE_INFORMATION

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-230 (Cont.) Unsupported Diameter Error Codes

Status Code	Description
5062	FILTER_RESTRICTIONS
5063	REQUESTED_SERVICE_NOT_AUTHORIZED
5064	DUPLICATED_AF_SESSION
5066	UNAUTHORIZED_NON_EMERGENCY_SESSION
5067	UNAUTHORIZED_SPONSORED_DATA_CONNECTIVITY
5068	TEMPORARY_NETWORK_FAILURE
5198	DIAMETER_OVERLOAD_RETRY_NOT_ALLOWED_TO_ANY
5199	DIAMETER_NEWER_SESSION_DETECTED
5999	ALLOWED_SERVICE_NO_POLICIES_REQUIRED
5003	DIAMETER_AUTHORIZATION_REJECTED
3003	DIAMETER_REALM_NOT_SERVED

7.6.6 Diameter Repaving

The **Diameter Repaving** page displays the configurations related to Diameter Gateway connection repaving. The page allows you to edit the configurations.

To edit Diameter Repaving:

1. From the navigation menu, under **Policy**, click **Diameter Configurations** and select **Diameter Repaving**.
   This opens the **Diameter Repaving** page. The page displays the existing Diameter Gateway connection repaving feature configuration.
2. To enable or disable the feature, configure **Enable Diameter Repaving** flag under **Feature Configuration** section.
3. Click **Trigger Disconnection** under **Diameter Repaving Trigger** section to disconnect the existing external Diameter connections established before the trigger timestamp.
4. The **Disconnection Trigger History** section displays the disconnection history, if any.

7.7 Data Source Configurations

Policy establishes connections with data sources to retrieve information about subscribers from the database. It queries a data source using a key attribute that uniquely identifies a subscriber and stores the results in the cache. A data source uses this key attribute, such as the phone or account number of the subscriber to index the information available in the database.

This section describes how to manage and view the Policy datasource configurations in Policy, using the **Data Source Configurations** pages.

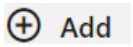
7.7.1 Data Sources

This procedure provides information about how to configure and manage the Policy data sources.

The **Data Sources** page allows you to create new and manage existing data sources. The page displays the list of defined data source configurations and provides the options to import, export, or add configurations.

Copyright © 2019, 2026, Oracle and/or its affiliates.

To configure data source:

1. From the navigation menu under **Policy**, navigate to **Data Source Configurations**, and select **Data Sources**.
   This opens the **Data Sources** page. The page lists the existing data source configurations. You can add new data sources using this page.
2. Click 

   .
   This opens the **Create Data Source** page.
3. On the **Create Data Source** page, enter the information specific to the available groups:

Table 7-231 Create Data Source Configuration

Field Name	Description
Name	Specifies the name of the data source. Example value: `ocs`
Description	Specifies additional information about the data source.
Type	Specifies the type of data source. Users can select any of the following valid values from the drop-down menu: • **LDAP** • **Sy** If LDAP data source is selected then see the "Setting Up LDAP as Policy Data Source" section. If Sy data source is selected then see the "Setting Up OCS as Policy Data Source" section.

4. Click **Save**.
   The Data source gets listed on the **Data Sources** page.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the data source configuration.

Setting up LDAP as Policy Data Source

To set LDAP as the data source:

1. On the **Create Data Source** page, in the **Type** drop-down list, select `LDAP`.
2. Following fields will become available on selecting LDAP as data source `Type`:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-232 Create LDAP Data Source Configuration

Field Name	Description
Read Connection	It is used to specify the number of read connections established with the data source. **Note:** For configuring the value of **Read Connection** as more than 1, contact My Oracle Support (https://support.oracle.com). **Note:** If the number of read connections is increased for the LDAP data source, it is recommended to decrease the keep-alive value to prevent frequent connection losses
Timeout value (in ms)	Specifies the LDAP request timeout value. Default value: 3000 **Note:** Setting it to more than 3000 millisecond needs update in helm env configuration PDS_RESPONSE_TIMEOUT.
Retry Enabled	Toggle button to enable LDAP retry functionality.
Max number of retries	Specifies the maximum number of retries. **Note:** The retry limit must be set as 1, irrespective of the number of configured servers.
Retries on errors/timeout	Specifies the list of error codes for retry. **Note:** The timeout error code is 85 and connection related error code is 91.
Primary Server:	The primary data source server details.
Identity	Primary LDAP server name.
Addr	FQDN/IP Address of LDAP server
Port	Primary server Port.
Secondary Server	The secondary data source server details. If primary server is not reachable, then data source connection is established with secondary (if available). You can add or remove the secondary data source server.
Identity	Secondary LDAP server name.
Addr	FQDN/IP Address of LDAP server
Port	Secondary server Port.
Tertiary Server	The tertiary data source server details. If primary and secondary are not reachable, then LDAP connection is established with tertiary (if available). You can add or remove the tertiary data source server.
Identity	Tertiary LDAP server name.
Addr	FQDN/IP Address of LDAP server
Port	Tertiary server Port.

Copyright © 2019, 2026, Oracle and/or its affiliates.

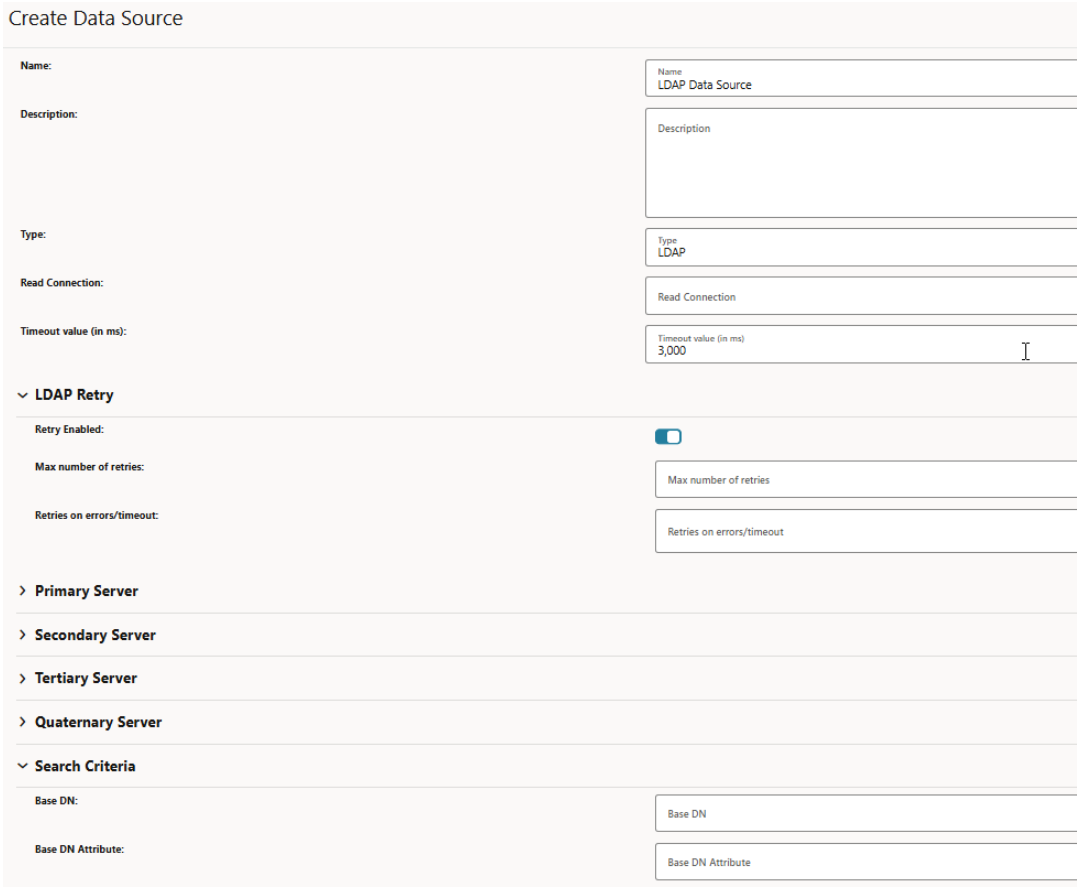
Table 7-232 (Cont.) Create LDAP Data Source Configuration

Field Name	Description
Quaternary Server	Quaternary data source server. You can add or remove the quaternary data source server. **Note** We do not support Quaternary server for LDAP datasource in LDAP Gateway.
Identity	Quaternary LDAP server name.
Addr	FQDN/IP Address of LDAP server
Port	Quaternary server Port.
Search Criteria	The criteria on which the data source search is performed. You can add or remove the Search Criteria settings.
Base DN	
Base DN Attribute	

3. Enter the **Primary Server** configurations.
The following screen capture shows an example on how to create LDAP data source with name **LDAP1**:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-38 LDAP Configuration using Edit Data Sources Page



4. Click **Save**.
   This creates the LDAP1 data source.

> **Note**
>
> If the LDAP data source lookup is configured to search with a specific Subscriber ID Type (such as MSISDN/GPSI), there is currently no fallback option to use an alternative Subscriber ID Type (like IMSI/SUPI) in case the initial lookup fails.

Setting Up OCS as Policy Data Source

To set OCS as the data source, perform the following steps:

1. On the **Create Data Source** page, in the **Type** drop-down list, select Sy.
2. Following fields will become available on selecting Sy as data sourceType:

Table 7-233 Create Sy Data Source Configuration

Field Name	Description
admin state	Enable this switch for data source (Sy) interaction to happen. When the admin state switch is disabled, the data source becomes unavailable temporarily.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-233 (Cont.) Create Sy Data Source Configuration

Field Name	Description
Realm	Specifies the realm of the primary and optional secondary servers to connect. In case of Sy data sources, the `DestinationRealm AVP` in request message to Diameter Gateway is set using this value.
Select OCS from Peer Configurations	When this switch is enabled, the user can configure primary, secondary, tertiary and quaternary servers by selecting diameter peer nodes using the drop-down menu. For the peer nodes to be made available while configuring a data source, the user must have performed the configurations on Peer Nodes page under **Diameter Configurations**.
Primary Server:	The primary data source server details.
Identity	Primary server identity. Example value: `oc-diam-gateway`
Addr	Load balancer IP of Diameter gateway.
Port	Primary server Port.
Secondary Server	The secondary data source server details. If primary server is not reachable, then data source connection is established with secondary (if available). You can add or remove the secondary data source server.
Identity	Secondary server identity. Example value: `oc-diam-gateway`
Addr	Load balancer IP of Diameter gateway.
Port	Secondary server Port.
Tertiary Server	The tertiary data source server details. Tertiary data source server. If primary and secondary are not reachable, then LDAP connection is established with tertiary (if available). You can add or remove the tertiary data source server.
Identity	Tertiary server identity.
Addr	Load balancer IP of Diameter gateway.
Port	Tertiary server Port.
Quaternary Server	Quaternary data source server. If primary, secondary and tertiary are not reachable then LDAP connection is established with tertiary (if available). You can add or remove the quaternary data source server.
Identity	Quaternary server identity.
Addr	Load balancer IP of Diameter gateway.
Port	Quaternary server Port.
Search Criteria	The criteria on which the data source search is performed. You can add or remove the Search Criteria settings.

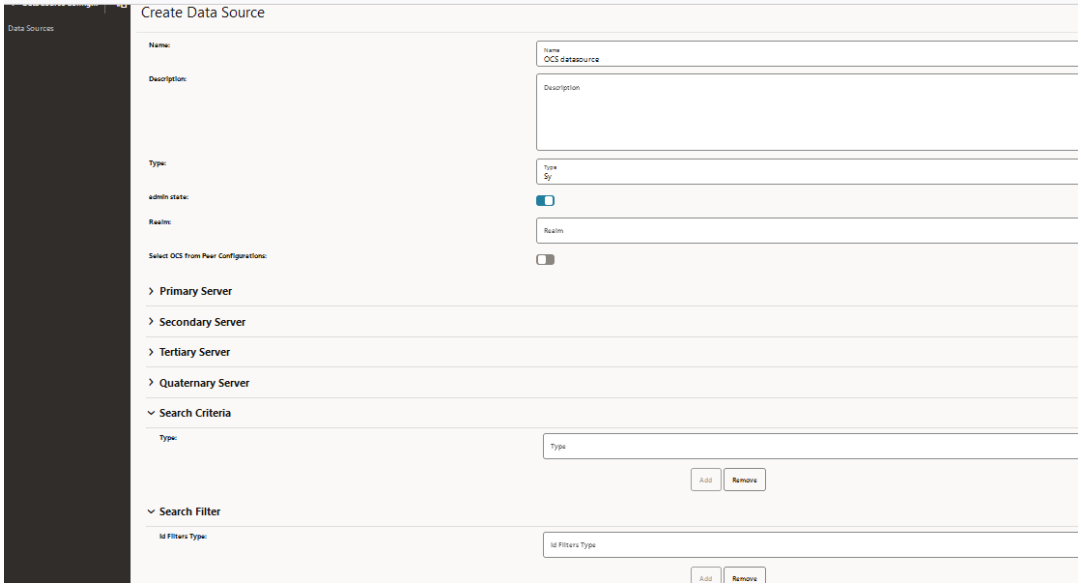
Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-233 (Cont.) Create Sy Data Source Configuration

Field Name	Description
Type	Users can select any of the following valid values from the drop-down menu: • NAI • MSISDN • IMSI
Search Filter	The search filter during the data source search. You can add or remove the **Search Filter** settings.
Id Filters Type	Users can select any of the following valid values from the drop-down menu: • NAI • MSISDN • IMSI

3. Select the **Primary Server** using the drop-down menu. The peer nodes are configured using the Peer Nodes page under **Diameter Configurations**.
   The following screen capture shows an example on how to create OCS data source with name **OCS datasource**:

Figure 7-39 OCS Configuration using Edit Data Sources Page



4. Click **Save**.
   This creates the `OCS datasource` .

7.8 Administration

This section describes how to perform administration tasks, such as bulk import and bulk export of configurable objects into the Policy system.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.8.1 Export & Import

This section describes how to perform the bulk export or bulk import of the managed objects (MOs) configured on Policy.

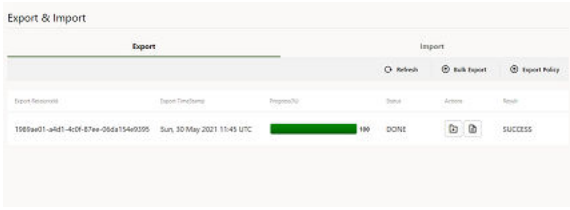
You can perform the bulk export and import of Policy data using the following methods:

- **Using CNC Console for Policy**:
  Policy provides the GUI to perform bulk export and import of Policy data.

  To access the export and import functionality from the CNC Console home page, expand **Policy**, navigate to **Administration**, and select **Export & Import**.

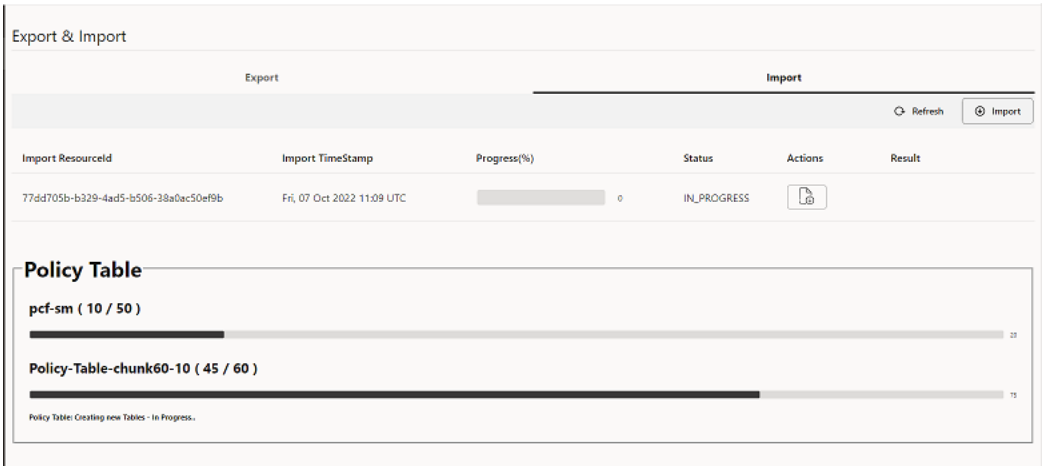
  The page displays the **Export** and **Import** tabs. By default, the **Export** tab remains selected. The following screen capture illustrates an example of the **Export & Import** page:

Figure 7-40 Export and Import



On initiating either bulk import or export for managed objects (MO's), a detailed progress information is displayed in the UI. Information like managed object type being imported or exported, total number of processes or tables, current number of managed object type being processed, managed object name like table name or rule name, number of records processed for managed Object, total number of managed object records present and progress messages. The following screen capture illustrates an example of the **Export & Import** page with detailed progress description:

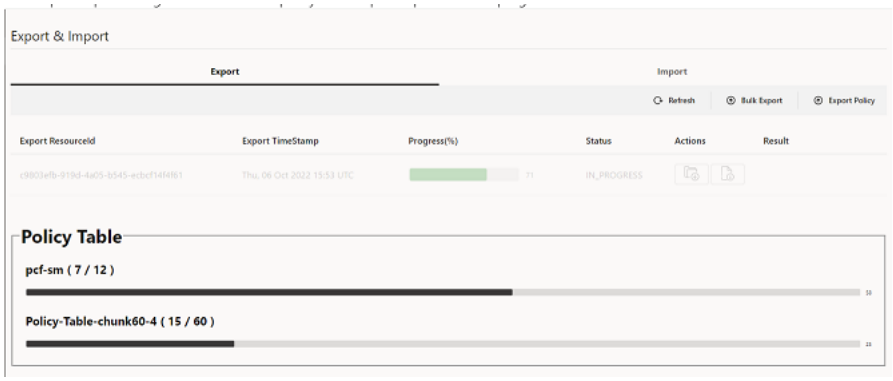
Figure 7-41 Import showing Managed Object count progress status



Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> – Importing the Overload Threshold Profile will be rejected if the CPU validation mentioned under `Configure Threshold Values` section in Overload Control Threshold fails for any of the three threshold levels.
> – The service names mentioned in the json file used to import the Overload Threshold Profile must be same as mentioned in the exported json file.
> – The default Overload Threshold Profile cannot be exported or imported. The default Overload Threshold Profile must be customized with a different profile name before exporting.

Figure 7-42 Export showing Managed Object count progress status



> **Note**
>
> Currently this detailed progress information display is supported for export/import of records from Policy Table MO only.

You can perform the following operations using the **Export & Import** page:

– Exporting Policy Data
– Importing Policy Data

> **Note**
>
> The following message priority data that was exported prior to Policy 23.2.0 cannot be imported as the data may be corrupt:
>
> – message containing Sd as interface
> – Sy-SLR as condition message
>
> The data with Sd interface or Sy-SLR condition messages that are exported only with Policy 23.2.0 or later versions can be imported.

- **Using REST API for Policy**:
  Policy provides REST APIs to bulk export and import of Policy data. For more information about REST API configuration, see Using REST API for Policy Export & Import.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.8.1.1 Exporting Policy Data

The export functionality allows you to export Policy configurations and Policy Projects with the respective dependencies. You can use the export functionality to perform the following operations:

- Exporting Policy Configurations with Dependencies
- Exporting Policy Projects with Dependencies

The Policy data export is aligned with the left navigation menu options under **Policy**, on the CNC Console. You can export either all the configurations or the configurations of the selected menu options.

To export the policy configuration data:

1. From **Policy**, navigate to **Administration** and select **Export & Import**.

   This opens the **Export & Import** page, displaying the **Export** and **Import** tabs. By default, the **Export** tab remains selected.

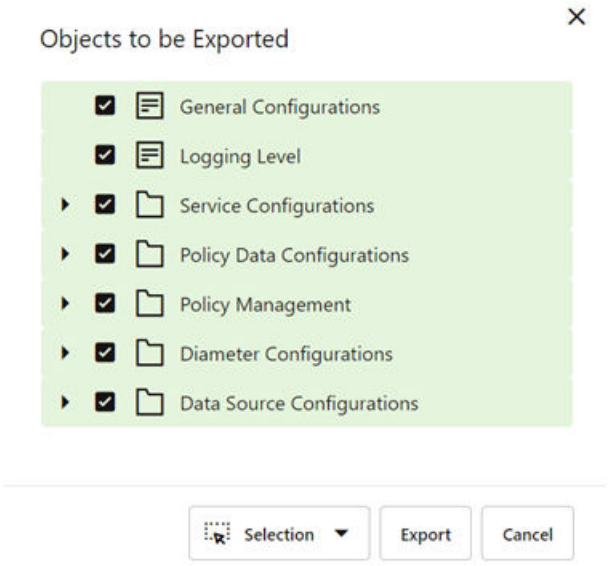
2. **Note**

   When new policy deployment is installed, before clicking the **Bulk Export** button User need to navigate to **Policy -> Service Configuration -> PCF Session Management** section. Here, click edit and then save in order to save the session management configuration and avoid PARTIAL_SUCCESS in Bulk Export.

   Click Bulk Export .

   This opens the **Objects to be Exported** dialog box, displaying the list of Policy configurations in a menu tree structure. The dialog box allows you to select the configurations to be exported. The following screen capture displays an illustration of the **Objects to be Exported** dialog box:

Figure 7-43 Objects to be Exported dialog box



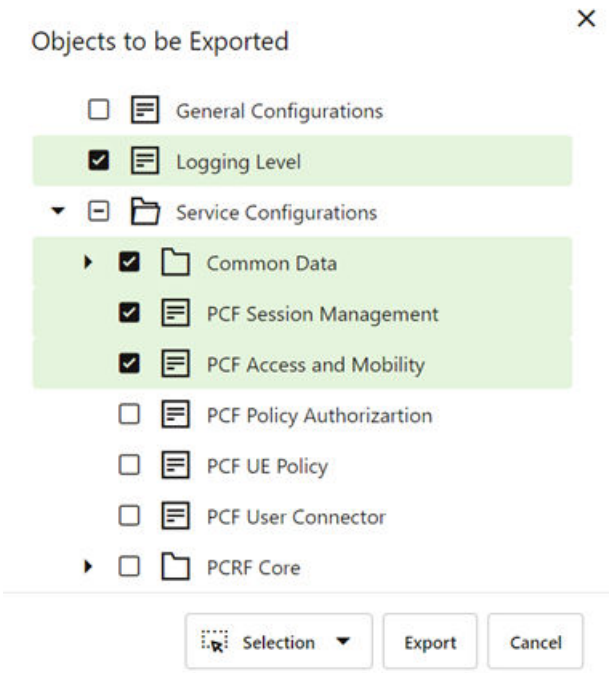
Copyright © 2019, 2026, Oracle and/or its affiliates.

By default, the **Objects to be Exported** dialog box has all the configurations selected for export. You can deselect the configurations.

3. In the dialog box, select or deselect the configurations according to the export requirement.

   Selecting or deselecting a parent folder, automatically selects or deselects all the child nodes respectively. In case a folder is selected partially, then a partial selection sign is displayed on the parent folder as shown in the following illustration:

Figure 7-44 Objects to be Exported dialog box with selected configurations



> **Note**
>
> To select or deselect all the configurations, click **Selection** and perform the required operation.

4. Click **Export**.

> **Note**
>
> Click **Cancel** to discard the export operation.

> **Note**
>
> Exported data is only available at the time of the operation. Subsequent exports with configuration changes will overwrite the previous export.

Copyright © 2019, 2026, Oracle and/or its affiliates.

This starts the export of all the configurations related to the selected MOs. A row is created in the export status table on the **Export & Import** page, displaying the export status with the following details:

- **Export ResourceId**: A new export resource ID is generated for each export operation. You can use this ID to get the export status.
- **Creation TimeStamp**: The timestamp of generation of **Export ResourceId**.
- **Progress (%)**: Shows the export progress in form of a percentage bar. The page auto refreshes the status, until the progress reaches 100 percent.
- **Status**: The status of the export operation. The status can be any of the following:
  - **INIT**: The validation of policies is in progress and the export of the MOs is not yet started.
  - **IN_PROGRESS**: The export is running.
  - **DONE**: The export is complete.
- **Actions**: Provides the buttons to download the following:
  - **Export configuration files in ZIP file format**: The exported configurations in ZIP file format. The ZIP file contains the MO data in JSON file format. You can download the exported data by clicking  under the **Action** column.
  - **Export report in TEXT file format**: The export report provides results for each JSON file present in the exported ZIP file. It also provides the reason for failure, in case the export of any of the configuration fails.

    You can download the export report by clicking  under the **Action** column.

    > **Note**
    >
    > The buttons remain enabled only for the export operation with **DONE** status.

- **Result**: Provides the result of an export operation. This result is available only for the export operations with **DONE** status. Following are the possible values:
  - **SUCCESS** : The export is successful
  - **FAILED** : The export is failed
  - **PARTIAL_SUCCESS** : The export is partially successful

Exporting Policy Projects with Dependencies

The Policy data export functionality explained in the above section allows you to export all the policy configurations with their dependencies. However, it does not export the dependencies of the selected Policy Projects.
The **Export & Import** page provides an option to export only the Policy Projects and Policies with their dependencies, without any MO configurations. The Policy Projects export is aligned with Policy services. You can export either all the Policy Projects or the projects of the selected services.

To export Policy Projects with dependencies:

5. On the **Export & Import** page, click 

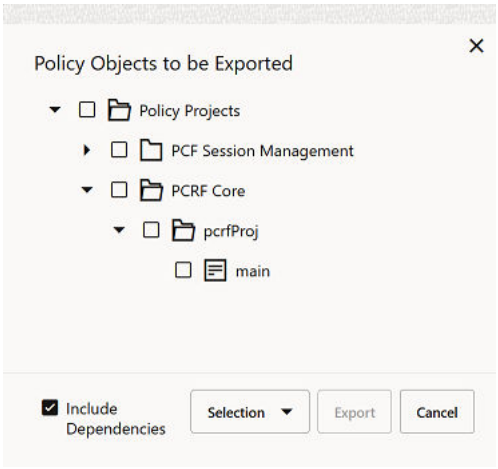
.

   This opens the **Objects to be Exported** dialog box, displaying the list of Policy Projects for each service. The dialog box allows you to select the Policy Projects to be exported with

Copyright © 2019, 2026, Oracle and/or its affiliates.

an option to include dependencies. The following screen capture displays an illustration of the **Objects to be Exported** dialog box:

Figure 7-45 Objects to be Exported dialog box for Exporting Policies



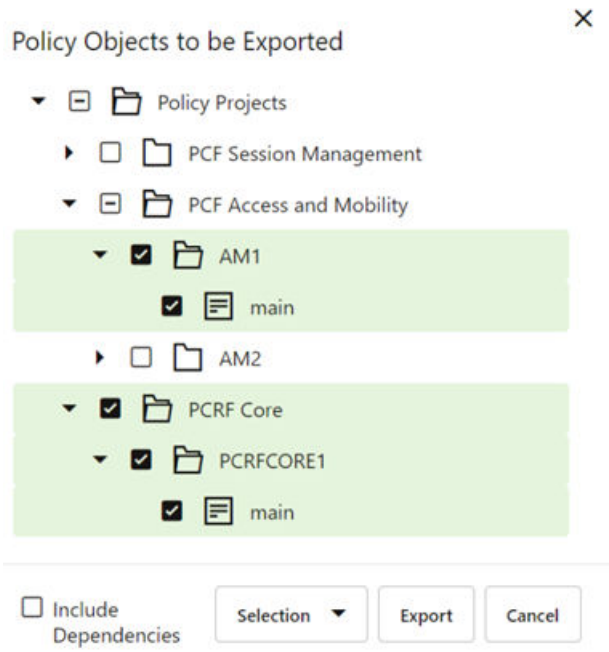
> **Note**
>
> Prior releases to Policy 23.1.0, Exporting of Managed objects and its dependencies is not supported for PCRF-CORE and PDS Services, this warning message "**Include Dependencies are not supported for PCRF-CORE & PDS Services**" is displayed.

6. In the dialog box, select the configurations that needs to be exported.

   Selecting a parent folder automatically selects all the child nodes. In case a folder is selected partially, then a partial selection sign is displayed on the parent folder as shown in the following illustration:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-46 Objects to be Exported with Selected Policy Projects



> **Note**
>
> To select or deselect all the configurations, click **Selection** and perform the required operation.

7. Select the **Include Dependencies** check box to export all the dependent MOs of the selected policies.

   If you do not select the check box, then no dependent MOs for the selected policies get exported. It exports the single Policy Project ZIP file.

> **Note**
>
> The **Include Dependencies** functionality is not applicable for the PCRF Core and PDS services.

8. Click **Export**.

> **Note**
>
> Click **Cancel** to discard the export operation.

This starts the export of all the configurations related to the selected Policy Projects. A row is created in the export status table on the **Export & Import** page, displaying the export status with the following details:

- **Export ResourceId**: A new export resource ID is generated for each export operation. You can use this ID to get the export status.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **Creation TimeStamp**: The timestamp of generation of **Export ResourceId**.
- **Progress (%)**: Shows the export progress in form of the percentage bar. The page auto refreshes the status until the progress reaches 100 percent.
- **Status**: The status of the export operation. The status can be any of the following:
  - **INIT**: The validation of policies is in progress and the export of the MOs is not yet started.
  - **IN PROGRESS**: The export is running.
  - **DONE**: The export is complete.
  - **FAILED** : The export is complete but errors exist in all the exported policies.
- **Actions**: Provides the buttons to download the following:
  - **Export configuration files in ZIP file format**: The exported configurations in ZIP file format. The ZIP file contains the MO data in JSON file format. You can download the exported data by clicking  under the **Action** column.

    > **Note**
    >
    > If you have not selected the **Include Dependencies** check box, then the exported Zip file contains only single JSON file named PolicyProjects.json.

  - **Export report in TEXT file format**: The export report provides results for each JSON file present in the exported ZIP file. It also provides the reason for failure, in case the export of any of the configuration fails.

    You can download the export report by clicking  under the **Action** column.

    > **Note**
    >
    > The buttons remain enabled only for the export operation with **DONE** status.

- **Result**: Provides the result of an export operation. This result is available only for the operations with **DONE** status. Following are the possible value:
  - **SUCCESS** : The export is successful
  - **FAILED** : The export is failed.
  - **PARTIAL_SUCCESS** : The export is partially successful

7.8.1.2 Importing Policy Data

The import functionality allows you to import Policy data configurations. Using this functionality, you can import the same set of policy data to different PCF systems.
To import Policy data from user provided ZIP file format:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

- The ZIP file must contain only JSON files and each JSON file must contain unique values and must not include duplicate entries.
- Importing configuration data exported from release N into any older release (for example, N-1, N-2, and earlier) is not supported.
- Do not attempt this downgrade import path, as it may lead to import failures or inconsistent configuration state.

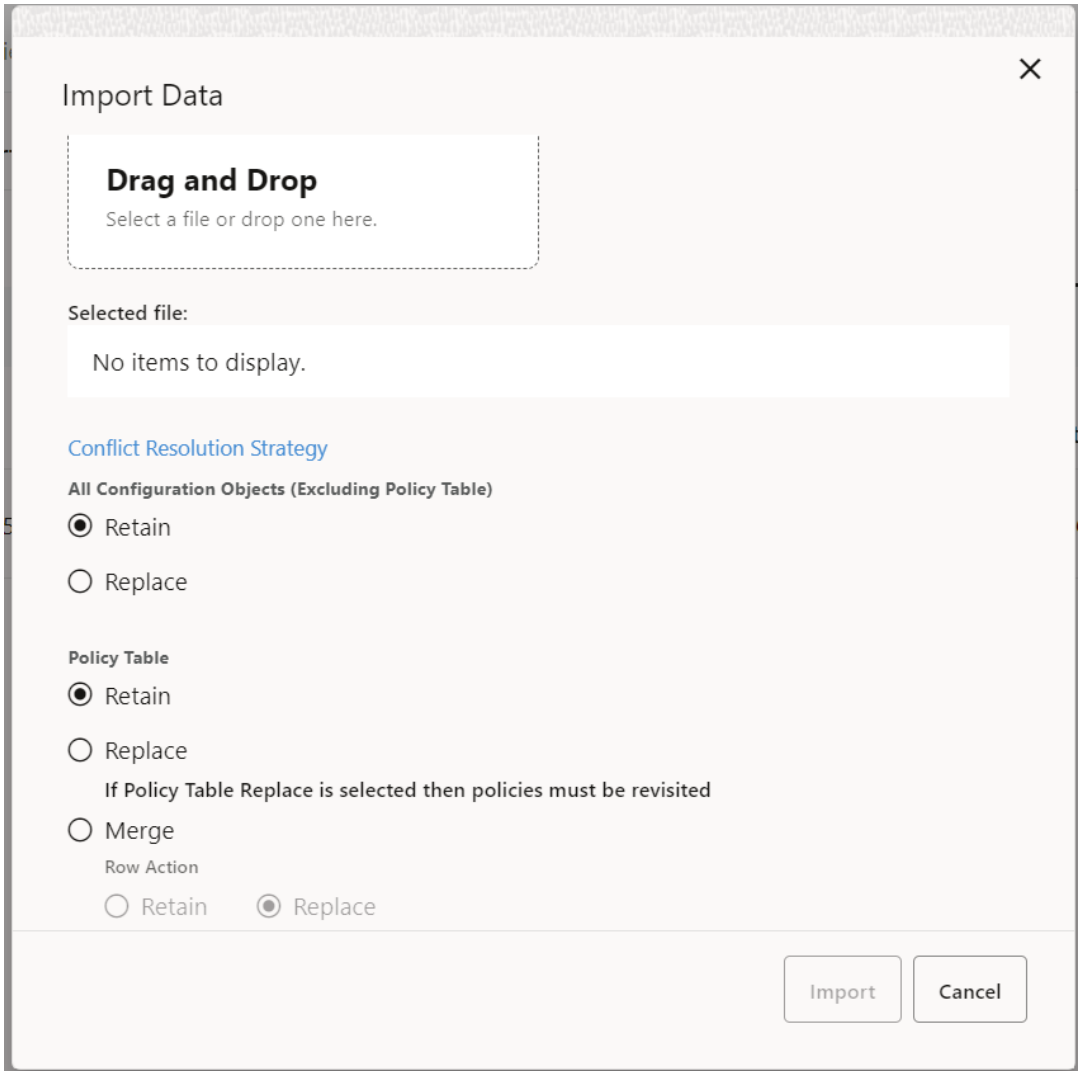
1. From **Policy**, navigate to **Administration** and select **Export & Import**.

   This opens the **Export & Import** page, displaying the **Export** and **Import** tabs. By default, the **Export** tab remains selected.

2. Select the **Import** tab and click Import .

   This opens the **Import Data** dialog box.

Figure 7-47 Import Data



Copyright © 2019, 2026, Oracle and/or its affiliates.

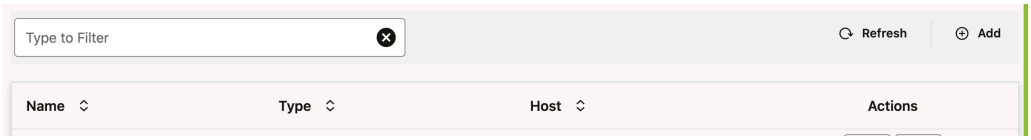
3. Upload the file in ZIP format by using the **Drag and Drop** button.

> **Note**
>
> You can not select the managed objects in the **Import Data** dialog box in Release 1.8.x.

4. Select any of the following options under **Conflict Resolution Strategy**.
   - **Attribute Configurations Screens**:

> **Note**
>
> This option is applicable to all the attribute configuration screens such as **Data Sources** under **Data Source Configurations** or **Subscriber Activity Logging** under **Logging Configurations** which have Add button at the top right corner along with a table. In such screens each row is considered as managed object.

Figure 7-48 Sample Attribute Configurations Screen



Conflict resolution:

- **Retain** : Ignores records already present in the database and does not overwrite. For each object in the import file, if the object already exists in the system, the import does not update the object with the configurations provided in the import file. If an object does not exists, then it is added to the system.
- **Replace** : For each object in the import file, if the object already exists in the system, the import replaces the object with the configuration provided in the import file. If an object does not exist, then it is added to the system.
  If an object existing in the system and is not present in the imported file, it is retained in the system.

   - **Service Configuration Screens**:

> **Note**
>
> - This option is applicable to all the service configuration screens such as **Session Management** under **Service Configurations** or **Settings** under **Diameter Configurations**, which have Edit button at the top right corner along with a table.
> - After fresh installation, the default GUI configurations are not persisted or exportable until each service configuration is explicitly saved at least once.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-49 Sample Service Configurations Screen

Conflict resolution:

- **Retain** : Ignores the records and data which are getting imported. For each object in the import file, the imported record will be ignored.
- **Replace**: For each object in the import file, data to be imported will overwrites the existing data in the database, irrespective of whether the object is already present in the database or not.

5. Click **Import**.

> **Note**
>
> Click **Cancel** to discard the import operation.

This starts the import of configuration objects and their settings to the database. A row is created in the Import status table, displaying the import status with the following additional details:

- **Import ResourceId**: A new import resource ID is generated for each import operation. You can use this ID to get the import status.
- **Creation TimeStamp**: The timestamp of generation of **Import ResourceId**.
- **Progress (%)**: Shows the import progress in form of the percentage bar. The page auto refreshes the status until the progress reaches 100 percent.
- **Status**: The status of the import operation. The status can be any of the following:
  - **IN_PROGRESS**: The import is running.
  - **DONE**: The import is complete.
- **Actions**: Provides a button to download the import report in text format. This button gets enabled, once the status is **DONE**. The report provides results for each JSON file present in the imported ZIP file. You can download the import report by clicking under the **Action** column.
- **Result**: Provides the result of an import operation. This result is available only for the operations with **DONE** status. Following are the possible value:
  - **SUCCESS** : The import is successful
  - **FAILED** : The import is failed
  - **PARTIAL_SUCCESS** : The import is partially successful

When importing Policy data exported from 23.x release into 25.x release, the following error may be displayed in the import report if the 23.x export contains congestion-type Load Shedding Profiles: **`congestion load shedding profile with name <profile_name> not found`**.
This error is expected because of the compatibility change between 23.x and 25.x. In 25.x, the **Congestion Control** option is removed for **Load Shedding Profiles**. See Load

Copyright © 2019, 2026, Oracle and/or its affiliates.

Shedding Profiles for more information. Complete the import operation and then perform the following steps:

a. Note the impacted profile names from the error messages.

b. Recreate the impacted Load Shedding Profiles in the 25.x GUI with Type set to Overload Control.

7.8.1.3 Using REST API for Policy Export & Import

Policy provides an option to perform the bulk export or import of Policy configurations and Policy Data using REST APIs. For more information about Bulk Import REST APIs, see "Bulk Import Export Controller" in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.

7.9 Status and Query

This section describes how to retrieve status of Policy profile registration and query sessions using the Session Viewer page.

7.9.1 Session Viewer

The **Session Viewer** page displays the detailed session information of subscribers. You can use this page to enter query parameters to render session data for specific subscribers.

This procedure provides information about how to view session details and perform different operations for a single, multiple, or all subscribers of a specific session type.

To view a session:

1. From the navigation menu, click **Policy**, select **Status and Query**, and then click **Session Viewer**.
   This opens the Session Viewer page.
2. Select the session type for which you want to view the subscriber details. Select any of the following services from the **Session Type** drop-down list:
   - SM Policy Association
   - AM Policy Association
   - PA Policy Association
   - SM TDF Session
   - PCRF-Core Session
   - Binding Data
   - User Data
   - UE Policy Association
   - Usage Monitoring
   - ALL
3. From the **Identifier Type** drop-down menu, select the required identifier type.
   The following table lists the identifier types supported for each session type:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-234 Supported values for Identifier type

Session Type	Identifier Type
SM Policy Association	• SUPI • GPSI • IPV4 • IPV6 • POLICY_ASSOC_ID **Note**: SM Data when fetched includes `tdfSessionId`. SM data is lazily purged. If TDF session is not created or deleted for some reason, `SMPolicyAssociation` will not be updated to remove the `tdfSessionId`. The `tdfSessionId` will be removed only during SM Update or SM Notify.
AM Policy Association	• SUPI • GPSI • POLICY_ASSOC_ID • PEI
PA Policy Association	• SUPI • GPSI • IPV4 • IPV6 • POLICY_ASSOC_ID
SM_TDF_Session	• SUPI • GPSI • IPV4 • IPV6 • TDF_SESSION_ID • TDF_DIAMETER_SESSION_ID
PCRF-Core Session	• DIAMETER_SESSION_ID • IMSI • MSISDN • IPV4 • IPV6 **Note:** For the `PCRF-Core Session` type, the page displays the **Session Subtype** dropdown containing the session type that can be used. The dropdown values depends on the **Identifier Type** value. For more details of the Session Subtype field, see Step 4.
Binding Session	• SUPI • GPSI • IPV4 • IPV6 • POLICY_ASSOC_ID • MAC
User Data	• SUPI • GPSI

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-234 (Cont.) Supported values for Identifier type

Session Type	Identifier Type
UE Policy Association	• SUPI • GPSI • PEI • POLICY_ASSOC_ID
Usage Monitoring	• SUPI • GPSI
ALL	• SUPI • GPSI **Note**: On selecting ALL as the session type, the following sessions are impacted: • SM session • PA session • UE session • AM session • Binding session • Diameter session • Usage Monitoring

Here are the regex patterns for the accepted values of each identifier type:

- SUPI: "^(?!imsi-0{5,15}$)(imsi-[0-9]{5,15}|nai-.+|gci-.+|gli-.+)$"
- GPSI: "^(msisdn-[0-9]{5,15}|extid-[^@]+@[^@]+|(?!(msisdn-|extid-)).+)$"
- DIAMETER_SESSION_ID: No validation needed, free-form strings to be accepted
- POLICY_ASSOCIATION_ID: No validation needed, free-form strings to be accepted
- IMSI: "^[0-9]{5,15}$"
- MSISDN: "^[0-9]{5,15}$"
- IPV4: "^(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\\.){3}([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])$"
- IPV6: "^((:|(0?|([1-9a-f][0-9a-f]{0,3})):)((0?|([1-9a-f][0-9a-f]{0,3})):){0,6}(:|(0?|([1-9a-f][0-9a-f]{0,3})))(\V(([0-9])|([0-9]{2})|(1[0-1][0-9])|(12[0-8])))$"
- MAC: "^([0-9a-fA-F]{2})((-[0-9a-fA-F]{2}){5})$"
- PEI: "^(imei-[0-9]{15}|imeisv-[0-9]{16}|.+)$"

> **Note**
>
> When attempting to retrieve PA or TDF sessions using SUPI, GPSI, IPv4, or IPv6, it is important to note that these sessions will only be accessible if a corresponding parent session (SM session) exists. However, child sessions can be directly retrieved by providing specific session IDs: POLICY_ASSOC_ID for PA Policy Association, and TDF_DIAMETER_SESSION_ID and/or TDF_SESSION_ID for SM_TDF_Session.

4. <*Optional*> In case of **PCRF-Core Session** type, the page displays the **Session Subtype** dropdown containing the session type that can be used. The dropdown values depends on the **Identifier Type** value.
   The following table lists the session subtypes supported for different identifier types:

Copyright © 2019, 2026, Oracle and/or its affiliates.

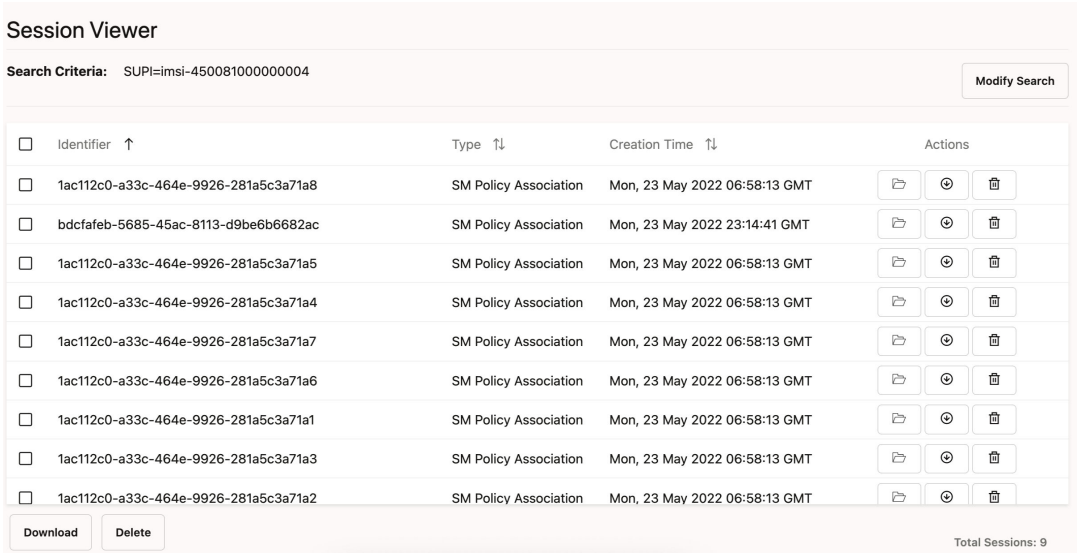
Table 7-235 Supported values for Identifier type

Session Type	Identifier Type
• IMSI • MSISDN • IPV4 • IPV6	• All sessions • Gx Session • Rx Session • Sd Session
DIAMETER_SESSION_ID	• Gx Session • Rx Session • Sd Session

5. Enter the value in the **Identifier Value** field for the selected identifier type.
   For more information on identifier values, see Subscriber Identifiers in Subscriber Activity Logging.
6. Enable the **User Data** switch to get the user data from the Policy directory.
7. Click the **Query** button.
   The page displays the subscriber information according to the selected session type.

   The following image displays the query results for session type as `SM Policy Association` with `SUPI` as the identifier type:

Figure 7-50 Query Results on Session Viewer



The query results are displayed in tabular form with each row displaying the following details:

- **Identifier:** The selected session identifier.
- **Type:** Type of the session.
- **Creation Time:** The session creation time.
- **Action:** Provides the buttons to perform the following actions:
  - **View Session Details:** Click the



Copyright © 2019, 2026, Oracle and/or its affiliates.

icon to view the selected session details in the JSON editor.

– **Download Session Details:** Click the



icon to download the selected file containing the details of the session on your system.

> **Note**
>
> To download multiple session files in single instance, select the sessions and click the **Download** button at the bottom of the page.

– **Delete Sessions:** Click the



icon to delete the selected session manually.

> **Note**
>
> * To delete multiple sessions in a single instance, select the sessions and click the **Delete** button at the bottom of the page.
> * For remote delete, enable
>
> 
>
>
> box. When this option is enabled, Policy sends delete subscriptions to remote NFs when any previous subscriptions are enabled with remote NFs.
>
> > **Note**
> >
> > **Initiate Remote Session Cleanup** is applicable only for SM Service.
> >
> > In case of AM_Policy_Association and UE_Policy_Association, when a session is deleted, the corresponding context information in PDS is cleaned. If all the PDS context for UDR data are deleted, the subscription data in the UDR is also deleted.

> **Note**
>
> Use the **Modify Search** button to modify the search criteria.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Policy also provides an option to configure session viewer using REST APIs. For more information, see "Session Viewer" in *Cloud Native Core, Converged Policy REST Specification Guide*.

7.9.2 NF Data

This section provides information on NF data.

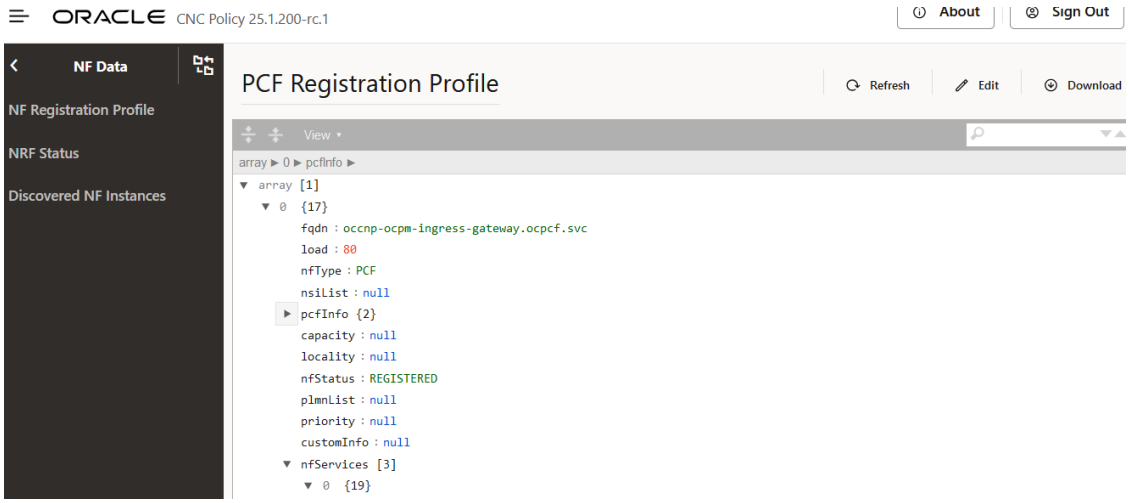
7.9.2.1 PCF Registration Profile

This page lists the PCF profile registered with NRF.

To make updates to any of the parameters of the PCF registration profile, perform the following steps:

1. From the navigation menu, click **Policy**, select **Status and Query**, then click **NF Data**, and then click **NF Registration Profile**.
   This opens the PCF Registration Profile page.
2. Click **Edit** button.
3. Update the values of the required parameters.
4. Click **Save**.

Figure 7-51 PCF Registration Profile



To download the PCF profile, click **Download** button. A file named `pcfRegistrationProfile.json` is saved on your system.

7.9.2.2 NRF Status

On the NRF Status page, you can view the status of PCF and the NRFs deployed in the cluster.

For PCF

You can view the following details for PCF:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- **PCF status with NRF** - It shows whether the PCF instance is registered, suspended, or deregistered with NRF.
- **FQDN** - It shows the FQDN of the PCF registered with NRF.
- **Instance ID** - It shows the unique Instance ID of PCF registered with NRF.
- **Registered with** - It shows the FQDN of the NRF with which PCF is registered.
- **Registration Time** - It shows the time at which PCF registered with NRF.

If you want to view more details of the PCF instance such as its registration profile, click **View More Details**. It opens the **NF Registration Profile** page.

For NRF

You can view the following details for NRF:

- **Health Status** - This ribbon-styled badge shows the health status of the NRF instance. It could be in either healthy or unhealthy state.
- **Primary NRF** - The circular icon with the label P indicates that the NRF is primary.
- **Active Status** - The pulsating green circular icon shows that the NRF is currently active.
- **FQDN** - It shows the FQDN of the NRF.
- **Priority** - It shows the priority of the NRF instances. An NRF instance with priority 1 is treated as primary NRF.
- **Last Connected Time** - It shows the time when PCF last connected with primary NRF.
- **Last Status Change Time** - It shows the time when the NRF status changed.

When the status of an NRF instance changes from healthy to unhealthy, the error reason is also displayed on the page.

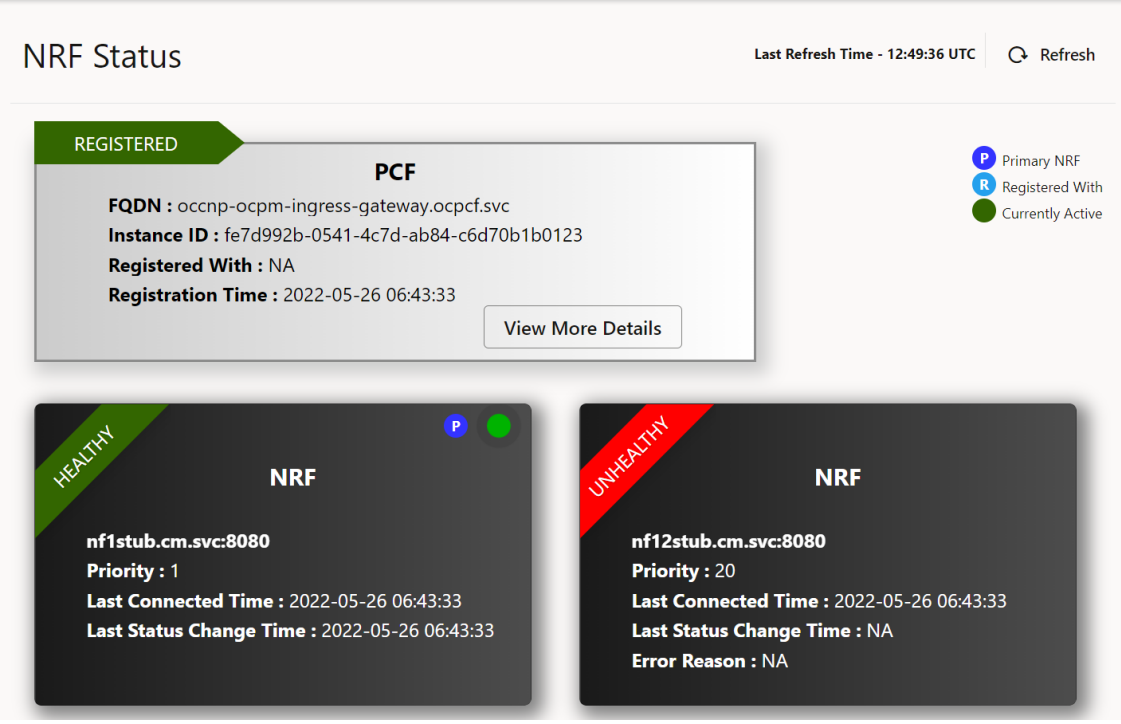
To reload the data on the page at any time, click the **Refresh** button.

Based on when the data refreshes, the Last Refresh Time on the page is also updated.

The number of NRFs displayed on the page are dynamic, and get updated according to the NRFs configured in the network.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-52 NRF Status



> **Note**
>
> Currently, the page is known to display the status of up to 8 NRF Instances.

In case of any network error, the page displays an error - **Unable to load NRF data**.

7.9.2.3 Discovered NF Instances

This page displays the list of discovered NF Instances.

On the **Discovered NF Instances** page, you can view the autonomously discovered NF profiles for BSF, CHF, UDR, and NWDAF.

Based on the value you select from the drop-down list, the following details are populated on the page:

- **NF Instance ID -** It shows the unique instance ID of the discovered NF.
- **FQDN** - It shows the FQDN of the discovered NF.
- **Priority** - It shows the priority assigned to the NF.
- **Status** - It shows whether the NF is registered or suspended.
- **View Details** - Click to view the NF profile.

If no profile is discovered or in case of any network error, the page shows "**No data to display**" along with 404-Not Found.

Copyright © 2019, 2026, Oracle and/or its affiliates.

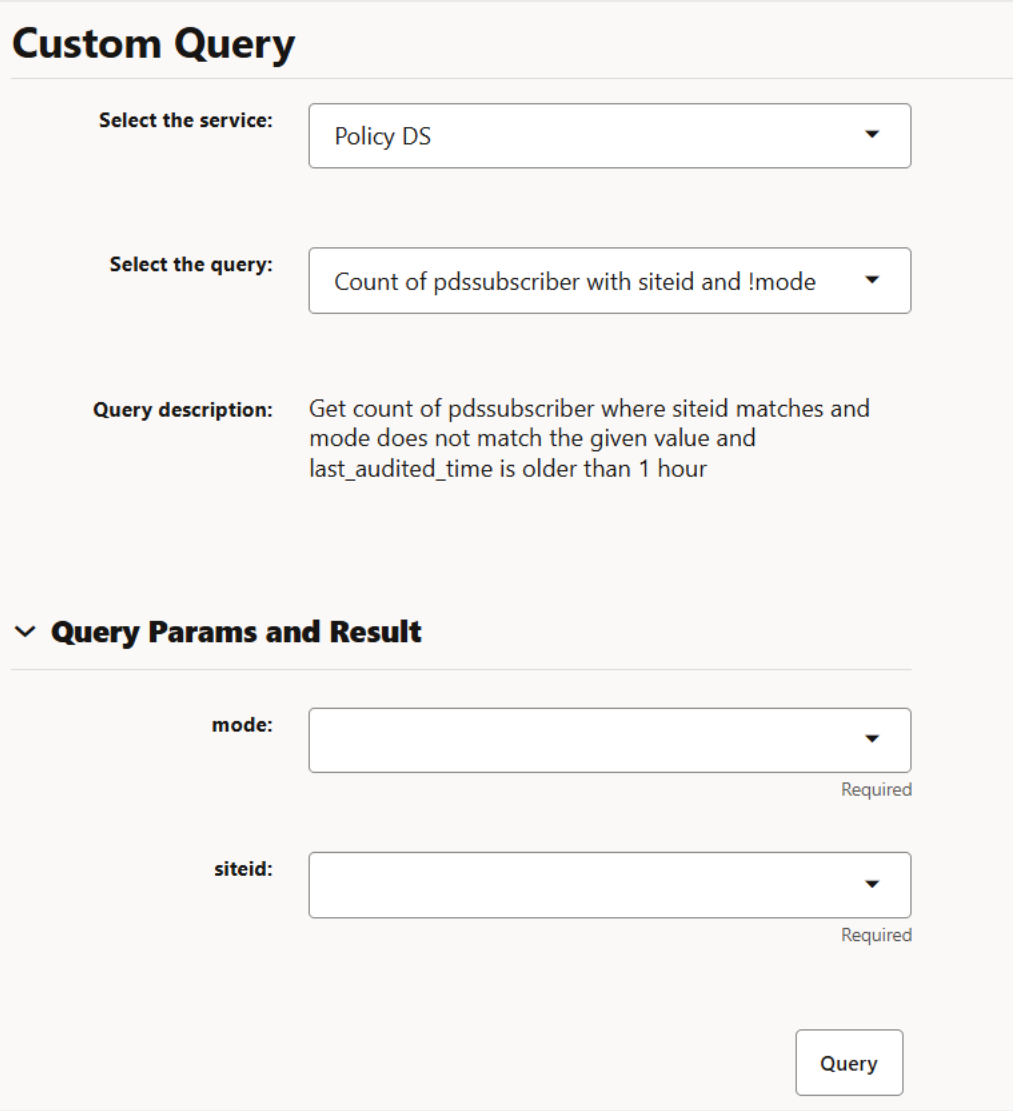
7.9.3 Custom Query

The **Custom Query** page allows to run pre-defined queries on the database. The query to be run on the database and the parameters for the query can be selected from this page.

1. Navigate to **Custom Query** page under **Status and Query** in CNC Console.
2. On the **Custom Query** page, configure the following query fields:

   Configure Custom Query on PolicyDS Database.

Figure 7-53 Custom Query on Policy DS



Copyright © 2019, 2026, Oracle and/or its affiliates.

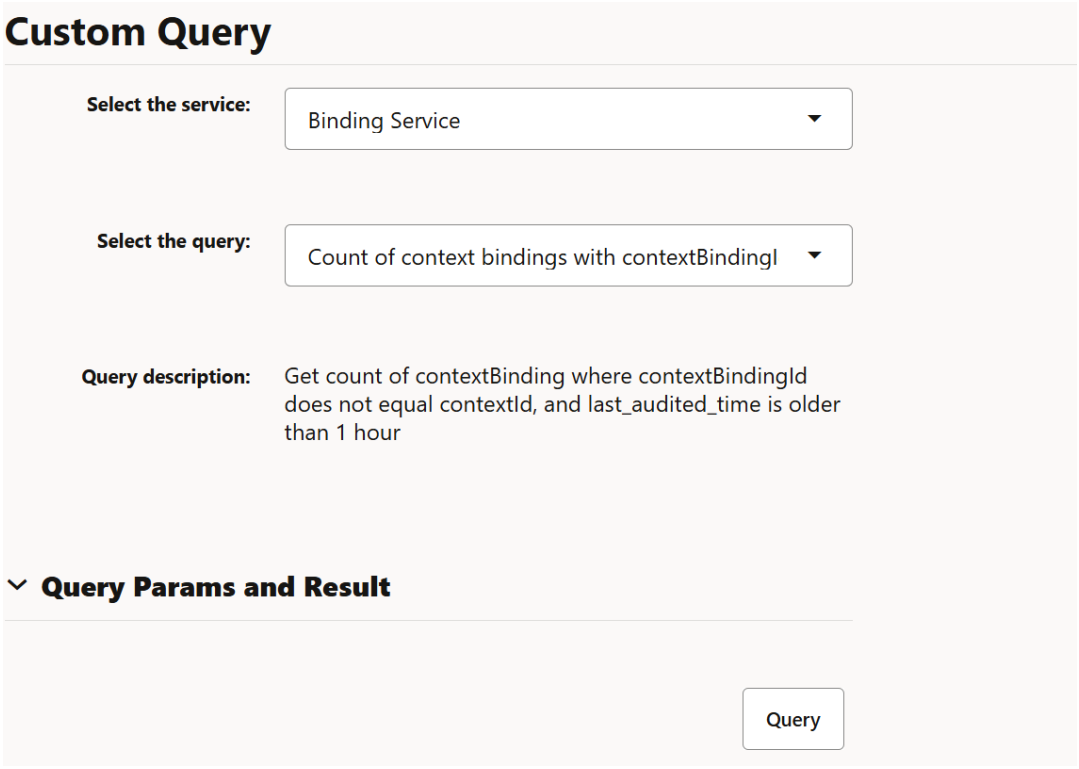
Table 7-236 To configure custom query for Policy DS.

Value	Description
Select the service	Lists the Policy service that uses the database to be queried. For example, to configure the query on PolicyDS database, select the service as `Policy DS`.
Select the query	Lists available options to query the migration of database. For example, if the selected service is `Policy DS`, `Select the query` list contains the following: • `Count of pdssubscriber with siteId and !mode`: Displays the count of `pdssubscriber` where `siteId` matches and mode does not match the given value and `last_audited_time` is older than 1 hour.
Query Params and Result	This section is used to configure the query parameters.
Mode	List the supported modes to query the PDS database: • MultiUEID: Allows user to select `MultiUeId` as the mode. • SingleUeId_SUPI_GPSI: Allows user to select `SingleUeId` with SUPI or GPSI as the mode. • SingleUeId_SUPI: Allows user to select `SingleUeId` with SUPI as the mode. • SingleUeId_GPSI: Allows user to select `SingleUeId` with GPSI as the mode. • PartitionBased_SUPI_GPSI: Allows user to select `PartitionBased` with SUPI or GPSI as the mode. • PartitionBased_SUPI: Allows user to select `PartitionBased` with SUPI as the mode. • PartitionBased_GPSI: Allows user to select `PartitionBased` with GPSI as the mode.
siteId	Specifies the site for which the query result must be displayed. This field appears depending on the value of **Select the query** field. For example, **siteId** field appears when the value of **Select the service** is `Policy DS` and the value of **Select the query** field is `Count of pdssubscriber with siteid and !mode`.

Configure Custom Query on Binding Service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-54 Custom Query on Binding ServiceCustom Query on Policy DS



The Binding Service query shows the number of records that are not yet migrated or indexed.

To avoid repeated execution, the query result is cached and displayed for one hour.

Table 7-237 To configure custom query for Binding Service.

Value	Description
Select the service	Lists the Policy service that uses the database to be queried. For example, to configure the query on Binding Service database, select the service as `Binding Service`.
Select the query	Lists available options to query the migration of database. For example, if the selected service is `Binding Service`, **Select the query** list contains `Count of context bindings with contextBindingId not equal to contextId`.

3. Click **Query** to get the query result.
The query result includes the number of non migrated records and the last executed time.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Sample output:

```
Query Result: 28
Last Executed Time: 2025-02-12 17:03:38.556
```

> **Note**
>
> The querying is optimized to be searched from cache rather than querying the database on every click of **Query** button.

7.10 Overload and Congestion Control Configurations

This section describes how to perform overload and congestion control configurations.

To use the Error Code Profiles page to create and manage error code profiles in Overload Control Configurations for Diameter Gateway and SBI interface, see *SBI Ingress Error Code Profiles Collection* section.

> **Note**
>
> When overload control feature is enabled, it should be enabled for both Diameter gateway and SBI interface. The overload control manager needs data from both Ingress Gateway and Diameter Gateway to determine the overall load on BSF management. It is not possible to enable overload control for Diameter Gateway and disable the same in Ingress Gateway.

7.10.1 Diameter

This section describes configuring the Load Shedding Profiles and the Message Priority Profiles for Diameter Gateway.

To use the Error Code Profiles page to create and manage error code profiles in Overload Control Configurations for Diameter Connector, see SBI Ingress Error Code Profiles Collection.

7.10.1.1 Load Shedding Profiles

This procedure provides information about how to create and manage load shedding profiles in Diameter Configurations.

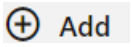
The Load Shedding Profiles page allows you to create new and manage existing load shedding profiles. The page displays the list of defined profiles and provides the options to import and export data as well.

To configure Load shedding profiles, perform the following steps:

1. From the navigation menu, under **Policy**, click **Overload and Congestion Control**, select **Diameter**, then select **Load Shedding Profiles**.
   This opens the Load Shedding Profiles page.
2. Click

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-55 Add icon with text



.

This opens the Create Load Shedding Profiles page.

3. Enter values for the available input fields, described in the following table:

Table 7-238 Load Shedding Profiles Configurations

Field Name	Description
Name	Unique name of the load shedding profile.
Scheme	Allows to configure the discard policy based on • Priority: to discard messages based on priority range • Priority and Percentage: to discard messages based on priority range and percentage for each range
Type	Defines the type of load shedding profile. You can select any of the following values from the drop-down list: • Overload Control **Note**: In Policy 25.1.200 the `Congestion Control` option is removed from the drop-down list.

To add load shedding rules for the profile type overload control, perform the following steps:

a. Under **Load Shedding Rules**, click Add .
This opens the **Add Load Shedding Rules** dialog box.

b. Enter values for the available input fields, described in the following table:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-239 Load Shedding Rules Configurations When the Selected Scheme is "Priority"

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's `ocdiscardpolicies`. Select any of the following values using the drop-down list: • L1 • L2 • L3 • L4 • L5 • L6 • L7 • L8 • L9 • L10 **Note**: Currently, Policy supports configuring load shedding profiles upto L10 only for PCF Session Management and Diameter call flows. For all other service call flows, load shedding profile can be configured only up to L3 level.
Discard Priority	Specifies the discard priority for the load shedding rule. The discard priority value can be a number from 0 to 15. Any request message with equal or greater priority is rejected.
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of overload control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE **Note**: When the EXPERIMENTAL_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Vendor ID**: Enter a valid value to specify vendor ID.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-240 Load Shedding Rules Configurations When the Selected Scheme is "Priority and Percentage"

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies. Select any of the following values using the drop-down list: • L1 • L2 • L3 • L4 • L5 • L6 • L7 • L8 • L9 • L10 **Note**: Currently, Policy supports configuring load shedding profiles upto L10 only for PCF Session Management and Diameter call flows. For all other service call flows, load shedding profile can be configured only up to L3 level.
Discard Priority Percentage	Configure the discard priority percentage as explained in the following step.

c. To configure Discard Priority Percentage, perform the following steps:

i. Under **Discard Priority Percentage**, click ⊕ Add .
This opens the **Add Discard Priority Percentage** dialog box.

Enter values for the available input fields, described in the following table:

Table 7-241 Adding Discard Priority Percentage

Field Name	Description
Priority Range	Specifies the discard priority range for the load shedding rule. The discard priority value can be a number from 0 to 31. Any request message with equal or greater priority will be rejected based on the percentage discard configured. **Note**: For Priority and Percentage type, when we give single number in the priority range, for example 9, only 9 priority messages will be rejected.
Discard Percentage	Specifies the discard percentage for the specified priority range.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-241 (Cont.) Adding Discard Priority Percentage

Field Name	Description
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of congestion control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE **Note**: When the EXPERIMENTAL_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Vendor ID**: Enter a valid value to specify vendor ID.

ii. Click **Save** to save the discard priority percentage.

d. Click **Save** to save the load shedding rule.

4. Click **Save** to save the load shedding profile.
   To discard the changes, click **Cancel**

   The value gets listed on the Load Shedding Profiles page. Use  or  available under the **Actions** column to update or delete the profile.

> **Note**
>
> While Diameter Gateway enters overload situation, messages only from network peer will be considered for load shedding. That is, messages from backed peers will not be considered for load shedding.
>
> For example, during overload Sy-SLR / Rx-RAR will not be considered for load shedding as they are generated by backend microservices.

Importing Load Shedding Profiles

To import load shedding profiles, perform the following steps:

1. Click 

   .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Exporting Load Shedding Profiles

To export load shedding profiles, click **Export**. A `json` file is saved to your device.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.10.1.2 Message Priority Profiles

This procedure provides information about how to create and manage message priority profiles in Diameter Configurations.

The Message Priority Profiles page allows you to create new and manage existing message priority profiles. The page displays the list of defined profiles and provides the options to import and export data as well.

To configure Message Priority profiles, perform the following steps:

1. From the navigation menu, under **Policy**, click **Overload and Congestion Control**, select **Diameter**, then select **Message Priority Profiles**.
   This opens the Message Priority Profiles page.
2. Click Add .
   This opens the Create Message Priority Profiles page.
3. Enter values for the available input fields, described in the following table:

Table 7-242 Message Priority Profiles Configurations

Field Name	Description
Name	Unique name of the message priority profile.

To add message priority rules for the profile, perform the following steps:

a. Under **Message Priority Rules**, click Add .
   This opens the **Add Message Priority Rules** dialog box.
b. Enter values for the available input fields, described in the following table:

Table 7-243 Message Priority Rules Configurations

Field Name	Description
Name	Specifies the unique name of the message priority rule.
Message Priority	Specifies the priority assigned to the message. It can be a number from 0 to 31. **Note**: The default message priority is 10, if no rule is available. For setting a different default message priority, a rule must be added with lowest rule priority(higher number) to match all the messages(application set to "any", message type set to "any"). This will ensure that, this rule will be run at the last i.e., when no other rules match.
Rule Priority	Specifies the priority assigned to the message priority rule. The range for this field is 0 to 65535. **Note:** During Import and Export, if the old data has rule priority value greater than the specified range, then the Rule Priority might be impacted.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-243 (Cont.) Message Priority Rules Configurations

Field Name	Description
Use DRMP Priority	When this switch is enabled, the priority for the message rule is assigned from DRMP AVP.
Use OC-Message-Priority	When this switch is enabled, the prioroty for the message rule is assigned from `OC-Message-Priority` header attribute. **Note**: • The default value of this switch depends on the message direction. • For incoming peer-initiated Diameter requests,this switch is disabled by default because external peers might send DRMP, OC-Message-Priority, or neither priority AVP. When this switch is disabled, priority is derived using the configured profile logic. • For outgoing PCF/PCRF-initiated control messages, this switch is enabled by default. This allows the system to propagate and use a deterministic OC-Message-Priority value end-to-end instead of recalculating a different priority. • In summary, incoming traffic does not assume that OC-Message-Priority is present and derives the priority, whereas outgoing control traffic is expected to use the propagated OC-Message-Priority value directly. • In case both `Use DRMP Priority` and `Use OC-Message-Priority` is enabled, then `OC-Message-Priority` value is considered. In case both are disabled then the default message priority is considered.
Conditions	Provide Conditions details:
Application	Specifies the type of application. Users can select any of the following values from the drop-down: • Gx • Sd • Rx • Sy • Any

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-243 (Cont.) Message Priority Rules Configurations

Field Name	Description
Message	Specifies the type of message for the selected application. The supported message values for each application type are as follow: • For Gx application, choose a value from CCR, RAR, or Any. • For Sd application, choose CCR, TSR, or RAR. • For Rx application, choose a value from AAR, ASR, RAR, STR, or Any. • For Sy application, choose a value from Sy-SLR, STR, Sy-SNR, or Any. • For application type selected as Any, choose a value from the drop-down list of **Message**.

c. To add pre-defined AVP conditions, click ⊕ Add under **Pre Defined AVP Conditions**. On the **Add Pre Defined AVP Conditions** dialog box, select Name and enter values as described in the following table:

Table 7-244 Pre Defined AVP Conditions Configurations

Name	Values
Called-Station-Id	This AVP can be used only when the application type is specified as Gx and Rx. Users can enter multiple comma-separated values. **Note**: CNC Policy supports wildcard format for this AVP.
CC-Request-Type	This AVP can be used for Gx application with message specified as CCR. You can select any of the following valid values from the drop-down list: • INITIAL_REQUEST • UPDATE_REQUEST • TERMINATION_REQUEST • EVENT_REQUEST
Rx-Request-Type	This AVP can be used for Rx application with message specified as AAR. You can select any of the following valid values from the drop-down list: • INITIAL_REQUEST • UPDATE_REQUEST • PCSCF_RESTORATION_REQUEST
`Service-URN`	This AVP indicates that an AF session is used for emergency traffic. It is of type OctetString. Examples: "sos", "sos.fire", "sos.police" and "sos.ambulance". **Note**: CNC Policy supports wildcard format for this AVP.
`MPS-Identifier`	This AVP indicates that an AF session relates to an MPS session and contains the national variant for MPS service name. It is of type OctetString. Example: NGN GETS
`MCPTT-Identifier`	This AVP includes either one of the namespace values used for MCPTT and may include the name of the MCPTT service provider. It is of type OctetString.
`MCVideo-Identifier`	This AVP includes the name of the MCVideo service provider. It is of type OctetString.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-244 (Cont.) Pre Defined AVP Conditions Configurations

Name	Values
Reservation-Priority	This AVP is of type Enumerated and is specified in an AA-Request as the main AVP to associate a priority with a resource reservation or modification request. You can specify a value from 0 to 7 for this AVP.
SN-Request-Type	This AVP informs the PCRF about the type of the Spending-Status-Notification-Request (SNR).You can select any of the following valid values from the drop-down list: • ABORT_SESSION_REQUEST • NORMAL_REQUEST
DRMP	For the Operator, You can select any of the following valid values from the drop-down list: • Equals • Not Equals • Less Than • Less Than Equals • Greater Than • Greater Than Equals For the Values, You can enter any numerical value between 1-15.
OC-Message-Priority	For the Operator, You can select any of the following valid values from the drop-down list: • Equals • Not Equals • Less Than • Less Than Equals • Greater Than • Greater Than Equals For the Values, You can enter any numerical value between 1-31.

Click **Save** to save the pre-defined AVP conditions for the message priority rule.

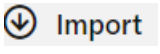
d. Click **Save** to save the message priority rule.

4. Click **Save** to save the message priority profile.
   To discard the changes, click **Cancel**

   The value gets listed on the Message Priority Profiles page. Use  or  available under the **Actions** column to update or delete the profile.

Importing Load Shedding Profiles

To import message priority profiles, perform the following steps:

1. Click 

   .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Exporting Message Priority Profiles

To export load shedding profiles, click **Export**. A json file is saved to your device.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.10.2 SBI

This section describes the Rate Limiting and overload control for SBI.

To use the Error Code Profiles page to create and manage error code profiles in Overload Control Configurations for SBI interface, see SBI Ingress Error Code Profiles Collection.

7.10.2.1 Overload Control

This section describes the Discard Policy Mapping and Discard Policy for SBI interface.

7.10.2.1.1 Discard Policy Mapping

This procedure provides information about how to use the Discard Policy Mapping page to manage discard policy mapping in Overload Control Configurations for SBI interface.

To configure Discard Policy Mapping, perform the following steps:

1. From the navigation menu, under **Policy**, click **Overload Control Configurations**, select **SBI**, then select **Overload Control**, and then select **Discard Policy Mapping**.
   This opens the Discard Policy Mapping page.
2. Click Edit.
   This opens the Edit Discard Policy Mapping page.
3. Enter values for the available input fields as described in the following table:

Table 7-245 Discard Policy Mapping Configurations

Field Name	Description
Enable Overload Control	Specifies whether to enable or disable overload control.
Sampling Period (in milliseconds)	Specifies the time frame for each cycle of overload control per service. Its default value is 200 ms.

4. Under **Mappings**, click 

   .
   This opens the Add Mappings dialog box.
5. Enter values for the available input fields as described in the following table:

Table 7-246 Mappings Configurations

Field Name	Description
Service Name	Specifies the name of the microservice that is further used to determine a mapping between service and discard policy name per service.
Policy Name	Specifies the name of the discard policy that is used to determine a mapping between service and discard policy name per service. The drop-down list shows the policies configured using the Discard Policy page.

6. Click **Save** to save the mappings.
   To discard the changes, click **Cancel**

Copyright © 2019, 2026, Oracle and/or its affiliates.

The value gets listed under the **Mappings** group on the Discard Policy Mapping page. Use  or  available under the **Actions** column to update or delete the mappings.

7. Click **Save** to save the discard policy mapping.
   To discard the changes, click **Cancel**.

7.10.2.1.2 Discard Policy

This procedure provides information about how to use the Discard Policy page to manage discard policies for overload control for SBI interface.

To configure discard policy, perform the following steps:

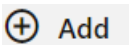
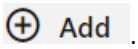
1. From the navigation menu, under **Policy**, click **Overload Control Configurations**, select **SBI**, then select **Overload Control**, and then select **Discard Policy**.
   This opens the Overload Control Discard Policy page.
2. Click Edit.
   This opens the Edit Overload Control Discard Policy page.
3. Click  .
   This opens the Add Discard Policies page.
4. Enter values for the available input fields as described in the following table:

Table 7-247 Discard Policy Configurations

Field Name	Description
Name	Specifies the unique name of the discard policy.
Scheme	Specifies the criteria of dropping requests for a microservice. It could be either priority based or percentage based. If you select the value as Priority Based, configure the values of the parameters under Priority Based Policies. For Percentage Based scheme, configure the parameters under Percentage Based Policies.

To add priority based policies, perform the following steps:

a. Under **Priority Based Policies**, click  .
   This opens the **Add Priority Based Policies** dialog box.
b. Enter values for the available input fields as described in the following table:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-248 Priority Based Policies Configurations

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies. Select any of the following values using the drop-down list: • L1 (Load Level 1) • L2 (Load Level 2) • L3 (Load Level 3) • L4 (Load Level 4) • L5 (Load Level 5) • L6 (Load Level 6) • L7 (Load Level 7) • L8 (Load Level 8) • L9 (Load Level 9) • L10 (Load Level 10) **Note**: Currently, Policy supports configuring load shedding profiles upto L10 only for PCF Session Management and Diameter call flows. For all other service call flows, load shedding profile can be configured only upto L3 level.
Discard Priority	Specify the discard priority for the discard policy rule. Any request message with equal or lower message priority is rejected. **Note** 1 is considered as the highest message priority.
Error Code Profile	Select an error code profile from the drop-down list. It displays the list of error profiles configured using the Error Code Profile page.
Action	Specifies the action taken when selected requests are rejected. Currently, it only supports the action to reject requests based on error code.

OR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-249 Percentage Based Policies Configurations

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies. Select any of the following values using the drop-down list: • L1 (Load Level 1) • L2 (Load Level 2) • L3 (Load Level 3) • L4 (Load Level 4) • L5 (Load Level 5) • L6 (Load Level 6) • L7 (Load Level 7) • L8 (Load Level 8) • L9 (Load Level 9) • L10 (Load Level 10) **Note**: Currently, Policy supports configuring load shedding profiles upto L10 only for PCF Session Management and Diameter call flows. For all other service call flows, load shedding profile can be configured only upto L3 level.
Discard Percentage	Specify the discard percentage for the policy rule. The specified percentage of the calculated rate for service in previous sampling period is discarded in current sampling period.
Error Code Profile	Select an error code profile from the drop-down list. It displays the list of error profiles configured using the Error Code Profile page.
Action	Specifies the action taken when selected requests are rejected. Currently, it only supports the action to reject requests based on error code.

c. Click **Save** to save the discard policy.
To discard the changes, click **Cancel**.

5. Click **Save** to save the overload control discard policy.
To discard the changes, click **Cancel**

The value gets listed on the Overload Control Discard Policy page. Use  or  available under the **Actions** column to update or delete any given policy.

7.10.2.2 Route Level Mapping

This procedure provides information about how to use the Route Level Mapping page to manage route level mapping for overload control on SBI interface.

To configure route level mapping, perform the following steps:

1. From the navigation menu, under **Policy**, click **Overload Control Configurations**, select **SBI**, then select **Route Level Mapping**.
This opens the Route Level Mapping page.
2. Click Edit.
This opens the Edit Route Level Mapping page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Under **Route Configuration**, click Add .

   This opens the Add Route Configuration dialog box.

4. Enter values for the available input fields as described in the following table:

Table 7-250 Rate Limiting Policy Configurations

Field Name	Description
Id	Specifies the list of route IDs available for Policy. The following are some of the supported values: • Create SM Policy Association • Delete SM Policy Association • Update SM Policy Association • UDR Notify • CHF Terminate • CHF Notify • Create PA Application Session • Update PA Application Session • Delete PA Application Session • Subscribe PA Events • Unsubscribe PA Events • NRF Notification • SOAP Notification • Create AM Policy Association • Delete AM Policy Association • Update AM Policy Association • Create UE Policy Association • Delete UE Policy Association • Update UE Policy Association • UE Notify • UE Notify Failure • Binding Audit Notification • UDR Usage Monitoring Notify • NWDAF Event Notify
Failure Request Count Profile	Specifies the mapping between error series and failure count. This field allows to select one of the **Profiles** from the **Error Code Series List** created on **IGW** page under **Service Configurations**.

5. Under **Rate Limiting**, click Add .

   This opens the Add Method dialog box.

6. Enter values for the available input fields as described in the following table:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-251 Method Configurations

Field Name	Description
Http Method	Specifies the HTTP method. Depending on the value select for **Id**, you can select any of the following values from the drop-down list: • POST • PUT • GET • DELETE • PATCH
Message Rate (per sampling period)	Specifies the message rate per sampling period for a given method. Range of value: 0 to 1000000
Rate Limit Policy	Select a rate limit policy from the drop-down list. It displays the list of rate limit policies configured using the Rate Limiting Policy page.

7. Click **Save** to save the method. The value gets listed under the **Rate Limiting** group.
   To discard the changes, click **Cancel**.

   Use  or  available under the **Actions** column to update or delete any given policy.
8. Click **Save** to save the route configuration.
   To discard the changes, click **Cancel**.
9. Click **Save** to save the route level mapping.
   To discard the changes, click **Cancel**.

7.10.2.3 Failure Count

> **Note**
>
> Currently, all the configurations for failure count can be performed only using REST APIs.
>
> Only the failure count threshold can be configured using CNC Console. Configuring the error codes and mapping the respective routes must be done only through REST APIs.
>
> Also, if the system requires overload configuration for both rate limiting and failure count, it is suggested to perform these configuration using API's only.
>
> For more details, see *Rate Limiting* and *Failure Count at Ingress gateway* sections in *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*.
>
> From 24.1.0 release, you can configure failure count using CNC Console. For more details, see IGW .

7.10.3 Congestion Control

Copyright © 2019, 2026, Oracle and/or its affiliates.

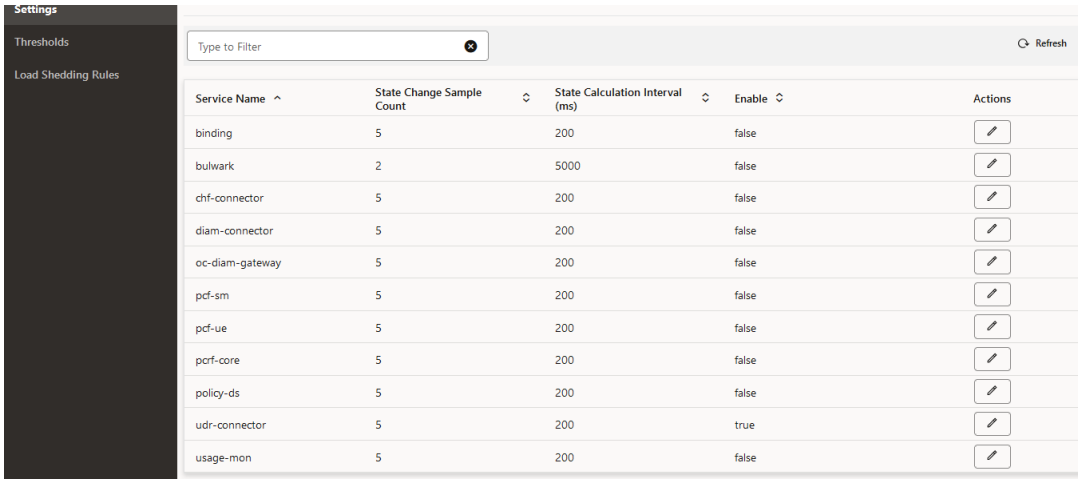
7.10.3.1 Settings

The **Settings** page displays the general configurations related to the Congestion Control. The page allows you to edit the configurations.

To edit settings:

1. From the navigation menu under **Policy**, click **Overload and Congestion Control** and select **Congestion Control** and then select **Settings**.
   This opens the **Settings** page. The page displays the existing configurations for different Policy services.

Figure 7-56 Congestion Control Settings



2. Click Edit .
   This opens the **Edit Settings** page.
3. Enter values for the available input fields as described in the following table:

Table 7-252 Edit Configurations

Field Name	Description
Service Name	Specifies the Policy service name. You can check the default configuration for the all fields and edit as necessary.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-252 (Cont.) Edit Configurations

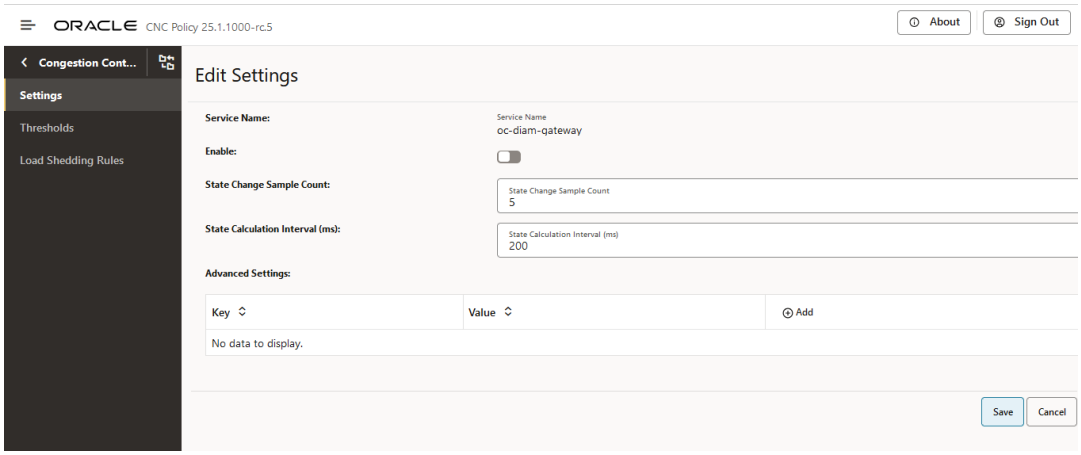
Field Name	Description
Enable	Specifies whether to enable or disable Congestion Control for the selected Policy service. The Pod Congestion Control can be enabled for the following Policy services: • Bulwark • Binding • PDS • Usage Monitoring • SM Service • PCRF Core Service • UE Service • Diameter Gateway • Diameter Connector • UDR Connector • CHF Connector • Notifier • AM Service **Default value**: False
State Change Sample Count	This specifies after how many continuous intervals, the pod state can be changed. This count can range from 1 to 2147483647. **Default Value**: 5
State Calculation Interval (in milliseconds)	This specifies that after this time duration or interval, the pod congestion state will be re-verified. This interval in milliseconds can range from 50 to 2147483647. **Default Value**: 200

Note

The **State Change Sample Count** and **State Calculation Interval** settings helps in preventing sudden state transition to final calculated state and higher rejection of requests. These states are reverified after every **State Calculation Interval**. The state transition occurs step by step and on each increment or decrement of state, the **State Change Sample Count** increases. If the current state or intermediate state is adjacent to final calculated state, the **State Change Sample Count** will increase on every **State Calculation Interval** and transition will happen once the remaining sample count gets exhausted.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-57 Edit Congestion Control Settings



4. Perform the following steps to configure **Advanced Settings** for configuring algorithm that should be used for calculating the CPU and Queue usage for Congestion Control feature:

   a. Click the Add
   The page opens the **Add Advanced Settings** dialog box.

   b. In the dialog box, enter the following **keys** and respective **values**:

The following table describes the keys and values:

Table 7-253 Add Advanced Settings Configurations

Key	Value
CPU_CONGESTION_RESOURCE_CALC_ALGORITHM	This enables the congestion control CPU resource calculation to use the algorithm provided. If invalid value is provided then default method is used to calculate the CPU usage. **Allowed Values**: EMA
CPU_CONGESTION_RESOURCE_CALC_INTERVAL_MS	This configuration sets the time interval in milliseconds for CPU congestion resource to be calculated by the configured algorithm. **Default Value**: 200ms
QUEUE_CONGESTION_RESOURCE_CALC_ALGORITHM	This enables the congestion control Queue resource calculation to use the algorithm provided. If invalid value is provided then default method is used to calculate the Queue usage. **Allowed Value**: EMA
QUEUE_CONGESTION_RESOURCE_CALC_INTERVAL_MS	This configuration sets the time interval in milliseconds for Queue congestion resource to be calculated by the configured algorithm. **Default Value**: 200ms
EMA_CPU_CONGESTION_RESOURCE_CALC_RATIO	This configuration will be used to set the EMA ratio in which congestion resource(s) calculated using EMA algorithm to be considered for calculation. **Default Value**: 70:30

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-253 (Cont.) Add Advanced Settings Configurations

Key	Value
EMA_QUEUE_CONGESTION_RESOURCE_CALC_RATIO	This configuration will be used to set the EMA ratio in which congestion resource(s) calculated using EMA algorithm to be considered for calculation. **Default Value**: 70:30

5. Perform the following steps to configure **Advanced Settings**:
   a. Click the Add
   The page opens the **Add Advanced Settings** dialog box.
   b. In the dialog box, enter the following **keys** and respective **values**:
   The following table describes the keys and values for Diameter Connector discard priority :

Table 7-254 Add Advanced Settings Configurations

Key	Value	Description
SM.NOTIFY.REQUEST.PRIORITY	25	Re Authorization notification (RAR)
SM.NOTIFY.TERMINATE.REQUEST.PRIORITY	20	Terminate notify (ASR)
PDS.FETCH.REQUEST.PRIORITY	25	PDS Fetch SLR
PDS.NOTIFY.TERMINATE.REQUEST.PRIORITY	20	PDS Notify terminate (STR)
RX.AAR.REQUEST.PRIORITY	30	Rx AAR
RX.STR.REQUEST.PRIORITY	20	Rx STR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-254 (Cont.) Add Advanced Settings Configurations

Key	Value	Description
RX.ASR.REQUEST.PRIORITY	25	Rx ASR
SY.SNR.DEFAULT.PRIORITY	25	Sy SNR
CONGESTION.USE.EXPERIMENTAL.RESULT.CODE	false	To set if user wants to use experimental result code when rejecting diameter messages. Allowed values are true or false. By default it will be false.
CONGESTION.VENDOR.ID	0	This is to configure the diameter vendor id for the congestion control discards and data type of value will be numerical. If value is non-zero, then the *CONGESTION_DIAMETER_RESPONSE_CODE* considered as the experimental result code. If value is zero / not configured, then *CONGESTION_DIAMETER_RESPONSE_CODE*considered as the normal result code. **Examples**:CONGESTION_DIAMETER_VENDOR_ID=10415CONGESTION_DIAMETER_VENDOR_ID=21274
CONGESTION.DIAMETER.RESPONSE.CODE	3004	To set response code when rejecting diameter messages. Only valid 3xxx, 4xxx, 5xxx response codes are allowed.
CONGESTION.HTTP.RESPONSE.CODE	503	Configure the response code of any rejected requests by Diameter Connector Core service due to congestion state. By default, the service sends 503 as response code. If configured then it shall be 1xx, 3xx, 4xx or 5xx response code.
SM.TDF.CREATE.SESSION.REQUEST.PRIORITY	24	Create TDF Session (TSR)
SM.TDF.TERMINATE.REQUEST.PRIORITY	16	RAR Terminate

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-254 (Cont.) Add Advanced Settings Configurations

Key	Value	Description
SM.TDF.UPDATE.REQUEST.PRIORITY	18	RAR Update
SD.CCR.TERMINATE.REQUEST.PRIORITY	16	Sd CCR-T
SD.CCR.UPDATE.REQUEST.PRIORITY	18	Sd CCR-U

6. Click **Save** to save the congestion control configuration.
   To discard the changes, click **Cancel**.

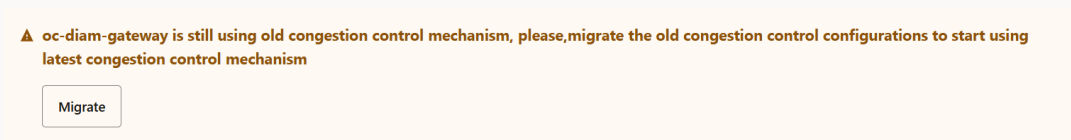
   The value gets listed on the Settings page.

Migration of Diameter Gateway Congestion Control Configuration Data

After upgrade to Policy 25.1.200, perform migration of Congestion Control configurations using CNC Console, follow these steps:

1. From the navigation menu under **Policy**, click **Overload and Congestion Control** and select **Congestion Control** and then either selects **Thresholds** or **Load Shedding Rules** then the following warning message is displayed on all the respective pages on selection of **Diameter Gateway** service: .
   The following picture illustrates the Diameter Gateway congestion control data migration warning message:

Figure 7-58 Diameter Gateway Data Migration Warning



2. Click on `Migrate`. This opens the Migration Dialog box, to migrate the Load Shedding Profiles, Message Priority Profiles, and Threshold data.

> **Note**
>
> In the configuration data, if the load shedding profiles are not configured or available for the Diameter Gateway then only Migrate Threshold Data page will be displayed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. The Migrate Load Shedding Profiles Data page, displays all the load shedding profiles created using the previous version.
   a. In the dialog box select values for the available input fields as described in the following table:

Table 7-255 Migrate Load Shedding Profiles Data, with scheme as Priority

Field Name	Description
Load Shedding Profile	Choose a profile from the drop down lists of previous versions load shedding profiles.
Discard Priority	Under `Discard Priority` Click to edit DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2, and CONGESTED states, and configure their respective **Discard Priority** values.

   b. Click **Next** to continue with the data migration process. This opens the Migrate Load Shedding Profiles Response Code Data page.
   c. Click **Cancel** to discontinue the data migration process.
4. The Migrate Load Shedding Profiles Data page, displays all the load shedding profiles created using the previous version.
   a. In the dialog box select values for the available input fields as described in the following table:

Table 7-256 Migrate Load Shedding Profiles Data, with scheme as PriorityAndPercentage

Field Name	Description
Load Shedding Profile	Choose a profile from the drop down lists of load shedding profiles.
Discard Priority	Under `Discard Priority` Click to edit CONGESTION_L1 and CONGESTION_L2 states and configure the respective **Discard Priority** values. Click to view DANGER_OF_CONGESTION and CONGESTED states respective **Discard Priority** values.

   b. Click **Next** to continue with the data migration process. This opens the Migrate Load Shedding Profiles Response Code Data page.
   c. Click **Cancel** to discontinue the data migration process.
5. Configure values for the **Congestion Response Codes** input fields as described in the following table:

Table 7-257 Congestion Response Codes

Field Name	Result Code	Vendor Id
DIAMETER_TOO_BUSY	3004	0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-257 (Cont.) Congestion Response Codes

Field Name	Result Code	Vendor Id
DIAMETER_UNABLE_TO_COMPLY	5012	0
DIAMETER_UNABLE_TO_DELIVER	3002	0
EXPERIMENTAL_RESULT_CODE	3006	6

6. Click **Next** to continue with the data migration process. This opens the Migrate Message Priority Profiles Data page.
7. Configure values for the **Migrate Message Priority Profiles Data** input fields as described in the following table:

Table 7-258 Migrate Message Priority Profiles Data

Field Name	Description
Message Priority Profile	Choose a profile from the drop down lists of message priority profiles. This profile will be used for both Congestion Control and Overload Control features.

8. Click **Cancel** to discontinue the data migration process.
9. Click **Back** to the previous page.
10. Click **Next** to continue with the data migration process. This opens the Migrate Message Threshold Data page.
11. Configure values for the **Migrate Message Threshold Data** input fields as described in the following table:

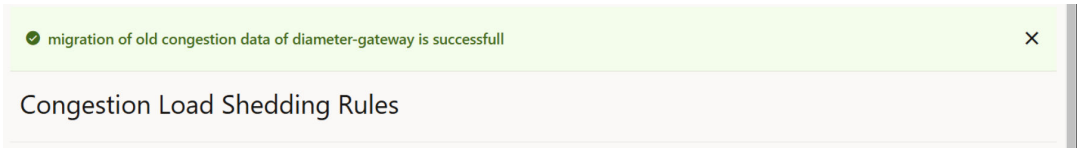
Table 7-259 Migrate Message Threshold Data

Field Name	Description
Name of the Profile	Choose a profile from the drop down lists of message threshold profiles.
Threshold Data	Under `Threshold Data` Click  to edit DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2, and CONGESTED states and configure their respective **Queue** and **CPU** values.

12. Click **Migrate** to perform the data migration. This will migrate all the configuration data for Congestion Control to the 25.1.200 versions, and the feature is not enabled for Diameter Gateway services.
13. Click **Migrate and Enable** to perform the data migration and enable Congestion Control for Diameter Gateway services.
14. Click **Cancel** to discontinue the data migration process.
15. Click **Back** to the previous page and perform any updates or changes.
16. Data migration is successful, the message ***migration of old congestion data of diameter-gateway is successfull*** is shown.

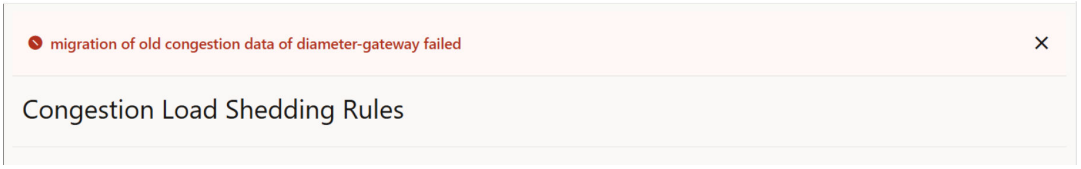
Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-59 Migration of old Diameter Gateway congestion data success status



17. Data migration fails, the message ***migration of old congestion data of diameter-gateway failed*** is shown.

Figure 7-60 Migration of old congestion data of diameter-gateway failure status



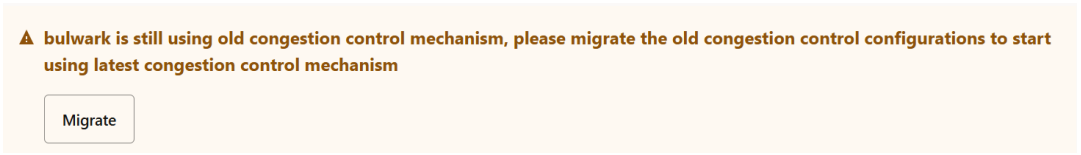
18. To verify if the Diameter Gateway Congestion Control configurations migration is successful,
    a. From the navigation menu under **Policy**, click **Overload and Congestion Control** and select **Settings**.
    This opens the **Settings** page. The page displays the default Congestion Control configurations for the selected services along with other policy services in the drop-down list, and now the migration message is not displayed.

Migration of Bulwark Service Congestion Control Configurations

After upgrade to Policy 25.1.200, perform migration of Congestion Control configurations using CNC Console, follow these steps:

1. From the navigation menu under **Policy**, click **Overload and Congestion Control** and select **Congestion Control** and then either selects **Thresholds** or **Load Shedding Rules** then the following warning message is displayed on all the respective pages on selection of **Bulwark** service: .
   The following picture illustrates the Bulwark service congestion control data migration warning message:

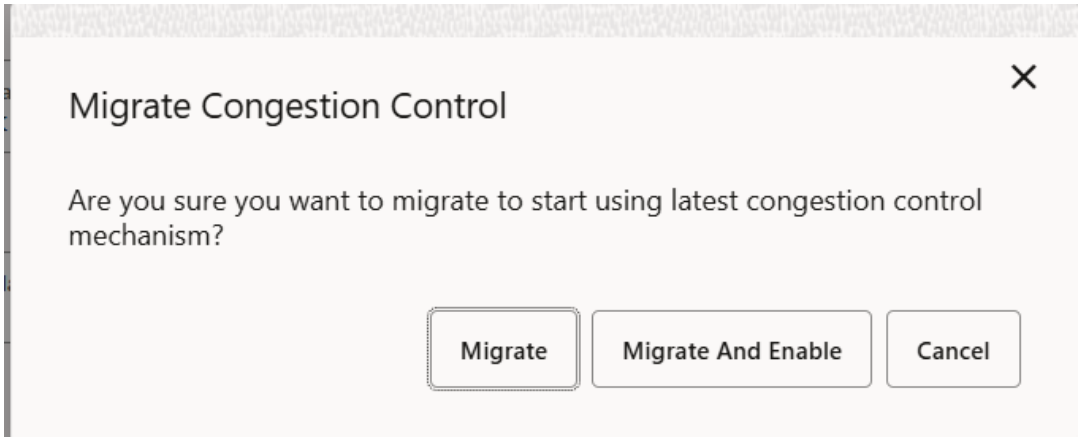
Figure 7-61 Bulwark Service Data Migration Warning



2. Click on `Migrate`. This opens the Migration Congestion Control dialog box to perform data migration for Bulwark service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-62 Migrate Congestion Control



> **Note**
>
> In the configuration data, if the load shedding profiles are not configured or available for the Bulwark service then only Migrate Threshold Data page will be displayed.

- Click **Migrate** in the Migrate Congestion Control box, this opens Migrate Load Shedding Profiles Data page. The previous version's list of Congestion Control settings, threshold profiles, and load shedding profiles configurations for Bulwark service will be migrated to the current version. During migration process the user can select a active threshold profile and load shedding rule from the list. But the pod congestion control is disabled for the Bulwark service.
- Click **Migrate and Enable** in the Migrate Congestion Control box migrate the previous version's list of Congestion Control settings, threshold profiles, and load shedding profiles configurations for Bulwark service to the current versions. During migration process the user can select a active threshold profile and load shedding rule from the list. But the pod congestion control is enabled for the Bulwark service.
- Click **Cancel** in the Migrate Congestion Control box to o discontinue the data migration process.

3. The Migrate Load Shedding Profiles Data page, displays all the load shedding profiles created using the previous version.
   a. In the dialog box select values for the available input fields as described in the following table:

Table 7-260 Migrate Load Shedding Profiles Data, with scheme as Priority

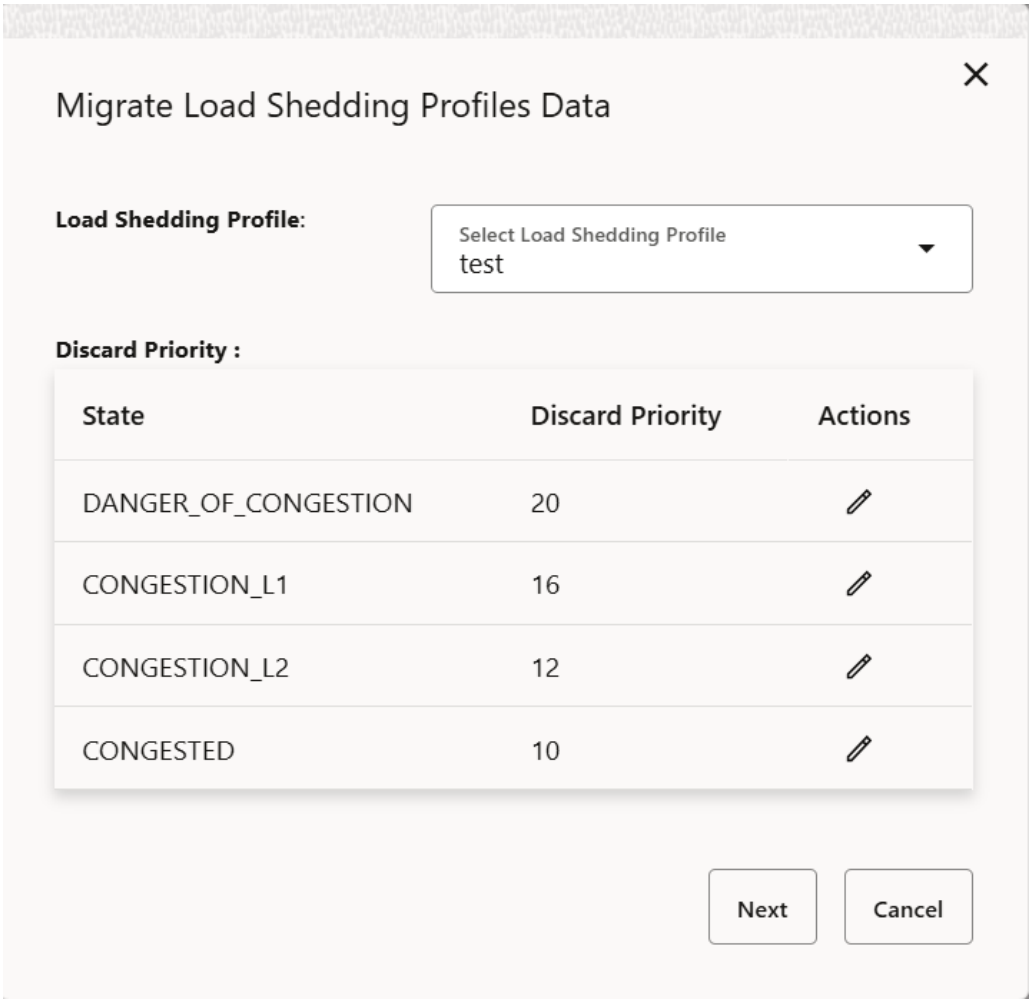
Field Name	Description
Load Shedding Profile	Choose a profile from the drop down lists of previous versions load shedding profiles.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-260 (Cont.) Migrate Load Shedding Profiles Data, with scheme as Priority

Field Name	Description
Discard Priority	Under `Discard Priority` Click  to edit DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2, and CONGESTED states, and configure their respective **Discard Priority** values.

Figure 7-63 Migrate Load Shedding Profiles Data



b. Click **Next** to continue with the data migration process. This opens the Select Active Load Shedding Profile page.

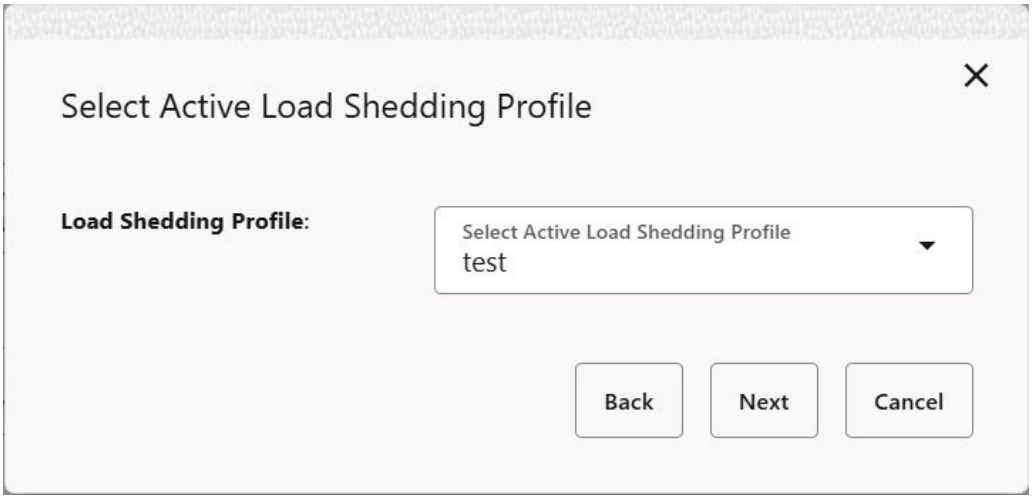
c. Click **Cancel** to discontinue the data migration process.

4. The Select Active Load Shedding Profile page, displays a drop down with all the load shedding profiles.

   a. User can select a load shedding profile from the **Load Shedding Profile** drop down to make it active.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-64 Select Active Load Shedding Profile



b. Click **Back** to go to previous page.

c. Click **Next** to continue with the data migration process. This opens the Migrate Threshold profiles Data page.

d. Click **Cancel** to discontinue the data migration process.

5. The **Migrate Threshold profiles Data** displays all the threshold profiles created using the previous version.

   a. In the dialog box select values for the available input fields as described in the following table:

Table 7-261 Migrate Threshold profiles Data

Field Name	Description
Threshold Profile	Choose a profile from the drop down lists of message threshold profiles.
Threshold Data	Under `Threshold Data` Click to edit DANGER_OF_CONGESTION, CONGESTION_L1, CONGESTION_L2, and CONGESTED states and configure their respective **Queue** and **CPU** values.

   b. Click **Back** to go to previous page.

   c. Click **Next** to continue with the data migration process. This opens the Select Active Threshold Profile page.

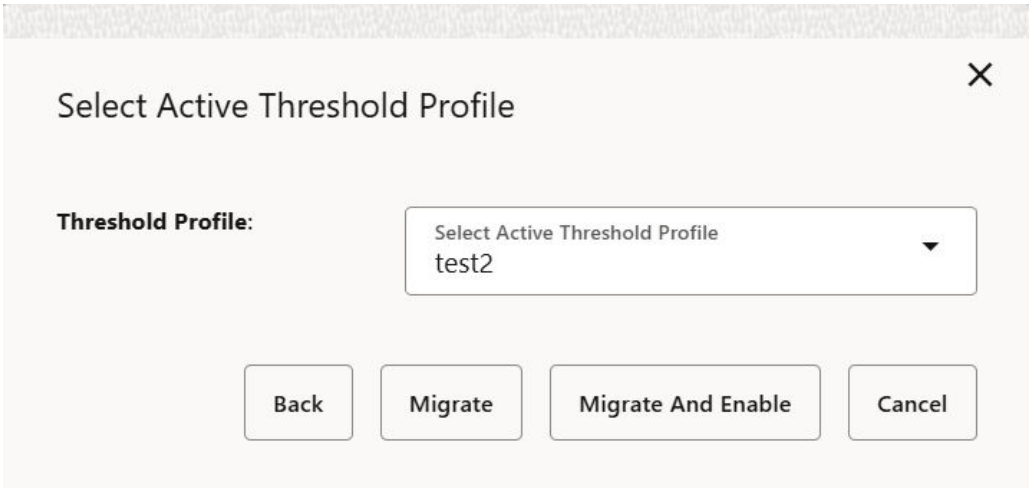
   d. Click **Cancel** to discontinue the data migration process.

6. The Select Active Threshold Profile page, displays a drop down with all the threshold profiles.

   a. User can select a load shedding profile from the **Threshold Profile** drop down to make it active.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-65 Select Active Threshold Profile



b. Click **Back** to go to previous page.

c. Click **Migrate** to perform the data migration. This will migrate all the configuration data for Congestion Control to the 25.1.200 versions, and pod congestion control feature is not enabled for Bulwark services.

d. Click **Migrate and Enable** to perform the data migration and enable pod congestion Control for Bulwark services.

e. Click **Cancel** to discontinue the data migration process.

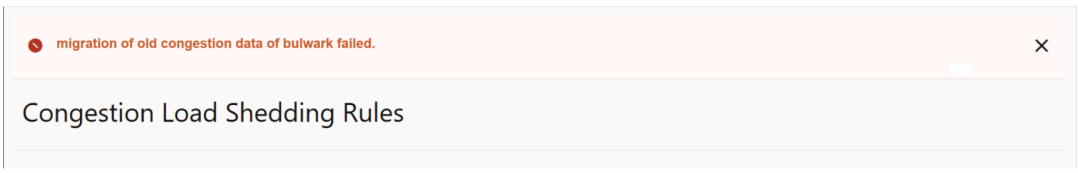
7. Data migration is successful, the message ***migration of old congestion data of bulwark is successful*** is shown.

Figure 7-66 Bulwark Migration Successful



8. Data migration fails, the message ***migration of old congestion data of bulwark failed*** is shown.

Figure 7-67 Bulwark Migration Unsuccessful



9. To verify if the Bulwark Congestion Control configurations migration is successful,

a. From the navigation menu under **Policy**, click **Overload and Congestion Control** and select **Settings**.
This opens the **Settings** page. The page displays the default Congestion Control configurations for the selected services along with other policy services in the drop-

Copyright © 2019, 2026, Oracle and/or its affiliates.

down list, and now the migration message is not displayed on selection of Bulwark service.

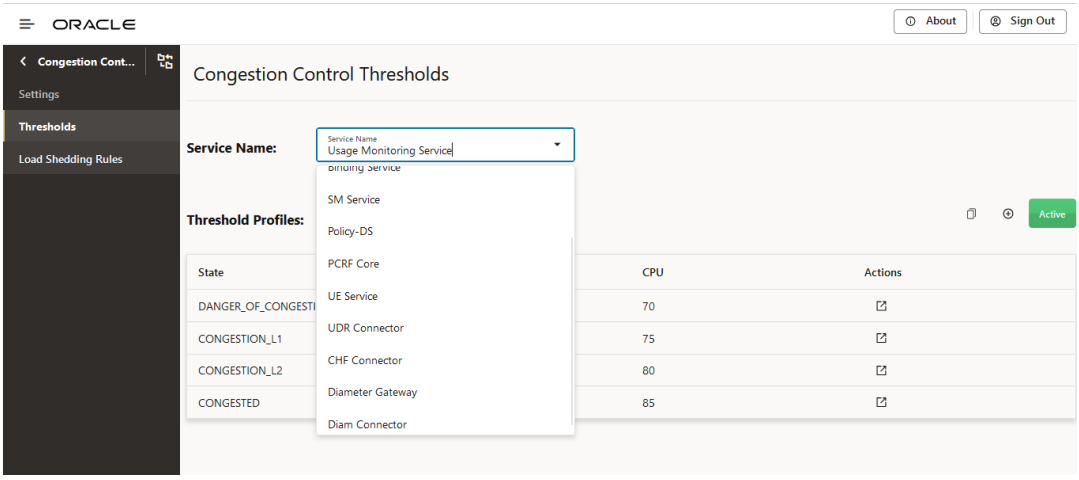
7.10.3.2 Thresholds

Policy allows you to configure the congestion control threshold values for a Policy service using a threshold profile. You can either use a default that is set during PCF deployment or create a new profile using CNC Console. You must activate one of the profiles to use the threshold values. At any time, you can activate only one profile. To open **Congestion Control Thresholds** page:

1. From the navigation menu under **Policy** navigate to **Overload and Congestion Control**, select **Congestion Control** and select **Thresholds**.

   This opens the **Congestion Control Thresholds** page. The page shows the existing configurations for a specific Policy service. You can add a new threshold profile configuration or copy the existing profile and modify it.

Figure 7-68 Congestion Control Thresholds



2. Select from the drop down list fields, as described in the following table:

Table 7-262 Thresholds Configuration

Field Name	Description
Service Name	Provides a drop down lists of Policy services. You can select the service for which the congestion control thresholds are to be configured.
Threshold Profiles	Provides a drop down lists of all the configured threshold profiles. A default congestion control threshold profile is provided during PCF deployment. You cannot either edit or delete this profile. If the selected profile is already active, you can see **`Active`** button in green color next to the profile name.

3. Click **Go To Active** button. The current active profile from the **Threshold Profile** drop down list is selected.

Copyright © 2019, 2026, Oracle and/or its affiliates.

4. Click Add.
This opens the **Create Profile** window and allows you to create a new profile.
   a. Enter values for the available input fields, described in the following table:

Table 7-263 Create Profile Configurations

Field Name	Description
Service Name	Specifies the selected PCF service for which a new threshold profile is to be created.
Name of the profile	Provide a unique name for the threshold profile to be created. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.

   b. Click **Create** to create the threshold profile.
To discard the changes, click **Cancel**.
   c. The value gets listed on the Congestion Control Thresholds page.
By default, the newly created profile has the same values as the default profile configuration values.
   d. Click  to view the Queue and CPU values for the various congested states.
   e. Click  to edit each of the various congested states **Queue** and **CPU** values. This opens the **Edit <Congestion States>** page, where <Congestion States> will be different for different services.
The Bulwark pod's can be in following Congestion states:

Table 7-264 Bulwark Congestion States with Default CPU and Queue values

Congestion States	CPU Percentage	Queue Percentage
DANGER_OF_CONGESTION (DOC)	60	6300
CONGESTION_L1	70	7200
CONGESTION_L2	80	8100
CONGESTED	90	9000

> **Note**
>
> If user either adds or updates the Threshold configurations for Bulwark service, then Congestion Control feature gets disabled for Bulwark service. The user will have to enable the congestion control feature again for Bulwark service using the **Settings** menu in CNC Console, and the new/updated Threshold configurations will be applied.

The Binding service pod's can be in following Congestion states:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-265 Binding Service Congestion States with Default CPU and Queue values

Congestion States	CPU Percentage	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	70	30
CONGESTION_L1	75	36
CONGESTION_L2	80	42
CONGESTED	85	48

The SM Service pods can be in following Congestion states:

Table 7-266 SM Services Congestion States with Default CPU and Queue values

Congestion States	CPU Percentage	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	75	720
CONGESTION_L1	80	1080
CONGESTION_L2	85	1440
CONGESTED	90	1800

The Usage Monitoring and PDS Services pods can be in following Congestion states:

Table 7-267 Usage Monitoring and PDS Services Pod Congestion States with Default CPU and Queue values

Congestion States	CPU Percentage	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	65	50
CONGESTION_L1	70	100
CONGESTION_L2	75	150
CONGESTED	80	200

The PCRF Core Services pods can be in following Congestion states:

Table 7-268 PCRF Core Service Congestion States with Default CPU and Queue values

Congestion States	CPU Percentage	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	65	250
CONGESTION_L1	70	300
CONGESTION_L2	75	350
CONGESTED	85	400

The UE Services pods can be in following Congestion states:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-269 UE Service Congestion States with Default CPU and Queue values

Congestion States	CPU Percentage	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	65	1400
CONGESTION_L1	70	2100
CONGESTION_L2	75	2800
CONGESTED	80	3500

The Diameter Gateway Services pods can be in following Congestion states:

Table 7-270 Diameter Gateway Service Congestion States with Default CPU and Queue values

Congestion States	CPU	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	99997	97
CONGESTION_L1	99998	98
CONGESTION_L2	99999	99
CONGESTED	100000	100

The Diameter Connector Services pods can be in following Congestion states:

Table 7-271 Diameter Connector Service Congestion States with Default CPU and Queue values

Congestion States	CPU	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	6300	75
CONGESTION_L1	7200	80
CONGESTION_L2	8100	85
CONGESTED	9000	90

The UDR Connector Services pods can be in following Congestion states:

Table 7-272 UDR Connector Service Congestion States with Default CPU and Queue values

Congestion States	CPU	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	50	2100
CONGESTION_L1	55	2400
CONGESTION_L2	60	2700
CONGESTED	65	3000

The CHF Connector Services pods can be in following Congestion states:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-273 CHF Connector Service Congestion States with Default CPU and Queue values

Congestion States	CPU	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	60	3000
CONGESTION_L1	65	3400
CONGESTION_L2	70	3800
CONGESTED	75	4200

The Notifier Connector Services pods can be in following Congestion states:

Table 7-274 Notifier Connector Service Congestion States with Default CPU and Queue values

Congestion States	CPU	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	77	140
CONGESTION_L1	78	160
CONGESTION_L2	79	180
CONGESTED	80	200

The AM Services pods can be in following Congestion states:

Table 7-275 AM Service Congestion States with Default CPU and Queue values

Congestion States	CPU	Queue (Pending Requests)
DANGER_OF_CONGESTION (DOC)	75	688
CONGESTION_L1	80	1032
CONGESTION_L2	85	1376
CONGESTED	90	1720

f. Enter the following information:

Table 7-276 Edit <Congestion State> Fields

Field Name	Description
Service Name	Specifies the selected service for which threshold profile configurations are to be edited.
Profile Name	Specifies the selected threshold profile for which DOC type queue and CPU values are to be edited.
Queue	Specifies the Queue percentage for Bulwark and Queue (pending requests) for all other Policy services across all the congestion levels. For Bulwark the range is 1 to 100 and for other services the range is between 1 to 2147483647.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-276 (Cont.) Edit <Congestion State> Fields

Field Name	Description
CPU	Specifies the CPU percentage across all the congestion levels. The number can be between 1 to 100.

g. Click **Save** to save the configurations.
To discard the changes, click **Cancel**.

The updated value gets listed on the Congestion Control Thresholds page.

5. Click  . This opens the **Copy Profile** window to copy an existing profile.
While using the copy profile option, whichever profile is selected in the **Threshold Profile** drop down, the values are copied from that profile.

6. Click  . This deletes the selected threshold profile. User cannot delete the default and active threshold profiles.

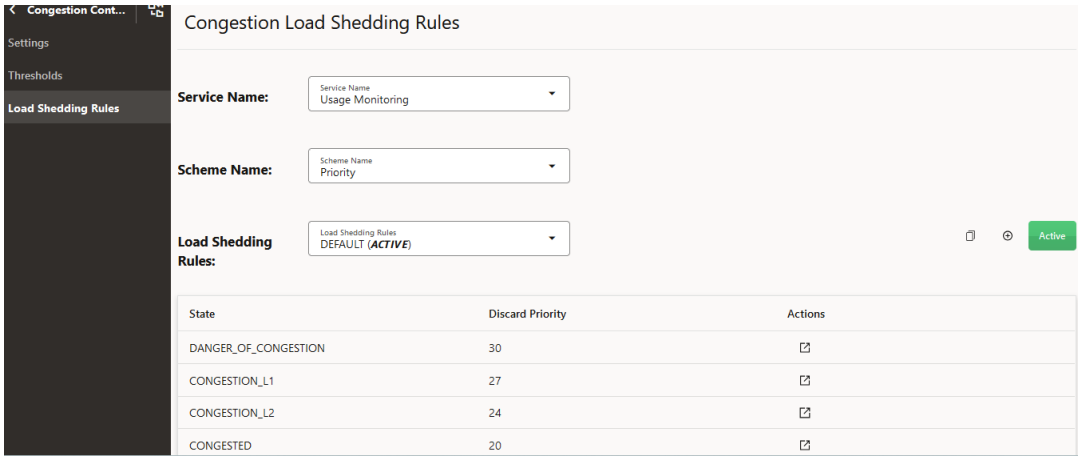
7.10.3.3 Load Shedding Rules

The Congestion Load Shedding Rules page allows you to create new and manage existing congestion load shedding rules.

To configure Congestion Load Shedding rules, perform the following steps:

1. From the navigation menu under **Policy** navigate to **Overload and Congestion Control**, select **Congestion Control** and then select **Load Shedding Rules**.
This opens the Congestion Load Shedding Rules page. The page shows the existing configurations for a specific Policy service. You can add a new congestion control load shedding rule or copy the existing rule and modify it.

Figure 7-69 Congestion Load Shedding Rules



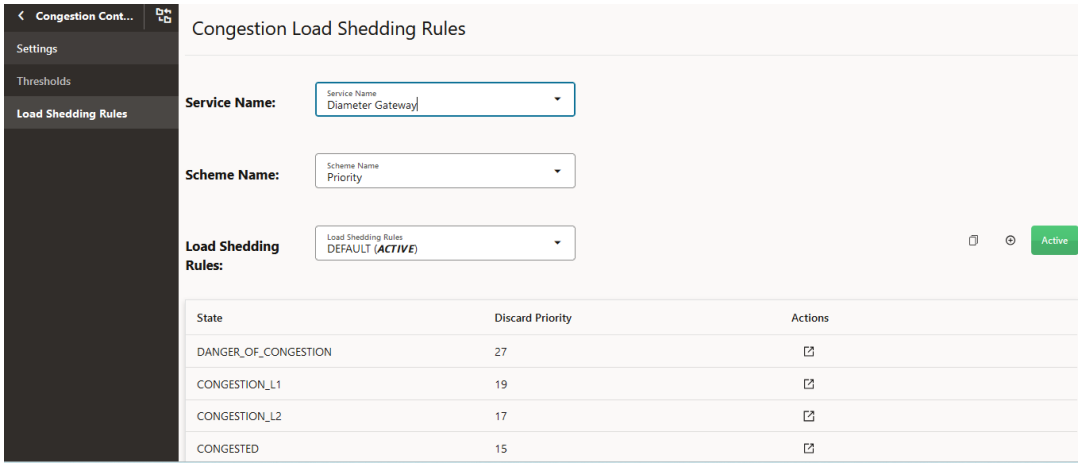
2. Select from the drop down list fields, as described in the following table:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-277 Congestion Load Shedding Rules

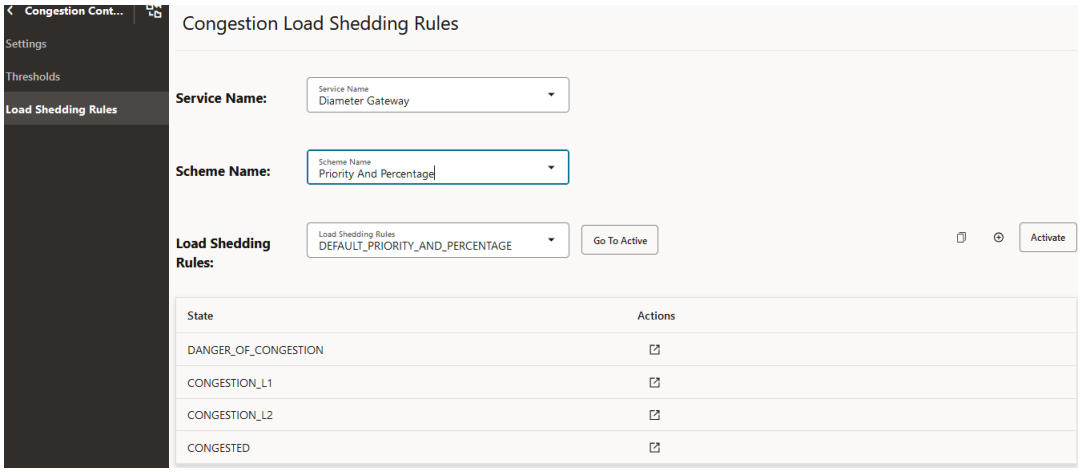
Field Name	Description
Service Name	Provides a drop down lists of Policy services. You can select the service for which the congestion load shedding rules are to be configured.
Scheme Name	Provides different schemes to configure load shedding rules. Currently following two types of load shedding can be performed in Policy: • **Priority** • **Priority And Percentage** All Policy services by default uses `Prioirty` scheme to perform the request discards. Currenlty, for Diameter Gateway services you can use both the scheme types to configure the discards. But for other policy services, `Priority` scheme only can be used.
Load Shedding Rules	Provides a drop down lists of all the configured load shedding rules. A default load shedding rule is provided during PCF deployment. You cannot either edit or delete this rule. If the selected profile is already active, you can see **`Active`** button in green color next to the profile name.

Figure 7-70 Diameter Gateway Congestion Load Shedding Rules with Scheme Name set to "Priority"



Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-71 Diameter Gateway Congestion Load Shedding Rules with Scheme Name set to "Priority And Percentage"



3. Click **Go To Active** button. The current ACTIVE rule from the **Load Shedding Rules** drop down list is selected.

4. Click Add.
This opens the **Create rule** window and allows you to create a new rule.

   a. Enter values for the available input fields, described in the following table:

Table 7-278 Create Rule Configurations

Field Name	Description
Service Name	Specifies the selected PCF service for which a new load shedding rule is to be created.
Name of the rule	Provide a unique name for the load shedding rule to be created. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.

   b. Click **Create** to create the load shedding rule.
To discard the changes, click **Cancel**.

   c. The value gets listed on the Congestion Load Shedding Rules page.
By default, the newly created rule has the same values as the default rule configuration values.

> **Note**
>
> Before performing the Policy upgrade, check for load shedding profiles having discard priority value greater than 31. If it exists then ensure to change this to any value in the range of 0-31.

   d. Click to view the Discard Priority values for the various congested states.
The Bulwark pod's can be in following Congestion states:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-279 Bulwark Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	27
CONGESTION_L1	19
CONGESTION_L2	17
CONGESTED	15

The Binding service pod's can be in following Congestion states:

Table 7-280 Binding Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	30
CONGESTION_L1	27
CONGESTION_L2	24
CONGESTED	20

The SM service pod's can be in following Congestion states:

Table 7-281 SM Services Pod Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	27
CONGESTION_L1	19
CONGESTION_L2	17
CONGESTED	15

The Policy service pod's can be in following Congestion states:

Table 7-282 Usage Monitoring and PDS Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	28
CONGESTION_L1	20
CONGESTION_L2	17
CONGESTED	15

The PCRF Core service pod's can be in following Congestion states:

Table 7-283 PCRF Core Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	29
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

Copyright © 2019, 2026, Oracle and/or its affiliates.

The UE service pods can be in following Congestion states:

Table 7-284 UE Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	28
CONGESTION_L1	25
CONGESTION_L2	20
CONGESTED	17

Table 7-285 Diameter Gateway Congestion States with Default Discard Priority

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	27
CONGESTION_L1	19
CONGESTION_L2	17
CONGESTED	15

The Diameter Connector service pods can be in following Congestion states:

Table 7-286 Diameter Connector Congestion States with Default Discard Priority

Congestion State	Discard Priority (Default Value)
DANGER_OF_CONGESTION	28
CONGESTION_L1	25
CONGESTION_L2	20
CONGESTED	17

The UDR Connector service pods can be in following Congestion states:

Table 7-287 UDR Connector Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	29
CONGESTION_L1	23
CONGESTION_L2	17
CONGESTED	15

The CHF Connector service pods can be in following Congestion states:

Table 7-288 CHF Connector Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	29
CONGESTION_L1	23

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-288 (Cont.) CHF Connector Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
CONGESTION_L2	17
CONGESTED	15

The Notifier service pods can be in following Congestion states:

Table 7-289 Notifier Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	27
CONGESTION_L1	19
CONGESTION_L2	17
CONGESTED	15

The AM service pods can be in following Congestion states:

Table 7-290 AM Service Congestion States with Default Discard Priority

Congestion States	Discard Priority
DANGER_OF_CONGESTION (DOC)	28
CONGESTION_L1	25
CONGESTION_L2	20
CONGESTED	17

e. Click  to edit each of the various congested states **Discard Priority** value. This opens the **Edit <Congestion States>** page, where <Congestion States> will be different for different services.

f. Enter the following information:

Table 7-291 Edit <Congestion State> Fields

Field Name	Description
Service Name	Specifies the selected PCF service for which the load shedding rule is edited.
Rule Name	Specifies the selected load shedding rule for the chosen Congestion state.
Discard Priority	Specifies the discard priority that can be configured for the selected Congestion state. This number can be between 0 to 31.

g. Click **Save** to save the configurations.
To discard the changes, click **Cancel**.

The updated value gets listed on the Congestion Load Shedding Rules page.

5. Click  . This opens the **Copy Rule** window to copy an existing profile.

Copyright © 2019, 2026, Oracle and/or its affiliates.

While using the copy rule option, whichever rule is selected in the **Load Shedding Rules** drop down, the values are copied from that rule.

6. Click  . This deletes the selected load shedding rule. User cannot delete the default and active load shedding rules.

7.10.4 Overload Control Threshold

To open Overload Control Threshold page:

1. From the navigation menu under **Policy**, navigate to **Overload Control Configurations**, and select **Overload Control Threshold**.

   Overload Control Threshold page is displayed. The page shows the existing configurations.

2. Policy allows you to configure the threshold values using a profile. You can either use a default or custom profile or create a new profile. You must activate one of the profiles to use the values. At a time, you can activate only one profile.

   > **Note**
   >
   > If there are no profiles activated, Policy calculates the load level based on `overloadLevelThreshold` configured in `custom-values.yaml` file.

   If you are upgrading from an older version of Policy to 23.1.0 or later, the following message appears at the top of the page:

   ```
   System looks to be using old configuration (Not profile based). Request you to
   please migrate the data or activate one of the profile
   ```

   a. Click **Migrate**.
   Migrate Data window opens.

   b. Enter the name of the profile.

   c. Either click **Migrate** to migrate the data from the previous version of Policy or click **Migrate and Activate** to migrate the data and activate the profile.

   > **Note**
   >
   > Migrate button will only migrate the existing threshold data to profile. It does not activate the profile. Until one of the profile is not active , the UI will continue to show the above message to migrate the data.
   >
   > In case of fault recovery, the active profile details are recovered and used from the database. No need to migrate again.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-292 Create and Manage Threshold Profiles

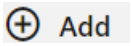
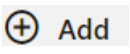
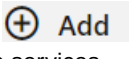
Button/icon	Action
	Opens the **Create Profile** window and allows you to create a new profile. By default, the values of the default profile are associated with the new profile. Click  next to each of the services to edit the values.
	Deletes the selected threshold profile. **Note**: You cannot delete the default system provided profile.
	Opens the **Copy Profile** window to copy an existing profile. While using the copy profile option, whichever profile is selected in the **Threshold Profile** dropdown, the values are copied from that profile.
Threshold Profile	Lists all the threshold profiles. You can select any of the profiles from the list to activate. If the selected profile is already active, you can see **(ACTIVE)** button in green color next to the profile name.
Activate	Activates the profile selected from **Threshold Profile** list. At a time, you can have only one active profile.
Go To Active	**Go To Active** button selects the current active profile from the **Threshold Profile** drop down list. **Note**: If none of the profiles are active, the **Go To Active** button does not appear.

Table 7-293 Configure Threshold Values

Configuration	Description
Service Name	You can configure the threshold values for the following services: • PCRF Core • Diameter Connector • PCF Session Management • PCF Access and Mobility • PCF UE Policy • CHF Connector • UDR Connector **Note**: Irrespective of PCF or PCRF mode of deployment, this list of services remains the same. For PCRF-CORE deployment mode, configuring overload level threshold for SM Service, AM Service, and UE Policy Service is not required. For PCF deployment mode, configuring the overload level threshold for PCRF Core is not required.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-293 (Cont.) Configure Threshold Values

Configuration	Description
CPU	Click  to view the abatement and onset values for each of the levels (L1, L2, and L10). The onset and abatement values for CPU are calculated in percentage (%) and the range is from 1 to 100. Click  to edit the abatement and onset values for each of the levels. In the **Edit CPU** window, click **Add** to add new load levels and configure the **Abatement Value (%)** and **Onset Value (%)** for each level. For every service, Overload Control Threshold for L1, L2, L3 load levels must be configured. For PCF SM service, and Diameter Connector services, new load levels can be added by clicking the **Add** button and configured up to L10. For other services, Policy supports only L1-L3 load levels and does not allow to add any load level beyond L3. For PCF SM service, and Diameter Connector services, load levels added beyond L3 can be deleted using the **Delete** button. Clicking the **Delete** button deletes the highest load level configuration. That is, if L1-L8 load levels are configured for PCF SM service, clicking the **Delete** button deletes L8 from the configuration. **Note**: Make sure that the onset value of L1 is less than the abatement value of L2 and the onset value of L2 is less than the abatement value of L3 and so on. You can click  to delete the CPU values for a service. The application prompts you to confirm before deleting the values. **Note**: If the above mentioned CPU validation fails for any of the threshold levels, importing of the Overload Threshold Profile will be rejected.
Pending Message Count	Click  to add the pending message count for each of the services. Pending message count accepts an integer value between 1 to 1000000.
Failure Count	Click  to add the failure count for each of the services. The failure count accepts an integer value between 1 to 1000000.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-293 (Cont.) Configure Threshold Values

Configuration	Description
Memory	Click Add to add the abatement and onset memory values for each of the three levels (L1, L2, and L3). Memory details are calculated in Percentage (%) and ranges between 1 to 100.

7.10.5 Advance Overload Control

This section describes the procedure to perform overload control configurations.

7.10.5.1 Overload Configurations

To open Overload Configurations page:

1. From the navigation menu under **Policy**, navigate to **Overload and Congestion Control Configurations**. Under **Advance Overload Control** select **Overload Configurations**.

   Overload Configurations page is displayed. The page shows the existing configurations.
2. Policy allows you to perform overload configurations using a Overload Profile. You can either use an existing profile or create a new profile.

   The **Type to Filter** text box allows to filter the required list of profiles based on a given keyword.
3. Click **Refresh** (Refresh) to refresh the list of existing Overload Profile Names.
4. Click **Add** (Add) to create a new Overload Profile.

Table 7-294 Create Overload Configuration

Field Name	Description
Overload Profile Name	Unique name to represent Overload configuration profile created.
Service Type	Specifies the Policy microservice for which the Overload Configurations are applied. Currently, Policy supports only PCF Session Management service.
Message Profile	The associated message profile containing rules for handling different message types and their attributes during overload. Provides a dropdown selection from pre-configured message profiles.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-294 (Cont.) Create Overload Configuration

Field Name	Description
Overload Rules	Overload Rules are created where mapping of system `Load Level` is done with `MessageIDs`, along with `Conditional Message Priority` and `Reject Percentage` is defined for the rule as well. Define the overload rules as described in Table 7-295 table. **Note**: Before deleting any Message Profile, make sure to verify and remove existing associations of the Message Profile with any of the Overload Rules.

Table 7-295 Add Overload Rules

Field Name	Description
Level	Specifies the overload severity level at which the mapped rule must be applied. Select any of the following values using the drop-down list: • L1 • L2 • L3 • L4 • L5 • L6 • L7 • L8 • L9 • 10
Message ID	Unique identifier representing a combination of message rule parameters, including request type, message type, attributes, interface type, and priority. Message ID must map to a configured message profile.
Message Priority	This field is used to configure priority-based rejections. It specifies a priority number. Messages with priority greater than or equal to the specified number is selected for Overload actions. The number is automatically preceded by Greater than or equal to condition(>=) The Message Priority value must be between 0 and 31.
Service Profile	This field allows to select one of the service profiles created on **Service Profile** page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-295 (Cont.) Add Overload Rules

Field Name	Description
Service Profile Apply Percentage	This field appears when the **Service Profile** field is configured. Specifies the percentage of messages selected to perform 'Assume Positive' action where service interactions are skipped for the configured Overload rule. **Note**: Service Profile Apply Percentage together with Reject Percentage should not exceed 100%. **Range**: 0 to 100
Reject Percentage	Specifies the percentage of matching messages to be rejected when the overload level is triggered. **Default value**: 100 **Range**: 0 to 100 **Note**: If a Overload reject action is written for Create, Update, or Delete for DNN1. During an overload state, if the value of DNN1 is changed to DNN2 within the DNN Profile and there are overload actions written for DNN2 and DNN1 actions are removed as well, although expectation with this use case can be that for DNN1 Update or Delete overload control action should not be performed, but in this use case Update or Delete overload control action is performed for DNN1.
Rule Priority	Indicates the evaluation priority among multiple overload rules. Higher priority rules are matched first. **Range**: 1-65535
Error Code	Specifies the error code returned to requests when the reject percentage triggers rejection due to overload. This value is selected from a predefined list of error codes relevant to each message type and protocol being handled. For details on how to create and manage error code profiles collection, see SBI Ingress Error Code Profiles Collection. The default error code if not configured with the Overload Reject action will Return `503` Error with cause as `NF_Congested`. One of the parameters for load level calculation at Perf-info is based on Failure Counts received for a service at Ingress Gateway. Overload reject actions being performed at SM service are not required to be accounted for failure count calculation, as these are known rejections configured by the end user under known conditions. To avoid these load level calculation, it is required that Error code being used for rejection at SM service is not required to be configured for 'Route Level mapping' of N7/N5 interface requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

5. Click **Save** to save the Overload configurations.

7.11 Controlled Shutdown Configurations

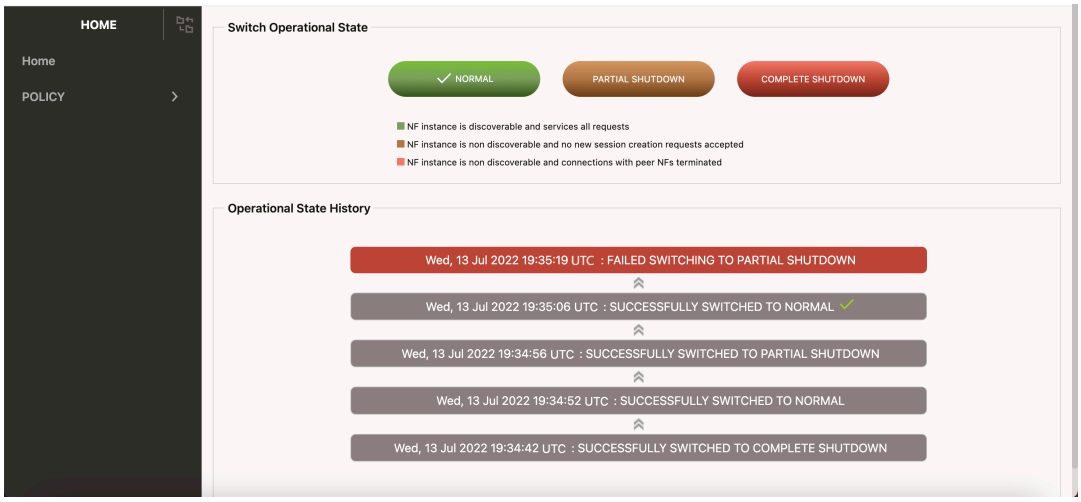
This section describes how to perform Controlled Shutdown configurations for Diameter and Ingress interface.

7.11.1 Operational State

To change Operational State of a site:

- From the navigation menu, under **Policy**, click **Controlled Shutdown**, and then select **Operational State**.
  This opens the page displaying the two groups, **Switch Operational State** and **Operational State History**:

Figure 7-72 Operational State



  - Switch Operational State It displays the following operational states:
    * NORMAL: NF instance is discoverable and services all requests.
    * PARTIAL SHUTDOWN: NF instance is non discoverable and no new session creation requests accepted.
    * COMPLETE SHUTDOWN: NF instance is non discoverable and no new session creation requests accepted.

> **Note**
>
> By default, NORMAL state is assigned to a site. The current state of any site can be identified with a tick mark.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> The operational state is stored in configuration server. The service instances (pod) detects the state change only after the configuration refresh is performed. Hence if the config refresh interval is set at 5 seconds then te pods recognise the operational state change after 5 seconds.

You can switch to a different operational state by clicking the NORMAL, PARTIAL SHUTDOWN, or COMPLETE SHUTDOWN button.

– Operational State History: It displays the history of the operational states along with the timestamp.

> **Note**
>
> It displays maximim of ten records at a time. On scrolling further, another set of ten records is displayed. The maximum number of record maintained is hundred.

7.11.2 Diameter Error Mapping

To configure Diameter Error Mapping, perform the following steps:

1. From the navigation menu under **Policy**, click **Controlled Shutdown** and then select **Diameter Error Mapping**.
   This opens the **Diameter Error Mapping** page. The page lists the existing configurations. You can add or import new diameter error mapping configurations using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the Create Diameter Error Mapping page.

3. On the **Create Diameter Error Mapping** page, enter the following information:

Table 7-296 Create Diameter Error Mapping

Field Name	Description
Message Type	Type of the request

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-296 (Cont.) Create Diameter Error Mapping

Field Name	Description
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of congestion control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • CUSTOM_RESULT_CODE **Note**: When the CUSTOM_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Use Experimental Result Code**: This is disabled by default. You can enable it by clicking the icon against it. When it is enabled, Vendor ID field is populated on the page: – **Vendor ID**: Enter a valid value to specify vendor ID.

4. Click **Save**.
   The configuration gets listed on the **Diameter Error Mapping** page. The page defines the Diameter Error Mapping configuration in the Policy database and it is available to be used in a Policy.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the configuration.

Importing Diameter Error Mapping

To import Diameter Error Mapping configuration:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

7.11.3 SBI Ingress Error Mapping

To configure SBI Ingress Error Mapping, perform the following steps:

1. From the navigation menu, under **Policy**, click **Controlled Shutdown**, and then select **SBI Ingress Error Mapping**.
   This opens the SBI Ingress Error Mapping page.
2. Click Edit.
   This opens the Edit SBI Ingress Error Mapping page.

Copyright © 2019, 2026, Oracle and/or its affiliates.

3. Click Add .

   This opens the Add SBI Ingress Error Mapping page.

4. Enter values for the available input fields as described in the following table:

Table 7-297 Ingress Error Mapping Configurations

Field Name	Description
Id	Specifies the list of IDs available for Policy.
Error Code Profile	Select an error code profile from the dropdown list. It displays the list of error profiles configured using the SBI Ingress Error Code Profiles Collection.

5. Click **Save** to save the Ingress error mapping.
   To discard the changes, click **Cancel**.

   The value gets listed on the SBI Ingress Error Mapping page. Use or available under the **Actions** column to update or delete the profile.

7.12 NF Scoring Configurations

You can configure the NF Scoring feature using the CNC Console. To navigate to NF Scoring, click NF Scoring, under Policy. It shows Settings and Calculated Score, which are described as follows:

Settings:

Table 7-298 CNC Console NF Scoring Settings

Field Name	Description
Enable NF Scoring	Specifies whether to enable or disable the NF Scoring. **Note**: Enabling the NF Scoring feature for the first time, requires configuring `prometheusUrl` and `alertmanagerUrl` under the `appinfo` and `perfinfo` sections in the `custom-yaml`. These Urls get reflected in the config-map of AppInfo and Perf-Info services. For AppInfo and PerfInfo pods to pick up these changes, they need to be restarted.
TPS	
Enable	Enables the TPS.
Max Score	Specifies the maximum score of the TPS.
Max TPS	Specifies the maximum TPS.
Service Health	Specifies the service health of a site.
Enable	Enables the Service Health.
Max Score	Specifies the maximum score of the Service Health.
Signaling Connections	Specifies the Signaling Connections of a site.
Enable	Enables the Signaling Connections.
Max Score	Specifies the maximum score of the Signaling Connections.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-298 (Cont.) CNC Console NF Scoring Settings

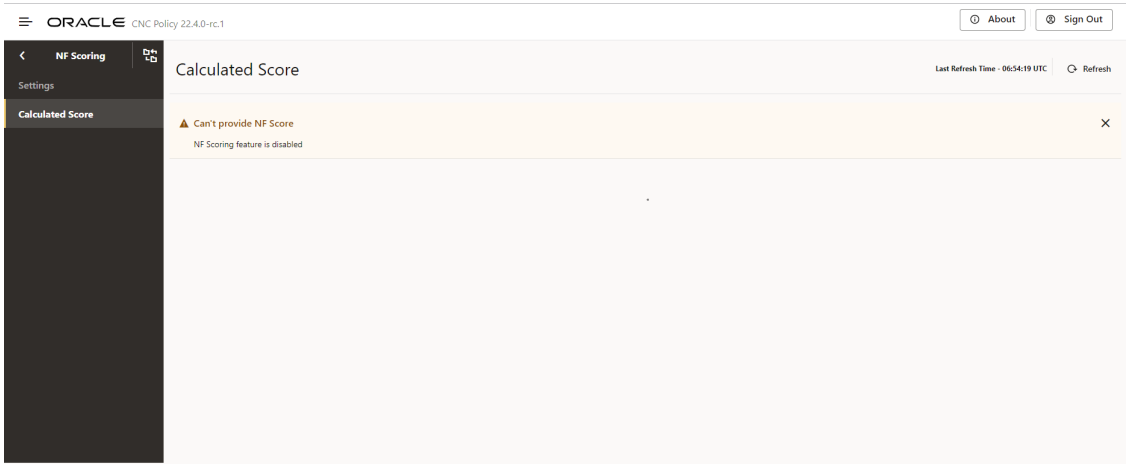
Field Name	Description
Max Connections	Specifies the maximum connections. **Range**: 1 to 10000
Replication Health	Specifies the Replication Health of a site.
Enable	Enables the Replication Health.
Max Score	Specifies the maximum score of the Replication Health.
Locality/Site Preference	Specifies the Locality or Site Preference.
Enable	Enables the Locality or Site Preference.
Score	Specifies the score of the Locality or Site Preference.
Active Alert	Specifies the Active Alerts of a site.
Enable	Enables the Active Alert.
Critical Alert Weightage	The site with more critical alerts is unhealthy.
Major Alert Weightage	The site with more major alerts is unhealthy.
Minor Alert Weightage	The site with more minor alerts is unhealthy.

Calculated Score:

To check the calculated Score of a site:

From the navigation menu, under Policy, click NF Scoring and then select Calculated Score. This opens the page displaying the Calculated Score.

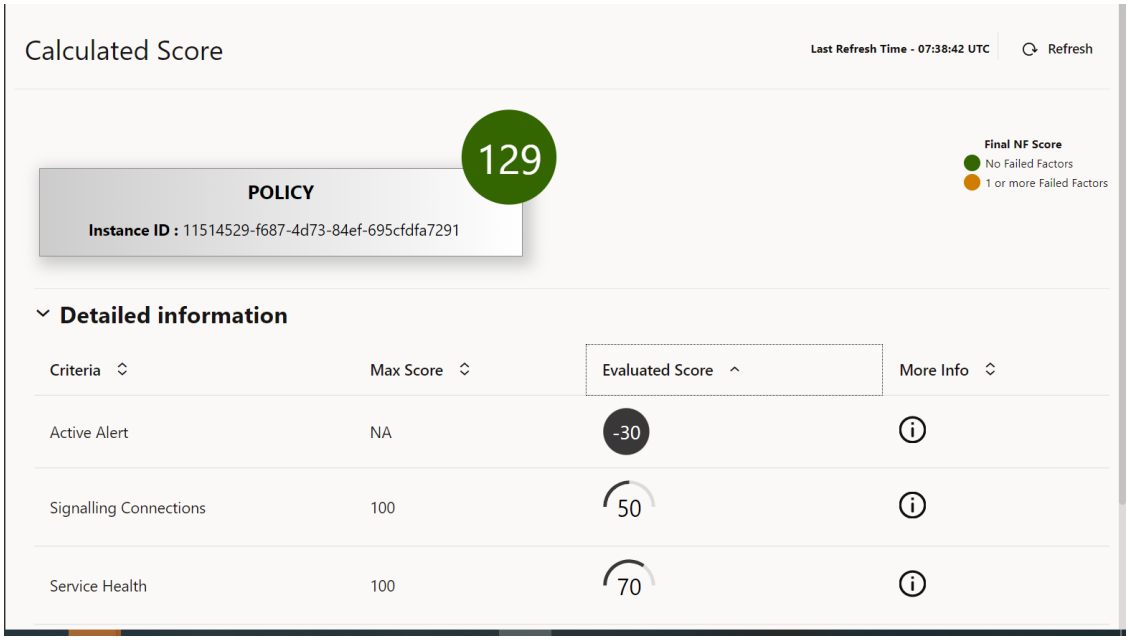
Figure 7-73 NF Scoring Disabled



If the NF Scoring feature is enabled. The calculated Screen page displays as:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Figure 7-74 NF Scoring Enabled



> **Note**
>
> If app-info pod is down, you will not be getting the NF Score. You will get an error message that "Data can't be fetched due to internal server error".

Calculated Score shows the total score along with the Instance ID. The total score is shown in either Green or Orange color. If the NF Score is shown in green color there are no failed factors. And, if the NF Score is shown in Orange color there are one or more failed factors. You can click on **Detailed information** to view different criteria and their Max Score, Evaluated Score, and More Info. The criteria in the detailed information tab show the evaluated score. The failed factors are shown with a warning symbol under the evaluated score.

On the top-right of the screen, the *Last Refresh Time* information is available. Moreover, a *Refresh* button is given to refresh the NF Score of a site.

7.13 Viewing cnDBTier APIs in CNC Console

Perform the following procedure to view the cnDBTier version, status of cnDBTier clusters, georeplication status, and georeplication recovery status on the CNC Console.

> **Note**
>
> The following cnDBTier functionalities are read only and is available only through CNC Console.

7.13.1 Backup List

Perform the following procedure to view the list of completed backups:

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **Backup List** to view the list of completed backups along with Backup ID, Backup size, and Creation Timestamp.
   The **Backup List** page is displayed.

Table 7-299 Backup List

Fields	Description
Backup Details	This field displays information such as backup Id, backup size, and backup creation timestamp.
Site Name	This field displays the name of the current site to which Policy is connected.
Backup Id	This field displays the ID of the stored backup.
Backup Size (bytes)	This field displays the size of the stored backup.
Creation TimeStamp	This field displays the time recorded when the backup was stored.

7.13.2 Database Statistics Report

Perform the following procedure to view the available database:

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **Database Statistics Report** to view the available database.

Table 7-300 Database Statistics Report

Fields	Description
Database Count	This field displays the number of available database.
Database Tables Count	This field displays the available database names and their table count.
Database Name	This field displays the database name.
Table Count	This field displays the table count for each database.
Database Table Rows Count	This field displays the table rows present in each table.

   a. Click the **View** icon available next to the database name to view the **View Database Table Rows Count** page.

Table 7-301 View Database Table Rows Count

Fields	Description
Database Name	This field displays the database name.
Tables	This field displays the table names and the corresponding rows in each table.
Table Name	This field displays the table name.
Row Count	This field displays the table rows present in each table.

7.13.3 Georeplication Status

Perform the following procedure to view the local site and remote site name to which Policy is connected.

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **Georeplication Status** to view the local site and remote site name to which Policy is connected.

Table 7-302 GeoReplication Status

Fields	Description
Local Site Name	This field displays the local site name to which Policy is connected.
Remote Site Name	This field displays the remote site name.
Replication Status	This field displays the replication status with corresponding sites.
Seconds Behind Remote Site	This field displays the number of seconds that the last record read by the local site is behind the latest record written by the remote site for all the replication groups.

a. Click the **View** icon in the **Actions** menu to view the **View Georeplication Status** page.

Table 7-303 Georeplication Status

Fields	Description
Replication Group Delay	This field displays the number of seconds that the last record read by the local site is behind the latest record written by the remote site for individual replication groups.
Replication Channel Group Id	This field displays the ID of the replication channel group.

b. Click the **View** icon to view the **Replication Group Delay** attributes.

Table 7-304 View Replication Group Delay

Fields	Description
Channel Details	This field displays the channel details such as Remote Replication IP and Role.
Remote Replication IP	This field displays the IP of the remote replication channel.
Role	This field displays the role of the replication channel IP.

7.13.4 Georeplication Status Across All Sites

Perform the following procedure to retrieve the georeplication status across all configured sites, offering a consolidated view of the overall replication health:

1. From the navigation menu, click **Policy**, and then click **DB Tier**.
2. Click **Georeplication Status Across All Sites** to access the georeplication status across all configured sites in the cnDBTier cluster.
   The **Georeplication Status Across All Sites** page is displayed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-305 Georeplication Status Across All Sites

Fields	Description
Site Name	This field displays the primary site for which the georeplication status is being reported.
Remote Site Name	This field displays the remote site involved in replication with the local site.
Site To Mate Site Replication Status	This field displays the overall georeplication status with all the groups.
Replication Details Per Group ID	This field displays the list of replication-group-specific details with the site name and the remote site name.

3. Click the  option to view the **View Georeplication Status Across All Sites** attributes.
   The **View Georeplication Status Across All Sites** page is displayed.

Table 7-306 View Replication Details Per Group ID

Attribute	Description
Replication Group ID	This field displays the unique identifier assigned to the replication group.
Replication Channel Group Status	This field displays the replication status for the specific replication group.
All SQL Status Details	This field displays the detailed SQL and replication state information for all SQL nodes for the specified replication group.

4. Click the  option to view the **View All SQL Status Details** attributes.
   The **View All SQL Status Details** page is displayed.

Table 7-307 View All SQL Status Details

Attribute	Description
SQL Node	This field displays the SQL node whose replication metrics are being reported.
Source Host	This field displays the remote host from which the SQL node pulls replication data.
External IP	This field displays the external endpoint through which the SQL node is accessible within the site.
Replica I/O Running Status	This field displays whether the replication I/O thread is currently active or not. Possible values: Yes or No.
Replica SQL Running Status	This field displays whether the SQL thread responsible for applying replicated changes is running or not. Possible values: Yes or No.
Server ID	This field displays the unique server identifier used in the replication topology.
Role	This field displays the role of the SQL node within the replication setup (for example, ACTIVE or STANDBY).
Last Error Code	This field displays the most recent SQL thread error code encountered during replication.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-307 (Cont.) View All SQL Status Details

Attribute	Description
Last Error Message	This field displays the most recent error message reported by the SQL thread.
Last I/O Error Code	This field displays the most recent I/O thread error code encountered during replication.
Last I/O Error Message	This field displays the most recent error message reported by the I/O thread.
Last SQL Error Code	This field displays the most recent SQL execution error code encountered while applying replicated transactions.
Last SQL Error Message	This field displays the last SQL execution error message reported.
SQL Remaining Delay	This field displays the replication lag or delay (if any) between the source site and this SQL node. Unit: seconds.

7.13.5 cnDBTier Health

1. From the navigation menu, click **Policy**, and then click **DB Tier**.
2. Click **cnDBTier Health** to view the health status of the microservices like replication, backup manager, monitor services, and NDB services.
   - Click **Backup Manager Health Status** to view the health status of the backup manager.
     The **Backup Manager Health Status** page is displayed.

> **Note**
>
> The parameters listed in the below table are read-only.

Table 7-308 Backup Manager Health Status

Fields	Description
Service Name	This attribute displays the service name of the backup manager microservice.
Service Status	This attribute displays the service status of the backup manager microservice. Possible values are UP and DOWN.
DB Connection Status	This attribute displays the database connection status of the backup manager microservice. Possible values are UP and DOWN.
Overall Backup Manager Service Health	This attribute displays the overall health status of the backup manager microservice. Possible values are UP and DOWN.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-308 (Cont.) Backup Manager Health Status

Fields	Description
Backup Executor Health Status	This attribute displays the following information like node id and DB connection status of the backup executor. – Node Id: This attribute displays the id of the node. – DB Connection Status: This attribute displays the backup executor database connection status with the nodes. Possible values are UP and DOWN.

- Click **Monitor Health Status** to view the health status of the services.
The **Monitor Health Status** page is displayed.

> **Note**
>
> The parameters listed in the below table are read-only.

Table 7-309 Monitor Health Status details

Attribute	Description
Service Name	This attribute displays the service name of the monitor microservice.
DB Connection Status	This attribute displays the database connection status of the monitor microservice. Possible values are UP and DOWN.
Metric Scrape Status	This attribute displays the status of the metric scrape, that is if the metrics are fetched or not. If the metrics are fetched then the service is up and vice versa. Possible values are UP and DOWN.
Overall Monitor Service Health	This attribute displays the overall health status of the monitor microservice. Possible values are UP and DOWN.

- Click **NDB Health Status** to view the health status of the network database.
The **NDB Health Status** page is displayed.

> **Note**
>
> The parameters listed in the below table are read-only.

Table 7-310 NDB Health Status details

Attribute	Description
Local Site Name	This attribute displays the name of the current site. For example, site 1, site 2.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-310 (Cont.) NDB Health Status details

Attribute	Description
NDB Health Status Details	This attribute displays the health status of the network database like name of the NDB service, status of the service, health status of PVC.
Service Name	This attribute displays the service name. For example, ndbmgmd-0, ndbmtd-0, ndbmyappsqld-1, ndbmysqld-2.
Service Status	This attribute displays the status of the service. Possible values are UP and DOWN.

- Click **Replication Health Status** to view the health status of the replication sites. The **Replication Health Status** page is displayed.

> **Note**
>
> The parameters listed in the below table are read-only.

Table 7-311 Replication Health Status details

Attribute	Description
Local Site Name	This attribute displays the name of the current site (site 1, site 2).
Health Status Details	This attribute displays the health status details of the local site like replication service name, replication service status, database connection status of the replication service, and the overall health status of the replication micorservices. The number of rows in this table varies depending on the type of deployment (for example, two-site, three-site deployments).
Service Name	This attribute displays the name of the available replication service.
Service Status	This attribute displays the status of the available replication service. Possible values are UP and DOWN.
DB Connection Status	This attribute displays the database connection status of the replication microservice. Possible values are UP and DOWN.
Overall Replication Service Health	This attribute displays the overall health status of the replication microservice. Possible values are UP and DOWN.

7.13.6 Heartbeat Status

Perform the following procedure to view the connectivity between local site and remote site name to which Policy is connected.

Copyright © 2019, 2026, Oracle and/or its affiliates.

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **HeartBeat Status** to view the connectivity between local site and remote site to which Policy is connected.

Table 7-312 HeartBeat Status Details

Fields	Description
Site Name	This field displays the name of the current site to which Policy is connected.
HeartBeat Details	This field displays information such as the remote site name, heartbeat status, heartbeat lag, and replication channel group id.
Remote Site Name	This field displays the remote site name.
Heartbeat Status	This field displays the connectivity status with corresponding sites.
Heartbeat Lag	This field displays the lag or latency in seconds it took to synchronize between sites.
Replication Channel Group Id	This field displays the ID of the replication channel group.

7.13.7 IP Family Reference

1. From the left navigation menu, navigate to **DBTier** and then click **IP Family Preference**. The **IP Family Reference** page is displayed.
2. Click **Actions** to view the IP preference set for the sites.
   a. The **Edit IP Preference** page is displayed.

Table 7-313 IP Family Preference

Fields	Description
Local Site Name	This attribute displays the name of the current site to which PCF is connected.
Remote Site Name	This attribute displays the remote site name.
Preferred Family	This attribute displays the current site's preferred IP family type. IPV4- Indicates the IP Type selected is IPV4. IPV6- Indicates the IP Type selected is IPV6.
Status	This attribute displays the status of the IP family switchover. Values are RUNNING/IN-PROGRESS.

Copyright © 2019, 2026, Oracle and/or its affiliates.

7.13.8 Georeplication Recovery

> **Note**
>
> - Currently, if a site is used for georeplication recovery has failures, then it should not be marked as failed. Instead, the user must troubleshoot the issues and resolve it manually rather than mark it as failed.
> - All the georeplication sites must be on the same cnDBTier version as 24.2.x to perform georeplication recovery. However, you can perform georeplication recovery on a different cnDBTier version if it is newer than 24.2.x.
> - User must wait until all the GRR process is complete before selecting the same site for another site's georeplication recovery.

Perform the following procedure to mark cnDBTier cluster as failed, execute georeplication recovery, and monitor their status:

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **Georeplication Recovery** to access the Georeplication Recovery Status of the cnDBTier cluster. This includes options such as Update Cluster As Failed, Start Georeplication Recovery, and Georeplication Recovery Status.
   - Click the **Update Cluster As Failed** to mark the cluster as FAILED.
     The **Update Cluster As Failed** page is displayed.

Table 7-314 Update Cluster As Failed

Fields	Description
Cluster Names	This attribute lists the names of cnDBTier clusters. It allows you to select a cluster from the available list to mark as failed.
Failed Cluster Names	This attribute displays the list of names of cnDBTier clusters that are marked as failed.
Update Cluster	Click the **Update Cluster** to mark the cluster as FAILED.
Cancel	Click the **Cancel** to cancel the process.

   - Click the **Start Georeplication Recovery** to start the georeplication recovery process for a failed site.
     The **Start Georeplication Recovery** page is displayed.

Table 7-315 Start Georeplication Recovery

Attribute	Description
Failed Cluster Name	This attribute displays a list of cnDBTier clusters that have been marked as failed.
Backup Cluster Name (Optional)	This attribute displays the list of active cnDBTier clusters designated for georeplication recovery.
Start Georeplication Recovery	Click the **Start Georeplication Recovery** to start the georeplication recovery process for a failed site.
Cancel	Click the **Cancel** to cancel the process.

Copyright © 2019, 2026, Oracle and/or its affiliates.

- Click the **Georeplication Recovery Status** to view the status of georeplication recovery for cnDBTier clusters.
  The **Georeplication Recovery Status** page is displayed.

Table 7-316 Georeplication Recovery Status

Attribute	Description
Local Cluster Name	This attribute displays the name of the local cluster.
Georeplication Recover Status Details	This attribute displays the details of the georeplication recovery status for cnDBTier clusters.
Cluster Name	This attribute displays the names of all the clusters.
Georeplication Recovery Status	This attribute displays the current status of georeplication recovery for a cluster.
Refresh	Click **Refresh** to view the most current data.

The following are the states of Georeplication Recovery:

Table 7-317 Georeplication Recovery States

Georeplication Recovery State	Description
ACTIVE	The cluster is in a healthy state, and replication is up and running with its respective mate cluster.
REINSTALLED	The cluster enters this state during fatal error recovery when the end user reinstalls the cluster.
STARTDRRESTORE	When Georeplication recovery is started, the cluster will transition into this state.
INITIATEBACKUP	Once Georeplication recovery is started, the cluster will identify a healthy cluster for backup initiation and transition into this state.
CHECKBACKUP	Once the backup is initiated, the georeplication recovery cluster will monitor the progress of the backup until its completion. If the backup fails, the cluster will restart the backup.
COPY_BACKUP	Upon completion of the backup, the georeplication recovery cluster will request the transfer of the backup from the healthy cluster to the georeplication recovery cluster.
CHECK_BACKUP_COPY	Once backup copy is started georeplication recovery cluster will monitor for the backup transfer progress till it's completion and if it's fails the cluster will re-initiates the backup transfer.
BACKUPCOPIED	Once the backup copy is started, the georeplication recovery cluster will monitor the progress of the backup transfer until its completion. If the transfer fails, the cluster will restart the backup transfer.
BACKUPEXTRACTED	This state indicates that the backup has been successfully extracted at the georeplication recovery cluster, allowing the restoration of the backup to start.
FAILED	This state is used by end user to mark specific cluster as failed and hence georeplication recovery is essential to recover the cluster.This state can also indicates that georeplication recovery started and the database is restored using the healthy cluster backup.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-317 (Cont.) Georeplication Recovery States

Georeplication Recovery State	Description
UNKNOWN	This state is used by the end user to mark a specific cluster as failed, necessitating georeplication recovery for cluster recovery. Additionally, this state can indicate that georeplication recovery has started and the database has been restored using the backup from the healthy cluster.
RECONNECTSQLNODES	This state is used to instruct SQL nodes to be offline during backup restoration to prevent any records from entering the binlog of the georeplication recovery cluster.
BACKUPRESTORE	This state indicates that the backup, successfully copied from the healthy cluster, is currently being used to restore the georeplication recovery cluster.
RESTORED	Once the backup is successfully restored in the georeplication recovery cluster, the cluster will enter this state to start the reestablishment of replication channels.
BINLOGINITIALIZED	This state indicates the start of binlogs for the restoration of replication channels, necessary to start the restore process
RECONFIGURE	Once the binlog is restarted, the georeplication recovery cluster will reestablish the replication channels with respect to all its mate clusters.

7.13.9 Local Cluster Status

Perform the following procedure to view the local cluster status for the current site.

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **Local Cluster Status** to view the local cluster status for the current site:

Table 7-318 Local Cluster Status

Fields	Description
Site Name	This field displays the name of the current site to which Policy is connected.
Cluster Status	This field displays the local cluster status for the current site.

7.13.10 On Demand Backup

Perform the following procedure to view the available database.

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **On Demand Backup** to create a new backup and view the status of initiated on-demand backups.

> **Note**
>
> On Demand Backup can be initiated on both single site and multi-site cnDBTier cluster and can be used to restore the first standalone site. DB Backup will not be initiated if sites are not properly configured.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-319 On Demand Backup Details

Fields	Description
Site Name	This field displays the name of the current site to which Policy is connected.
DR Status	This field displays the status of DR.
Backup Id	This field displays the ID of the stored backup.
Backup Status	This field displays the status of backup.
Remote Transfer Status	The field displays the status of remote transfer.
Initiate Backup	The field displays whether the backup is initiated or not.

a. Click the **Edit** icon.
The **Edit** On Demand Backup screen appears.

> **Note**
>
> The **Edit** mode is available only for Initiate Backup.

b. To enable the Initiate Backup option, click **Save**.
A confirmation message "Save successfully" appears.

c. Click **Cancel** to navigate back to the On Demand Backup screen.

d. Click **Refresh** to reload the On Demand Backup screen.

7.13.11 Version

Perform the following procedure to view the cnDBTier version:

1. From the left navigation pane, click **Policy**, and then click **DB Tier**.
2. Click **cnDBTier Version** to view the version.

Table 7-320 cnDBTier Version Attributes

Fields	Description
cnDBTier Version	This field displays the cnDBTier version.
NDB Version	This field displays the network database (NDB) version.

7.13.12 PCF Cluster DB State

The **DB Cluster and PCF Functional State** page displays the database cluster state in cnDBTier.

To view the database cluster state:

1. From the left navigation pane, click Policy, and then click DB Tier.
2. Click **DB Cluster and PCF Functional State** to view the database cluster state information.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-321 cnDBTier Database Cluster State

Fields	Description
DB Cluster State	Displays the realtime status of the cnDBTier database cluster. The status of the cluster can any of the following: • START • FAILURE • RESTART • RESTORE • CHECKPOINT • RE_SYNC
NF State	Displays whether the database cluster for the Policy is `Running` or `Not_Running`.

7.13.13 Gracefully Stop and Start Georeplication

From the left navigation menu, navigate to **DBTier** and then click **Gracefully Stop and Start Georeplication**. The **Gracefully Stop and Start Georeplication** page is displayed.

1. Click **Stop Georeplication** from the left navigation menu to stop the georeplication between the sites. The **Stop Georeplication** page is displayed.

Table 7-322 Stop Georeplication

Fields	Description
Site Name	This attribute displays the name of the current PCF site.
Remote Site Name	This attribute displays the list of the remote PCF site names.
Replication Channel Group Ids	This attribute displays the list of replication group ids of the current site.
Georeplication Details	This attribute displays the details of the georeplication sites and their status.

Table 7-323 Georeplication Details

Fields	Description
Site Name	This attribute displays the name of the current PCF site.
Remote Site Names	This attribute displays the name of the remote PCF site.
Replication Channel Group Id	This attribute displays the replication group id.
Replication Status	This attribute displays the status of the georeplication between sites. • UP- Indicates the georeplication between the sites is up. • DOWN- Indicates the georeplication between the sites is down.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-323 (Cont.) Georeplication Details

Fields	Description
Switch Over Status	This attribute displays the switch-over status of the georeplication between sites. • SWITCH_OVER_ENABLED- Indicates the switch-over status of the georeplication between the sites is up. • SWITCH_OVER_DISABLED- Indicates the switch-over status of the georeplication between the sites is disabled.

2. Click **Stop Georeplication** to stop the replication between the sites.

Start Georeplication

1. Click **Gracefully Stop and Start Georeplication**. The **Gracefully Stop and Start Georeplication** page is displayed.
2. Click **Start Georeplication** from the left navigation menu to start the georeplication between the sites.
   The **Start Georeplication** page is displayed.

Table 7-324 Start Georeplication

Fields	Description
Site Name	This attribute displays the name of the current site to which PCF is connected.
Remote Site Name	This attribute displays the list of the remote site name.
Replication Channel Group Ids	This attribute displays the list of replication group ids of the current site.
Georeplication Details	This attribute displays the details of the georeplication sites and their status.

Table 7-325 Georeplication Details

Fields	Description
Site Name	This attribute displays the name of the current site to which PCF is connected.
Remote Site Names	This attribute displays the name of the remote site.
Replication Channel Group Id	This attribute displays the replication group id.
Replication Status	This attribute displays the status of the georeplication between sites. • UP- Indicates the georeplication between the sites is up. • DOWN- Indicates the georeplication between the sites is down.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 7-325 (Cont.) Georeplication Details

Fields	Description
Switch Over Status	This attribute displays the switch-over status of the georeplication between sites. • SWITCH_OVER_ENABLED- Indicates the switch-over status of the georeplication between the sites is up. • SWITCH_OVER_DISABLED- Indicates the switch-over status of the georeplication between the sites is disabled.

3. Click **Start Georeplication** to start the replication between the sites.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8
Alerts

This section provides information on Policy alerts and their configuration.

> **Note**
>
> The performance and capacity of the system can vary based on the call model, configuration, including but not limited to the deployed policies and corresponding data, for example, policy tables.

You can configure alerts in Prometheus and `Alertrules.yaml` file.

The following table describes the various severity types of alerts generated by Policy:

Table 8-1 Alerts Levels or Severity Types

Alerts Levels / Severity Types	Definition
Critical	Indicates a severe issue that poses a significant risk to safety, security, or operational integrity. It requires immediate response to address the situation and prevent serious consequences. Raised for conditions can affect the service of Policy.
Major	Indicates a more significant issue that has an impact on operations or poses a moderate risk. It requires prompt attention and action to mitigate potential escalation. Raised for conditions can affect the service of Policy.
Minor	Indicates a situation that is low in severity and does not pose an immediate risk to safety, security, or operations. It requires attention but does not demand urgent action. Raised for conditions can affect the service of Policy.
Info or Warn (Informational)	Provides general information or updates that are not related to immediate risks or actions. These alerts are for awareness and do not typically require any specific response. WARN and INFO alerts may not impact the service of Policy.

For details on how to configure Policy alerts, see *Configuring Alerts* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

For details on how to configure SNMP Notifier, see *Configuring SNMP Notifier* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1 List of Alerts

This section provides detailed information about the alert rules defined for Policy. It consists of the following three types of alerts:

1. Common Alerts - This category of alerts is common and required for all three modes of deployment.
2. PCF Alerts - This category of alerts is specific to PCF microservices and required for Converged and PCF only modes of deployment.
3. PCRF Alerts - This category of alerts is specific to PCRF microservices and required for Converged and PCRF only modes of deployment.

8.1.1 Common Alerts

This section provides information about alerts that are common for PCF and PCRF.

8.1.1.1 POD_CONGESTION_L1

Table 8-2 POD_CONGESTION_L1

Field	Details
Name in Alert Yaml File	PodCongestionL1
Description	Alert when CPU of pod is in CONGESTION_L1 state.
Summary	Pod Congestion status of {{$labels.microservice}} service is Congestion_L1
Severity	Critical
Expression	occnp_pod_congestion_state == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.71
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	**Cause**: The pod has entered a platform/app-defined congestion state (L1). Common reasons: rising queue depth, high CPU, memory pressure, threadpool saturation, or downstream slowness. **Diagnostic Information**: • Identify which pods are in L1 (by pod/namespace labels on the metric) - max by (namespace,pod) (occnp_pod_congestion_state) • Correlate with resource congestion sub-metrics (queue/cpu) - max by (namespace,pod,type) (occnp_pod_resource_congestion_state) • Correlate with Kubernetes/node signals - CPU throttling, restarts, OOMKills, latency, pending requests. **Recovery**: • Relieve pressure: scale out replicas, reduce incoming load (rate limiting/ admission controls), and/or restore slow downstream dependencies. • If CPU throttling: raise requests/limits appropriately and remove noisy-neighbor issues. • If caused by a specific dependency outage, restore it first; congestion should clear as backlog drains.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.2 POD_CONGESTION_L2

Table 8-3 POD_CONGESTION_L2

Field	Details
Description	Alert when CPU of pod is in CONGESTION_L2 state.
Summary	Pod Congestion status of {{$labels.microservice}} service is Congestion_L2
Severity	Critical
Expression	occnp_pod_congestion_state == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.72
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	**Cause**: Severe congestion (L2), typically meaning the pod is protecting itself by shedding/limiting work; likely to cause timeouts/errors. **Diagnostic Information**: • Same as L1, but treat as incident: Look for rapidly growing queue, high CPU, increased timeouts/errors. **Recovery**: • Immediate load shedding / reroute / scale out. • Restore downstream dependencies. • Consider temporarily draining/isolating the worst pods if only some are impacted; validate service stabilizes and state returns < L1.

8.1.1.3 POD_PENDING_REQUEST_CONGESTION_L1

Table 8-4 POD_PENDING_REQUEST_CONGESTION_L1

Field	Details
Description	Pod resource is in Congestion_L1 for Pending Request type
Summary	Pod Resource Congestion status of {{$labels.microservice}} service is Congestion_L1 for resource type queue
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="queue"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.73
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	**Cause**: Pending-request queue/backlog is high enough to trigger L1 congestion; usually due to traffic spike, slow processing, or downstream slowness. **Diagnostic Information**: • Confirm queue congestion pods: - max by (namespace,pod) (occnp_pod_resource_congestion_state{type="queue"}) • Correlate with pending/in-flight metrics (if available): - occnp_diam_pending_requests (or equivalent) **Recovery**: • Scale out or add capacity, reduce traffic, or fix slow downstream calls. • Identify and remove hotspots (single peer, single route, or single tenant) if applicable.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.4 POD_PENDING_REQUEST_CONGESTION_L2

Table 8-5 POD_PENDING_REQUEST_CONGESTION_L2

Field	Details
Description	Alert when queue of pod is in CONGESTION_L2 state.
Summary	Pod Resource Congestion status of {{$labels.microservice}} service is Congestion_L2 for resource type queue
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="queue"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.74
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	**Cause**: Severe queue backlog; likely to manifest as Diameter timeouts and retries. **Diagnostic Information**: • Same as L1 plus check for request retry storms and timeouts. **Recovery**: • Immediately scale out + load shedding + fix downstream slowness; validate queue drains and congestion state returns to normal.

8.1.1.5 POD_CPU_CONGESTION_L1

Table 8-6 POD_CPU_CONGESTION_L1

Field	Details
Description	Alert when cpu of pod is in CONGESTION_L1 state.
Summary	Pod Resource Congestion status of {{$labels.microservice}} service is Congestion_L1 for CPU type
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="cpu"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.73
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	**Cause**: Pod has hit CPU-based congestion threshold: sustained high CPU, throttling, inefficient workload, or hot shard. **Diagnostic Information**: • Confirm affected pods: - max by (namespace,pod) • (occnp_pod_resource_congestion_state{type="cpu"}) • Check CPU throttling/usage (Kubernetes / node exporter metrics) and GC/log indicators. **Recovery**: • Add CPU capacity (HPA/replicas), adjust CPU requests/limits to reduce throttling, re-balance traffic, and investigate hot loops/regressions. • If due to downstream retries/timeouts, fix root cause to stop wasted CPU.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.6 POD_CPU_CONGESTION_L2

Table 8-7 POD_CPU_CONGESTION_L2

Field	Details
Description	Alert when CPU of pod is in CONGESTION_L2 state.
Summary	Pod Resource Congestion status of {{$labels.microservice}} service is Congestion_L2 for CPU type
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="cpu"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.74
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	**Cause**: Severe CPU starvation; high likelihood of cascading failures/timeouts. **Diagnostic Information**: • Same as L1 but urgent; correlate with error/timeout spikes. **Recovery**: • Immediate scale out, reduce load, mitigate CPU throttling, rollback recent changes if regression suspected; validate CPU drops and service recovers.

8.1.1.7 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-8 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the critical threshold limit.
Summary	Alert RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	CRITICAL
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.35
Metric Used	occnp_diam_response_local_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-8 (Cont.) RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause**: The percentage of failed RAA (Re-Auth Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the critical threshold (greater than 90%). The condition indicates a severe failure in handling re-authorization responses over the Rx interface, which can disrupt policy updates, QoS adjustments, and session control between PCRF/PCF and the Application Function (AF). Likely causes include communication failures with AF, policy inconsistencies, or system instability. **Diagnostic Information**: • Evaluate the following metric: – Failed RAA (Rx) Responses / Total RAA (Rx) Responses * 100 over a 5-minute window. • Scope: – msgType = "RAA" (Re-Auth Answer) – appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 90% • Perform the following checks: – Analyze Diameter response codes (e.g., authorization failures, unable to comply, system errors) – Verify connectivity and health of AF (Application Function) peers – Check policy synchronization between PCRF/PCF and AF – Review logs for re-authorization failures, timeouts, or invalid requests – Monitor signaling performance (latency, retransmissions, error spikes) – Inspect system resource utilization (CPU, memory, thread pools) – Correlate with spikes in re-auth requests or policy update events **Recovery**: • Restore connectivity and stability with AF/Rx peer systems • Resolve policy inconsistencies or invalid re-authorization requests • Address specific Diameter error codes causing failures • Restart or scale affected components handling Rx traffic • Tune timeout and retry mechanisms if required • Roll back recent configuration or deployment changes if correlated • Monitor until failure rate drops below the critical threshold • For any additional guidance, contact My Oracle Support.

8.1.1.8 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-9 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the major threshold limit.
Summary	Alert RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	MAJOR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-9 (Cont.) RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.35
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of failed RAA (Re-Auth Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the major threshold (greater than 80% and up to 90%). The condition indicates a high failure rate in re-authorization handling, leading to partial degradation in policy updates, QoS enforcement, and session control between PCRF/PCF and the Application Function (AF). The issue may be due to backend instability, communication issues, or increasing signaling load. **Diagnostic Information**: • Evaluate the following metric: • Failed RAA (Rx) Responses / Total RAA (Rx) Responses * 100 over a 5-minute window • Scope: – msgType = "RAA" – appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% and 90% • Perform the following checks: – Analyze response code distribution (e.g., authorization failures, temporary/system errors) – Verify connectivity and health of AF (Application Function) peers – Check policy synchronization between PCRF/PCF and AF – Review logs for intermittent re-auth failures, timeouts, or malformed requests – Monitor signaling performance (latency, retransmissions, error trends) – Inspect system resource usage (CPU, memory, thread pools) – Correlate with spikes in re-authorization requests or policy update events **Recovery**: • Investigate and stabilize connectivity with AF/Rx peer systems • Resolve policy inconsistencies or invalid re-authorization scenarios • Address specific Diameter error codes contributing to failures • Optimize or scale system resources to handle load • Restart affected components if necessary • Roll back recent configuration or deployment changes if correlated • Closely monitor to prevent escalation to the critical threshold • For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.9 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-10 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the minor threshold limit.
Summary	Alert RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	MINOR
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.35
Metric Used	occnp_diam_response_local_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-10 (Cont.) RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: The percentage of failed RAA (Re-Auth Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the minor threshold (greater than 60% and up to 80%). The condition indicates an early stage of degradation in re-authorization handling, potentially affecting policy updates, QoS enforcement, and session control. While the system is still functional, a noticeable portion of re-auth responses are failing, signaling underlying issues such as intermittent connectivity problems or rising load. **Diagnostic Information**: • Evaluate the following metric: – Failed RAA (Rx) Responses / Total RAA (Rx) Responses * 100 over a 5-minute window • Scope: – msgType = "RAA" – appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% and 80% • Perform the following checks: – Observe trends to determine if failure rate is increasing toward major/critical levels – Analyze response codes for early indicators (e.g., temporary failures, authorization issues) – Verify connectivity and responsiveness of AF (Application Function) peers – Check policy synchronization between PCRF/PCF and AF – Review logs for intermittent re-auth failures, retries, or timeout issues – Monitor system performance (CPU, memory, thread pools, latency) – Identify if failures correlate with traffic spikes or policy update events **Recovery**: • Investigate and address early signs of issues in Rx signaling or AF connectivity • Validate and correct policy configurations or inconsistencies • Optimize or scale system resources to handle increasing load • Resolve issues based on observed Diameter error codes • Apply preventive measures (retry tuning, connection stability improvements) • Review and correct recent configuration or deployment changes if applicable • Continue close monitoring to prevent escalation to higher severity thresholds • For any additional guidance, contact My Oracle Support.

8.1.1.10 ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-11 ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA Rx fail count exceeds the critical threshold limit.
Summary	Alert ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	CRITICAL

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-11 (Cont.) ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.66
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of failed ASA (Abort Session Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the critical threshold (greater than 90%). The condition indicates a severe failure in handling session abort responses, which can prevent proper session termination initiated by the Application Function (AF). As a result, sessions may remain active incorrectly, leading to policy inconsistencies and potential resource leakage. The issue is likely due to communication failures with AF, session state mismatches, or backend instability. **Diagnostic Information**: • Evaluate the following metric: – Failed ASA (Rx) Responses / Total ASA (Rx) Responses * 100 over a 5-minute window • Scope: – msgType = "ASA" (Abort Session Answer) – appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 90% • Perform the following checks: – Analyze Diameter response codes (e.g., unknown session, unable to comply, system errors) – Verify connectivity and health of AF (Application Function) peers – Check session state synchronization between PCRF/PCF and AF – Review logs for abort session failures, timeouts, or invalid requests – Monitor signaling performance (latency, retransmissions, error spikes) – Inspect system resources (CPU, memory, session table utilization) – Correlate with spikes in abort session requests or abnormal session behavior **Recovery**: • Restore connectivity and stability with AF/Rx peer systems • Resolve session state inconsistencies or stale session entries • Address specific Diameter error codes causing failures • Restart or scale affected components handling Rx interface traffic • Clean up orphaned or stuck sessions if required • Roll back recent configuration or deployment changes if correlated • Monitor until failure rate drops below the critical threshold • For any additional guidance, contact My Oracle Support.

8.1.1.11 ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-12 ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA Rx fail count exceeds the major threshold limit.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-12 (Cont.) ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Summary	Alert ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	MAJOR
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.66
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of failed ASA (Abort Session Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the major threshold (greater than 80% and up to 90%). The condition indicates a high failure rate in handling abort session responses, leading to partial degradation in session termination initiated by the Application Function (AF). This may result in incomplete session cleanup, inconsistent policy states, and increased resource utilization. The issue is likely due to AF connectivity issues, backend instability, or increased signaling load. **Diagnostic Information**: • Evaluate the following metric: – Failed ASA (Rx) Responses / Total ASA (Rx) Responses * 100 over a 5-minute window • Scope: – msgType = "ASA" – appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% and 90% • Perform the following checks: – Analyze response code distribution. For example, unknown session, temporary failures, system errors – Verify connectivity and health of AF (Application Function) peers – Check session state synchronization between PCRF/PCF and AF – Review logs for intermittent abort session failures, timeouts, or malformed requests – Monitor signaling performance (latency, retransmissions, error trends) – Inspect system resource usage (CPU, memory, session table utilization) – Correlate with spikes in abort session requests or abnormal session behavior **Recovery**: • Investigate and stabilize connectivity with AF/Rx peer systems • Resolve session state inconsistencies or stale session entries • Address specific Diameter error codes contributing to failures • Optimize or scale system resources to handle load • Restart affected components if necessary • Roll back recent configuration or deployment changes if correlated • Closely monitor to prevent escalation to the critical threshold • For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.12 ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-13 ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA Rx fail count exceeds the minor threshold limit.
Summary	Alert ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	MINOR
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.66
Metric Used	occnp_diam_response_local_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-13 (Cont.) ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: The percentage of failed ASA (Abort Session Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the minor threshold (greater than 60% and up to 80%). The condition indicates an early stage of degradation in handling abort session responses. While the system remains operational, a significant portion of session abort operations are failing, which may lead to delayed or incomplete session termination, inconsistent policy states, and potential buildup of stale sessions. **Diagnostic Information**: • Evaluate the following metric: – Failed ASA (Rx) Responses / Total ASA (Rx) Responses * 100 over a 5-minute window • Scope: – msgType = "ASA" – appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% and 80% • Perform the following checks: – Observe trends to determine if failure rate is increasing toward major/critical levels – Analyze response codes for early indicators (e.g., unknown session, temporary/system errors) – Verify connectivity and responsiveness of AF (Application Function) peers – Check session state synchronization between PCRF/PCF and AF – Review logs for intermittent abort session failures, retries, or timeout issues – Monitor system performance (CPU, memory, session table utilization) – Identify if failures correlate with traffic spikes or abnormal session behavior **Recovery**: • Investigate and address early signs of issues in Rx signaling or AF connectivity • Validate session state consistency across systems • Resolve identified issues based on Diameter error codes • Optimize or scale system resources to handle load • Apply preventive measures (retry tuning, improved session cleanup mechanisms) • Review and correct recent configuration or deployment changes if applicable • Continue close monitoring to prevent escalation to higher severity thresholds • For any additional guidance, contact My Oracle Support.

8.1.1.13 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-14 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA Rx timeout count exceeds the minor threshold limit
Summary	Alert ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	MINOR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-14 (Cont.) ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.67
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of ASA (Abort Session Answer) Diameter requests timing out for application ID 16777236 (Rx interface) has exceeded the minor threshold (greater than 60% and up to 80%). The condition indicates an early stage of degradation where a noticeable portion of abort session requests are not receiving timely responses. While the system may still be operational, this condition suggests emerging issues such as increasing latency, intermittent AF (Application Function) unresponsiveness, or rising system load. **Diagnostic Information**: • Evaluate the following metric: • Timed-out ASA (Rx) Responses / Total ASA (Rx) Requests * 100 over a 5-minute window • Scope: – msgType = "ASA" – appId = "16777236" (Rx interface) – responseCode = "timeout" • Trigger condition: Timeout rate > 60% and 80% • Perform the following checks: – Observe trends to determine if timeout rate is increasing toward major/critical levels – Verify connectivity and latency to AF (Application Function) peers – Check for intermittent delays or partial unresponsiveness from AF – Review logs for timeout events, retries, and delayed responses – Monitor Diameter stack metrics (pending requests, queue buildup, retransmissions) – Inspect system performance (CPU, memory, thread pools, connection limits) – Identify network issues such as packet loss, congestion, or firewall delays **Recovery**: • Investigate and address early signs of latency or connectivity issues with AF/Rx peers • Optimize network performance and resolve packet loss or congestion • Tune timeout and retry parameters if needed • Scale system resources to handle increasing load • Apply preventive measures (connection pooling, traffic smoothing) • Review and correct recent configuration or deployment changes if applicable • Continue close monitoring to prevent escalation to higher severity thresholds • For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.14 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-15 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA Rx timeout count exceeds the major threshold limit
Summary	Alert ASA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	MAJOR
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.67
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of ASA (Abort Session Answer) Diameter requests timing out for application ID 16777236 (Rx interface) has exceeded the major threshold (greater than 80% and up to 90%). The condition indicates a high rate of delayed or missing responses for abort session requests, leading to partial degradation in session termination handling. It may result in incomplete session cleanup and increased resource utilization. The issue is likely due to network latency, partial unresponsiveness of the Application Function (AF), or system overload. **Diagnostic Information**: • Evaluate the following metric: – Timed-out ASA (Rx) Responses / Total ASA (Rx) Requests * 100 over a 5-minute window • Scope: – msgType = "ASA" – appId = "16777236" (Rx interface) – responseCode = "timeout" • Trigger condition: Timeout rate > 80% and 90% • Perform the following checks: – Analyze timeout trends to see if they are increasing toward critical levels – Verify connectivity and latency to AF (Application Function) peers – Check if AF is intermittently slow or partially unresponsive – Review logs for timeout events, retransmissions, and delayed responses – Monitor Diameter stack health (pending requests, queue buildup, retransmission count) – Inspect system resources (CPU, memory, thread pools, connection limits) – Check for network congestion, firewall filtering, or load balancer delays **Recovery**: • Investigate and stabilize connectivity with AF/Rx peer systems • Reduce network latency and resolve packet loss issues • Tune timeout and retry configurations if needed • Optimize or scale system resources to handle load • Restart affected components if necessary • Address infrastructure bottlenecks (firewalls, load balancers, routing issues) • Closely monitor to prevent escalation to the critical threshold • For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.15 ASA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-16 ASA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA Rx timeout count exceeds the critical threshold limit
Summary	Alert ASA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	CRITICAL
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA", appId="16777236"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.67
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of ASA (Abort Session Answer) Diameter requests timing out for application ID 16777236 (Rx interface) has exceeded the critical threshold (greater than 90%). The condition indicates a severe degradation where most abort session responses are not received within the expected time, likely due to communication failures with the Application Function (AF), network latency, or overloaded/unresponsive backend systems. **Diagnostic Information**: • Evaluate the following metric: – Timed-out ASA (Rx) Responses / Total ASA (Rx) Requests * 100 over a 5-minute window • Scope: – msgType = "ASA" – appId = "16777236" (Rx interface) – responseCode = "timeout" • Trigger condition: Timeout rate > 90% • Perform the following checks: – Verify connectivity to AF (Application Function) peers (network reachability, packet loss, latency) – Check if AF is responding slowly or not responding at all – Review logs for timeout errors, retransmissions, or request drops – Monitor Diameter stack metrics (queue size, pending requests, retransmission count) – Inspect system resource utilization (CPU, memory, thread pools, connection limits) – Check for network congestion, firewall issues, or load balancer delays – Correlate with spikes in abort session requests or traffic bursts **Recovery**: • Restore connectivity and responsiveness of AF/Rx peer systems • Investigate and resolve network latency or packet loss issues • Tune timeout and retransmission parameters if required • Scale or restart affected components handling Rx traffic • Reduce load or apply traffic throttling if system is overloaded • Fix infrastructure issues (firewalls, load balancers, routing) • Monitor until timeout rate drops below the critical threshold • For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.16 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT

Table 8-17 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT

Field	Description
Description	More than 70% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Summary	More than 70% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Severity	CRITICAL
Expression	sum by (namespace) (rate(occnp_sm_qosmon_decs_error_total[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.133
Metric Used	occnp_sm_qosmon_decs_error_total, occnp_pa_qosmon_request_total
Recommended Actions	The number of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF with QOS_MON_DECS_ERR represents 70% or more of the total app sessions. The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.17 SCP_PEER_UNAVAILABLE

Table 8-18 SCP_PEER_UNAVAILABLE

Field	Details
Description	Configured SCP peer is unavailable.
Summary	SCP peer [{{$labels.peer}}] is unavailable.
Severity	Major
Expression	occnp_oc_egressgateway_peer_health_status != 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.60
Metric Used	occnp_oc_egressgateway_peer_health_status

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-18 (Cont.) SCP_PEER_UNAVAILABLE

Field	Details
Recommended Actions	**Cause**: One or more SCP peer nodes are unavailable or unhealthy, as indicated by the peer health status not equal to 0. This suggests a failure in connectivity or health monitoring between the system and its configured peers, potentially impacting service routing, request forwarding, and overall signaling reliability. **Diagnostic Information**: • Evaluate the following metric: – occnp_oc_egressgateway_peer_health_status != 0 • Trigger condition: Peer health status is not equal to 0 (non-healthy state) • Interpretation: – 0 → Healthy – Non-zero → Peer unavailable/unhealthy • Perform the following checks: – Identify which peer(s) are marked unhealthy – Verify network connectivity to the affected peer(s) (ping, TCP checks) – Check health check endpoints or heartbeat mechanisms – Review logs for connection failures, timeouts, or DNS resolution issues – Validate peer configuration (IP, port, certificates, routing rules) – Inspect load balancer or gateway behavior if applicable – Check for TLS/SSL handshake failures or certificate issues – Monitor if multiple peers are affected (indicating broader network/system issue) **Recovery**: • Restore network connectivity to the affected peer(s) • Restart or recover the unavailable peer services • Fix configuration issues (endpoints, ports, certificates, routing rules) • Resolve DNS or service discovery issues if present • Ensure health check mechanisms are functioning correctly • Failover traffic to healthy peers if supported • Scale or redistribute load if peers are overloaded • Monitor until peer health status returns to 0 (healthy state)

8.1.1.18 SCP_PEER_SET_UNAVAILABLE

Table 8-19 SCP_PEER_SET_UNAVAILABLE

Field	Details
Description	None of the SCP peer available for configured peerset.
Summary	{{ $value }} SCP peers under peer set {{$labels.peerset}} are currently unavailable.
Severity	Critical
Expression	(occnp_oc_egressgateway_peer_count > 0 and (occnp_oc_egressgateway_peer_available_count) == 0)
OID	1.3.6.1.4.1.323.5.3.52.1.2.61
Metric Used	occnp_oc_egressgateway_peer_count and occnp_oc_egressgateway_peer_available_count

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-19 (Cont.) SCP_PEER_SET_UNAVAILABLE

Field	Details
Recommended Actions	**Cause**: One or more SCP peers within a configured peer set are unavailable. This condition occurs when the number of available peers is less than the total configured peers, indicating partial peer set degradation. While not all peers are down, this reduces redundancy and may impact load balancing, failover capability, and overall service reliability. **Diagnostic Information**: • Evaluate the following metric: – (Total Peers - Available Peers) != 0 AND Total Peers > 0 • Trigger condition: – At least one peer in the configured peer set is unavailable • Interpretation: – occnp_oc_egressgateway_peer_count → Total configured peers – occnp_oc_egressgateway_peer_available_count → Currently healthy/ available peers – Difference ≠ 0 → Some peers are unavailable • Perform the following checks: – Identify which peers in the peer set are unavailable – Verify network connectivity to affected peers (latency, packet loss, TCP checks) – Check health check/heartbeat status for each peer – Review logs for failures such as timeouts, connection errors, or TLS issues – Validate peer configuration (IP, port, certificates, routing policies) – Check if unavailable peers are due to maintenance, scaling events, or crashes – Monitor load on remaining peers to ensure they are not overloaded **Recovery**: • Restore connectivity or restart the unavailable peer(s) • Fix configuration issues related to endpoints, certificates, or routing • Resolve network issues (latency, packet loss, DNS resolution) • Re-enable peers if they were intentionally disabled or under maintenance • Ensure proper scaling and load distribution across available peers • Validate health check mechanisms and thresholds • Monitor until all peers in the set are available and stable • For any additional guidance, contact My Oracle Support.

8.1.1.19 POLICY_SERVICES_DOWN

Table 8-20 POLICY_SERVICES_DOWN

Field	Details
Description	{{$labels.service}} service is not running.
Summary	{{$labels.service}} service is not running.
Severity	Critical
Expression	sum by(service, namespace, category) (appinfo_service_running{application="occnp",service!~".*altsvc-cache",vendor="Oracle"}) < 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.1
Metric Used	appinfo_service_running{vendor="Oracle", application="occnp", category!=""}!= 1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-20 (Cont.) POLICY_SERVICES_DOWN

Field	Details
Recommended Actions	**Cause**: Indicates that a Policy service becomes unavailable or stops responding. Possible causes include pod failures, service restarts, node issues, network interruptions, deployment problems, or upstream dependency failures. It may also occur when the service is unhealthy due to resource pressure, configuration issues, or backend connectivity problems. **Diagnostic Information**: • Check related Policy service pod status, restarts, and readiness/liveness probe failures. • `Verify the running status of the service using kubectl get service -n <namespace>.` • Review service logs from Kibana to identify crashes, startup failures, or connection issues. • Check Grafana for CPU, memory, and network trends to see whether the service was under stress before going down. • Correlate the alert with recent deployments, config changes, or node-level incidents. • Verify whether related dependent services are healthy and reachable. **Recovery**: • Restart the affected service pods or perform a rolling restart if the failure is pod-specific. • Roll back recent changes if the issue started after a deployment or configuration update. • Fix the underlying cause such as resource exhaustion, probe failure, or dependency outage. • If the service does not recover cleanly, escalate to Oracle Support for further investigation.

8.1.1.20 DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 8-21 DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Description	Diameter Connector Ingress traffic Rate is above threshold of Max MPS (current value is: {{ $value }})
Summary	Traffic Rate is above 90 Percent of Max requests per second.
Severity	Major
Expression	sum(rate(ocpm_ingress_request_total{servicename_3gpp=~"rx|sy"}[2m])) >= 900
OID	1.3.6.1.4.1.323.5.3.52.1.2.6
Metric Used	ocpm_ingress_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-21 (Cont.) DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Recommended Actions	**Cause**: Indicates that the ingress traffic rate exceeds the configured threshold for the service. This condition indicates a surge in incoming requests due to increased client activity, retries, misbehaving clients, or upstream/downstream issues. Other causes include error loops (4xx/5xx), sudden traffic spikes, or configuration changes affecting routing or throttling. **Diagnostic Information**: • Check ingress traffic graphs to confirm whether the increase is sustained or a short-lived spike. Refer to the Ingress Gateway section in Grafana to identify any rise in 4xx and 5xx response codes. • Analyze Ingress Gateway logs in Kibana to determine the source and reason for errors or abnormal traffic patterns. • Verify recent deployments or configuration changes, and correlate with traffic sources or client behavior. • `Review threshold configuration in Common_Alertrules.yaml to ensure it aligns with expected traffic patterns.` **Recovery**: • If the traffic spike is legitimate, scale the service or ingress capacity to handle the load. • If errors (4xx/5xx) cause the condition, fix the underlying issue (e.g., routing, backend failures, misconfigurations). • Mitigate abnormal traffic by rate limiting, blocking faulty clients, or adjusting retry mechanisms. • The alert clears automatically once ingress traffic rate falls below the configured threshold.

8.1.1.21 DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 8-22 DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Name in Alert Yaml File	DiamIngressErrorRateAbove10Percent
Description	Transaction Error Rate detected above 10 Percent of Total on Diameter Connector (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 10 Percent of Total Transactions.
Severity	Critical
Expression	sum(rate(ocpm_ingress_response_total{servicename_3gpp=~"rx|sy",response_code!~"2.*"}[24h]))/sum(rate(ocpm_ingress_response_total{servicename_3gpp=~"rx|sy"}[24h])) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.7
Metric Used	ocpm_ingress_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-22 (Cont.) DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Recommended Actions	**Cause**: Indicates that failed transactions exceed 10% of total ingress transactions. The condition indicates a high error rate typically caused by backend service failures, misconfigurations, invalid requests, or dependency issues. It may also result from recent deployments, API contract mismatches, or traffic anomalies affecting specific services or methods. **Diagnostic Information**: • Check overall ingress error rate trends to confirm whether the increase is sustained or transient. • `Analyze service-specific metrics (e.g., ocpm_ingress_response_total{servicename_3gpp="rx",response_code!~"2.*"}) to identify which service is contributing to failures.` • Further filter errors by HTTP methods (GET, PUT, POST, DELETE, PATCH) to pinpoint problematic operations. • Correlate with recent deployments, configuration changes, and dependency health. • Review logs in Kibana for detailed error messages and failure patterns. **Recovery**: • Fix underlying service or dependency issues causing failed transactions (e.g., configuration errors, backend failures). • Roll back recent changes if the issue started after a deployment. • Address API/method-specific issues and validate request/response handling. • The alert clears automatically once failed transactions drop below 10% of total transactions.

8.1.1.22 DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Table 8-23 DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Description	Egress Transaction Error Rate detected above 1 Percent of Total on Diameter Connector (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 1 Percent of Total Transactions
Severity	Minor
Expression	sum(rate(ocpm_egress_response_total{servicename_3gpp=~"rx|sy",response_code!~"2.*"}[24h]))/sum(rate(ocpm_egress_response_total{servicename_3gpp=~"rx|sy"}[24h])) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.8
Metric Used	ocpm_egress_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-23 (Cont.) DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause**: Indicates that failed egress transactions exceed 1% of total outgoing transactions. This condition indicates issues in downstream communication, such as peer unavailability, response errors, timeout scenarios, or request/response handling problems. Other causes include misconfigurations, increased load, retry storms, or intermittent connectivity issues with the downstream service. **Diagnostic Information**: • Check egress error rate trends to determine whether the increase is sustained or transient. • `Analyze service-specific metrics (e.g., ocpm_egress_response_total{servicename_3gpp="rx",response_code !~"2.*"}) to identify which service is contributing to the failures.` • Further filter errors by HTTP methods (GET, PUT, POST, DELETE, PATCH) to isolate problematic operations. • Correlate failures with recent deployments, configuration changes, or downstream service behavior. • Review logs in Kibana to determine the exact reason for failures such as timeouts, connection issues, or invalid responses. **Recovery**: • Fix the downstream service or connectivity issue causing the failed egress transactions. • Roll back recent changes if the issue started after a deployment or configuration update. • Adjust timeout, retry, or routing behavior if the failures are caused by transient downstream instability. • If the issue persists, escalate to Oracle Support for further investigation.

8.1.1.23 UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 8-24 UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Description	User service Ingress traffic Rate from UDR is above threshold of Max MPS (current value is: {{ $value }})
Summary	Traffic Rate is above 90 Percent of Max requests per second
Severity	Major
Expression	sum(rate(occnp_userservice_inbound_count_total{service_resource="udr-service"}[2m])) >= 900
OID	1.3.6.1.4.1.323.5.3.52.1.2.9
Metric Used	ocpm_userservice_inbound_count_total{service_resource="udr-service"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-24 (Cont.) UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Recommended Actions	**Cause**: Indicates that the ingress traffic rate to the UDR service exceeds the configured threshold. This condition indicates a surge in incoming requests due to increased client activity, retry storms, or abnormal traffic patterns. Other causes include upstream service issues, misconfigurations, or spikes driven by specific workloads or events. **Diagnostic Information**: • Check ingress traffic graphs for the UDR service to determine whether the increase is sustained or a transient spike. • Refer to the Ingress Gateway section in Grafana to identify any corresponding rise in 4xx and 5xx response codes. • Analyze Ingress Gateway logs in Kibana to understand the source of traffic and reasons for errors. • Correlate traffic patterns with recent deployments, configuration changes, or upstream service behavior. • Review threshold configuration in `Common_Alertrules.yaml` to ensure it aligns with expected traffic levels. **Recovery**: • If traffic increase is expected, scale the UDR service or ingress capacity to handle the load. • If errors (4xx/5xx) cause the condition, resolve underlying issues such as routing problems, backend failures, or misconfigurations. • Mitigate abnormal traffic using rate limiting or by controlling retry behavior from clients. • The alert clears automatically once ingress traffic rate falls below the configured threshold.

8.1.1.24 UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 8-25 UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Description	Egress Transaction Error Rate detected above 10 Percent of Total on User service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 10 Percent of Total Transactions
Severity	Critical
Expression	sum(rate(ocpm_udr_tracking_response_total{servicename_3gpp="nudr-dr",response_code!~"2.*"}[24h])) / sum(rate(ocpm_udr_tracking_response_total{servicename_3gpp="nudr-dr"}[24h])) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.10
Metric Used	ocpm_udr_tracking_response_total{servicename_3gpp="nudr-dr",response_code!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-25 (Cont.) UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Recommended Actions	**Cause**: Indicates that failed egress transactions to UDR exceed the configured threshold. The condition indicates a high error rate in outbound communication, typically caused by UDR unavailability, latency issues, misconfigurations, or request/response handling failures. It may also result from connectivity issues, retry storms, or increased load impacting communication with UDR. **Diagnostic Information**: • Check egress error rate trends to determine whether the increase is sustained or transient. • Refer to the Egress Gateway section in Grafana to identify any increase in 4xx and 5xx error response codes. • Analyze Egress Gateway logs in Kibana to determine the reason for failures such as timeouts, connection issues, or invalid responses. • Correlate failures with recent deployments, configuration changes, or UDR service behavior. • Review threshold configuration in `Common_Alertrules.yaml` to ensure it aligns with expected traffic patterns. • The alert clears automatically once failed transactions fall below the configured threshold. **Recovery**: • Fix underlying issues with UDR such as availability, latency, or configuration problems. • Resolve connectivity or network issues between services and UDR. • Adjust retry, timeout, or routing configurations if failures are due to transient issues. • Roll back recent changes if the issue started after a deployment. • If the issue persists, escalate to Oracle Support for further investigation.

8.1.1.25 POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 8-26 POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Description	Ingress Traffic Rate is above threshold of Max MPS (current value is: {{ $value }})
Summary	Traffic Rate is above 90 Percent of Max requests per second
Severity	Critical
Expression	sum(rate(client_request_total[2m])) >= 900
OID	1.3.6.1.4.1.323.5.3.52.1.2.13
Metric Used	client_request_total **Note**: This is a Kubernetes metric used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-26 (Cont.) POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Recommended Actions	**Cause**: Indicates that the ingress traffic rate to the PolicyDS service exceeds the configured threshold. This condition indicates a surge in incoming requests due to increased client activity, retry storms, or abnormal traffic patterns. Other causes include upstream service issues, misconfigurations, or workload-driven spikes impacting PolicyDS. **Diagnostic Information**: • Check ingress traffic graphs for the PolicyDS service to determine whether the increase is sustained or a transient spike. • Refer to the Ingress Gateway section in Grafana to identify any rise in 4xx and 5xx response codes. • Analyze Ingress Gateway logs in Kibana to determine the source of traffic and the reason for errors or abnormal request patterns. • Correlate with recent deployments, configuration changes, or upstream service behavior impacting PolicyDS. • Review threshold configuration in Common_Alertrules.yaml to ensure it aligns with expected traffic levels. **Recovery**: • If the traffic increase is expected, scale the PolicyDS service or ingress capacity accordingly. • If errors (4xx/5xx) cause the condition, resolve underlying issues such as routing problems, backend failures, or misconfigurations. • Mitigate abnormal traffic by applying rate limiting or controlling retry behavior from clients. • The alert clears automatically once ingress traffic rate falls below the configured threshold.

8.1.1.26 POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 8-27 POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Description	Ingress Transaction Error Rate detected above 10 Percent of Total on PolicyDS service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 10 Percent of Total Transactions
Severity	Critical
Expression	sum(rate(client_response_total{response!~"2.*"}[24h])) / sum(rate(client_response_total[24h])) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.14
Metric Used	client_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-27 (Cont.) POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Recommended Actions	**Cause**: Indicates that failed transactions for PolicyDS exceed 10% of total ingress transactions. The condition indicates a high error rate typically caused by backend service failures, misconfigurations, invalid requests, or dependency issues. It may also result from recent deployments, API contract mismatches, or traffic anomalies affecting specific operations in PolicyDS. Database-related issues such as increased latency, high concurrency, optimistic lock exceptions, or transaction retries can also contribute to higher error rates. **Diagnostic Information**: • Check overall ingress error rate trends for PolicyDS to determine whether the increase is sustained or transient. • Check database exception metrics such as db_exception_total to identify DB-related failures. • Check client-side metrics to identify the workflow which is contributing to the failures (e.g., client_response_total{method="DELETE",workflow="SUBSCRIBER-DELETE",response="404 NOT_FOUND"}). • Further filter errors by HTTP methods (GET, PUT, POST, DELETE, PATCH) to isolate problematic operations. • Refer to Grafana dashboards for 4xx and 5xx trends and correlate with recent deployments or configuration changes. • Review PolicyDS and related service logs like UDR connector, CHF connector, and SM Service logs to identify the actual cause of the failure. **Recovery**: • Fix underlying service or dependency issues causing failed transactions (e.g., misconfigurations, backend failures). • Investigate and resolve database-related issues such as latency, contention, or optimistic locking conflicts. • If concurrency-related issues are observed, evaluate the need to enable Bulwark service for the specific call flow. • Rollback recent deployments or changes if the issue started after a release. • The alert clears automatically once failed transactions drop below 10% of total transactions.

8.1.1.27 POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Table 8-28 POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Description	Egress Transaction Error Rate detected above 1 Percent of Total on PolicyDS service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 1 Percent of Total Transactions
Severity	Minor
Expression	sum(rate(server_response_total{response!~"2.*"}[24h])) / sum(rate(server_response_total[24h])) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.15
Metric Used	server_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-28 (Cont.) POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause**: Indicates that failed transactions for PolicyDS exceed 1% of total egress transactions. The condition indicates a high error rate typically caused by backend service failures, misconfigurations, invalid requests, or dependency issues. It may also result from recent deployments, API contract mismatches, or traffic anomalies affecting specific operations in PolicyDS. **Diagnostic Information**: • Check overall egress error rate trends for PolicyDS to determine whether the increase is sustained or transient. • Check client-side metrics to identify the workflow which is contributing to the failures (e.g., client_response_total{method="DELETE",workflow="SUBSCRIBER-DELETE",response="404 NOT_FOUND"}). • Further filter errors by HTTP methods (GET, PUT, POST, DELETE, PATCH) to isolate problematic operations. • Refer to Grafana dashboards for 4xx and 5xx trends and correlate with recent deployments or configuration changes. • Review PolicyDS and related service logs like UDR connector, CHF connector, SM Service logs to identify the actual cause of the failure. **Recovery**: • Fix underlying service or dependency issues causing failed transactions (e.g., misconfigurations, backend failures). • Rollback recent deployments or changes if the issue started after a release. • The alert clears automatically once failed transactions drop below 10% of total transactions.

8.1.1.28 UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Table 8-29 UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	Ingress Timeout Error Rate detected above 10 Percent of Total towards UDR service (current value is: {{ $value }})
Summary	Timeout Error Rate detected above 10 Percent of Total Transactions
Severity	Major
Expression	sum(rate(ocpm_udr_tracking_request_timeout_total{servicename_3gpp="nudr-dr"}[24h])) / sum(rate(ocpm_udr_tracking_request_total{servicename_3gpp="nudr-dr"}[24h])) * 100 >=10
OID	1.3.6.1.4.1.323.5.3.52.1.2.16
Metric Used	ocpm_udr_tracking_request_timeout_total{servicename_3gpp="nudr-dr"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-29 (Cont.) UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: Indicates that the number of ingress requests to UDR resulting in timeout errors exceeds the configured major threshold. This condition indicates delayed or no response from UDR due to high latency, resource saturation, or backend processing delays. Other causes include network issues, misconfigurations, increased load, or downstream dependency slowness impacting UDR response times. **Diagnostic Information**: • Check timeout error trends to determine whether the increase is sustained or intermittent. • Refer to ingress-related metrics and Grafana dashboards to identify spikes in latency and timeout responses. • Analyze UDR service logs from Kibana to identify slow queries, processing delays, or request handling issues. • Check for resource utilization (CPU, memory) on UDR pods to identify saturation. • Correlate with recent deployments, configuration changes, or increased traffic patterns. • Verify connectivity and response times between dependent services and UDR. **Recovery**: • Investigate and resolve latency issues in UDR such as slow processing, backend delays, or resource constraints. • Scale UDR service if the timeouts are due to increased load. • Optimize queries or request handling to reduce processing time. • Adjust timeout and retry configurations if required. • Roll back recent changes if the issue started after a deployment. • If the issue persists, escalate to Oracle Support for further investigation. • The alert clears automatically once timeout errors fall below the configured major threshold.

8.1.1.29 DB_TIER_DOWN_ALERT

Table 8-30 DB_TIER_DOWN_ALERT

Field	Details
Description	DB cannot be reachable.
Summary	DB cannot be reachable.
Severity	Critical
Expression	appinfo_category_running{category="database"} != 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.18
Metric Used	appinfo_category_running{category="database"}
Recommended Actions	**Cause**: Database tier is unavailable or unreachable (appinfo_category_running{category="database"} != 1). **Diagnostic Information**: • Verify database pod status, readiness, events, network connectivity, database logs, storage/PVC health, and the appinfo_category_running metric. **Recovery**: • Restore the failed database component/connectivity; resolve storage or configuration issues; confirm the database category reports running again.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.30 CPU_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Table 8-31 CPU_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	CPU usage for {{$labels.namespace}}-{{$labels.service}} service is above 60%
Summary	CPU usage for {{$labels.namespace}}-{{$labels.service}} service is above 60%
Severity	Minor
Expression	avg by (namespace, service) (avg_over_time(cgroup_cpu_usage[2m])) >= 60 < 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.19
Metric Used	cgroup_cpu_usage **Note**: This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.
Recommended Actions	**Cause**: Indicates that CPU utilization for a service exceeds the configured minor threshold over a defined time window. This condition indicates increased processing load due to higher traffic, inefficient code paths, or resource-intensive operations. Other causes include traffic spikes, background jobs, tight loops, thread contention, or misconfigured CPU limits/requests. **Diagnostic Information**: • Check CPU usage graphs for the service to determine whether utilization is consistently high or showing intermittent spikes. • Correlate CPU usage with traffic patterns, batch jobs, or recent deployments. • Check pod-level metrics for CPU throttling, restarts, or abnormal usage patterns. • Check latency metrics to identify slow responses or performance degradation contributing to higher CPU usage. • If there is a sudden surge in traffic leading to higher CPU usage, check logs of upstream services interacting with this service to identify increased egress traffic or retry behavior. • Review service logs in Kibana to identify high-latency operations or repeated processing loops. • Verify CPU limits and requests configuration and check for node-level CPU contention. **Recovery**: • If CPU usage is consistently high, optimize application logic, reduce unnecessary processing, or tune configurations. • If caused by traffic spikes, scale out the service to distribute load. • Adjust CPU limits/requests cautiously if required, ensuring no impact on cluster stability. • Roll back recent changes if the issue started after a deployment. • The alert clears automatically once CPU usage falls below the configured threshold.

8.1.1.31 CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Table 8-32 CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	CPU usage for {{$labels.namespace}}-{{$labels.service}} service is above 80%
Summary	CPU usage for {{$labels.namespace}}-{{$labels.service}} service is above 80%
Severity	Major
Expression	avg by (namespace, service) (avg_over_time(cgroup_cpu_usage[2m])) >= 80 < 90

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-32 (Cont.) CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.20
Metric Used	cgroup_cpu_usage **Note**: This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.
Recommended Actions	**Cause**: Indicates that CPU utilization for a service exceeds the configured minor threshold over a defined time window. This condition indicates increased processing load due to higher traffic, inefficient code paths, or resource-intensive operations. Other causes include traffic spikes, background jobs, tight loops, thread contention, or misconfigured CPU limits/requests. **Diagnostic Information**: • Check CPU usage graphs for the service to determine whether utilization is consistently high or showing intermittent spikes. • Correlate CPU usage with traffic patterns, batch jobs, or recent deployments. • Check pod-level metrics for CPU throttling, restarts, or abnormal usage patterns. • Check latency metrics to identify slow responses or performance degradation contributing to higher CPU usage. • If there is a sudden surge in traffic leading to higher CPU usage, check logs of upstream services interacting with this service to identify increased egress traffic or retry behavior. • Review service logs in Kibana to identify high-latency operations or repeated processing loops. • Verify CPU limits and requests configuration and check for node-level CPU contention. **Recovery**: • If CPU usage is consistently high, optimize application logic, reduce unnecessary processing, or tune configurations. • If caused by traffic spikes, scale out the service to distribute load. • Adjust CPU limits/requests cautiously if required, ensuring no impact on cluster stability. • Roll back recent changes if the issue started after a deployment. • The alert clears automatically once CPU usage falls below the configured threshold.

8.1.1.32 CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Table 8-33 CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD
Description	CPU usage for {{$labels.namespace}}-{{$labels.service}} service is above 90%
Summary	CPU usage for {{$labels.namespace}}-{{$labels.service}} service is above 90%
Severity	Critical
Expression	avg by (namespace, service) (avg_over_time(cgroup_cpu_usage[2m])) >= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.21
Metric Used	cgroup_cpu_usage **Note**: This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-33 (Cont.) CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause**: Indicates that CPU utilization for a service exceeds the configured critical threshold over a defined time window. The condition indicates severe resource saturation and risk of service degradation or unresponsiveness. It is typically caused by sustained high traffic, inefficient processing, tight loops, thread contention, or misconfigured CPU limits/requests. It may also result from retry storms, sudden workload spikes, or downstream latency causing increased processing overhead. **Diagnostic Information**: • Check CPU usage graphs for the service to confirm sustained high utilization at critical levels. • Correlate CPU usage with traffic patterns, batch jobs, or recent deployments. • Check pod-level metrics for CPU throttling, restarts, and saturation indicators. • Check latency metrics to identify performance degradation contributing to high CPU usage. • If there is a sudden surge in traffic, check logs of upstream services interacting with this service to identify increased egress traffic or retry behavior. • Review service logs in Kibana to identify high CPU-consuming operations, loops, or bottlenecks. • Verify CPU limits and requests configuration and check for node-level CPU contention. **Recovery**: • Immediately scale out the service to reduce CPU load per pod. • If required, perform a rolling restart to stabilize pods under extreme load. • Optimize application logic or disable non-critical processing to reduce CPU consumption. • Mitigate retry storms or abnormal traffic by controlling client retry behavior. • Adjust CPU limits/requests cautiously if needed to stabilize the service. • Rollback recent deployments if the issue started after a change. • The alert clears automatically once CPU usage falls below the configured critical threshold.

8.1.1.33 MEMORY_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Table 8-34 MEMORY_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	Memory usage for {{$labels.service}} service is above 60%
Summary	Memory usage for {{$labels.service}} service is above 60%
Severity	Minor
Expression	avg by (namespace, service) (avg_over_time(cgroup_memory_usage[2m])) >= 60 < 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.22
Metric Used	container_memory_usage_bytes **Note**: This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-34 (Cont.) MEMORY_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: Indicates that the service's memory usage stays at or above the minor threshold for the configured window that is 60% This usually indicates sustained memory growth, repeated spikes from traffic or payload size, cache expansion, or a memory leak in the PRE service. It can also be triggered by recent deployment changes, higher concurrency, or a misconfigured memory limit. **Diagnostic Information**: • Check memory graphs for the PRE service to confirm whether usage is constantly high or only spiking. • Review whether the alert aligns with traffic bursts, deployment changes, or a specific job or request pattern. **Recovery**: • Scale out or increase memory limits only after confirming the trend and ruling out a leak or abnormal workload

8.1.1.34 MEMORY_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Table 8-35 MEMORY_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	Memory usage for {{$labels.service}} service is above 80%
Summary	Memory usage for {{$labels.service}} service is above 80%
Severity	Major
Expression	avg by (namespace, service) (avg_over_time(cgroup_memory_usage[2m])) >= 80 < 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.23
Metric Used	container_memory_usage_bytes **Note**: This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.
Recommended Actions	**Cause**: Indicates that the service's memory usage stays at or above the minor threshold for the configured window that is 80% This usually indicates sustained memory growth, repeated spikes from traffic or payload size, cache expansion, or a memory leak in the PRE service. It can also be triggered by recent deployment changes, higher concurrency, or a misconfigured memory limit. **Diagnostic Information**: • Check memory graphs for the PRE service to confirm whether usage is constantly high or only spiking. • Review whether the alert aligns with traffic bursts, deployment changes, or a specific job or request pattern. **Recovery**: • Scale out or increase memory limits only after confirming the trend and ruling out a leak or abnormal workload

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.35 MEMORY_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Table 8-36 MEMORY_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	Memory usage for {{$labels.service}} service is above 90%
Summary	Memory usage for {{$labels.service}} service is above 90%
Severity	Critical
Expression	avg by (namespace, service) (avg_over_time(cgroup_memory_usage[2m])) >= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.24
Metric Used	container_memory_usage_bytes **Note**: This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.
Recommended Actions	**Cause**: Indicates that the service's memory usage stays at or above the minor threshold for the configured window that is 90% This usually indicates sustained memory growth, repeated spikes from traffic or payload size, cache expansion, or a memory leak in the PRE service. It can also be triggered by recent deployment changes, higher concurrency, or a misconfigured memory limit. **Diagnostic Information**: • Check memory graphs for the PRE service to confirm whether usage is constantly high or only spiking. • Review whether the alert aligns with traffic bursts, deployment changes, or a specific job or request pattern. **Recovery**: • If memory usage reaches ~90% of the defined threshold, perform a rolling restart of PRE pods to immediately relieve memory pressure. • Investigate and address underlying causes such as leaks, cache growth, or abnormal traffic patterns. • If the issue persists or root cause is unclear, reach out to Oracle Support for further analysis and guidance.

8.1.1.36 POD_CONGESTED

Table 8-37 POD_CONGESTED

Field	Details
Description	The pod congestion status is set to congested.
Summary	Pod Congestion status of {{$labels.service}} service is congested
Severity	Critical
Expression	occnp_pod_congestion_state == 4
OID	1.3.6.1.4.1.323.5.3.52.1.2.26
Metric Used	occnp_pod_congestion_state

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-37 (Cont.) POD_CONGESTED

Field	Details
Recommended Actions	**Cause**: This alert is caused when the pod has reached the CONGESTED state based on CPU consumption and/or the pending request queue exceeding the active threshold profile. **Diagnostic Information**: • Check occnp_pod_congestion_state (expect 4), pod_resource_congestion_state for cpu/queue, pod_resource_stress, and occnp_http_congestion_message_reject_total (filter by congestionState, requestUri, requestMethod, priority). **Recovery**: • In CNC Console (PCF → Overload and Congestion Control → Congestion Control), ensure the feature is enabled and the intended Thresholds and Load Shedding profiles are active. • If rejections are excessive: – Raise discard priority for the current state or relax thresholds based on performance baselines. – Consider increasing stateChangeSampleCount and/or the calculation interval to reduce flapping due to short spikes.

8.1.1.37 POD_DANGER_OF_CONGESTION

Table 8-38 POD_DANGER_OF_CONGESTION

Field	Details
Description	The pod congestion status is set to Danger of Congestion.
Summary	Pod Congestion status of {{$labels.service}} service is DoC
Severity	Major
Expression	occnp_pod_congestion_state == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.25
Metric Used	occnp_pod_congestion_state

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-38 (Cont.) POD_DANGER_OF_CONGESTION

Field	Details
Recommended Actions	**Cause**: This alert is caused when the pod has reached the DANGER_OF_CONGESTION state based on CPU consumption and/or the pending request queue exceeding the active threshold profile. **Diagnostic Information**: • Check occnp_pod_congestion_state (expect 1), pod_resource_congestion_state for cpu/queue, pod_resource_stress, and occnp_http_congestion_message_reject_total (filter by congestionState, requestUri, requestMethod, priority). **Recovery**: • In CM GUI (PCF → Overload and Congestion Control → Congestion Control), ensure the feature is enabled and the intended Thresholds and Load Shedding profiles are active. • If rejections are excessive: • Lower the load-shedding aggressiveness for Major (if profiles are staged by state): • Raise the discard priority threshold for Danger of Congention state (i.e., be less aggressive in Major). In Major, reject only lower-priority traffic, and allow more mid/high-priority requests through. • Keep Critical/Congested configured to reject more aggressively than Major so escalation still protects the system. • Also validate the rules are not unintentionally catching important traffic: • Check mapping/classification so that critical call flows are assigned higher priority and are not being discarded in Major • If frequent transitions between Normal and Major due to brief spikes: • Increase stateChangeSampleCount (requires more consecutive samples before state changes) • Increase the calculation interval (smooths short spikes) • After changes: • Monitor Major-state duration, rejection rate, latency, and resource utilization • Confirm Major no longer causes excessive rejections, but still escalates to Critical when true overload occurs • Apply changes incrementally and follow change control procedures

8.1.1.38 POD_PENDING_REQUEST_CONGESTED

Table 8-39 POD_PENDING_REQUEST_CONGESTED

Field	Details
Description	The pod congestion status is set to congested for PendingRequest.
Summary	Pod Resource Congestion status of {{$labels.microservice}} service is congested for resource type
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="queue"} == 4
OID	1.3.6.1.4.1.323.5.3.52.1.2.28
Metric Used	occnp_pod_resource_congestion_state{type="queue"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-39 (Cont.) POD_PENDING_REQUEST_CONGESTED

Field	Details
Recommended Actions	**Cause**: The pod has reached the CONGESTED state based on the pending request queue exceeding the active threshold profile. **Diagnostic Information**: • Check occnp_pod_congestion_state (expect 4), pod_resource_congestion_state for type queue, pod_resource_stress, and occnp_http_congestion_message_reject_total (filter by congestionState, requestUri, requestMethod, priority). **Recovery**: • In CNC Console (PCF → Overload and Congestion Control → Congestion Control), ensure the feature is enabled and the intended Thresholds and Load Shedding profiles are active. • If rejections are excessive: • Raise discard priority for the current state or relax pending request queue thresholds based on performance baselines. • Consider increasing stateChangeSampleCount and/or the calculation interval to reduce flapping due to short spikes.

8.1.1.39 POD_PENDING_REQUEST_DANGER_OF_CONGESTION

Table 8-40 POD_PENDING_REQUEST_DANGER_OF_CONGESTION

Field	Details
Description	The pod congestion status is set to Danger of Congestion for pending requests.
Summary	Pod Resource Congestion status of {{$labels.service}} service is Danger of Congestion for PendingRequest type.
Severity	Major
Expression	occnp_pod_resource_congestion_state{type="queue"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.27
Metric Used	occnp_pod_resource_congestion_state{type="queue"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-40 (Cont.) POD_PENDING_REQUEST_DANGER_OF_CONGESTION

Field	Details
Recommended Actions	**Cause**: This alert is caused when the pod has reached the DANGER_OF_CONGESTION state based on the pending request queue exceeding the active threshold profile. **Diagnostic Information**: • Check occnp_pod_congestion_state (expect 1), pod_resource_congestion_state for queue, pod_resource_stress, and occnp_http_congestion_message_reject_total (filter by congestionState, requestUri, requestMethod, priority). **Recovery**: • In CM GUI (PCF → Overload and Congestion Control → Congestion Control), ensure the feature is enabled and the intended Thresholds and Load Shedding profiles are active. • If rejections are excessive: • Lower the load-shedding aggressiveness for Major (if profiles are staged by state): • Raise the discard priority threshold for Danger of Congention state (i.e., be less aggressive in Major). In Major, reject only lower-priority traffic, and allow more mid/high-priority requests through. • Keep Critical/Congested configured to reject more aggressively than Major so escalation still protects the system. • Also validate the rules are not unintentionally catching important traffic: • Check mapping/classification so that critical call flows are assigned higher priority and are not being discarded in Major • If frequent transitions between Normal and Major due to brief spikes: • Increase stateChangeSampleCount (requires more consecutive samples before state changes) • Increase the calculation interval (smooths short spikes) • After changes: • Monitor Major-state duration, rejection rate, latency, and resource utilization • Confirm Major no longer causes excessive rejections, but still escalates to Critical when true overload occurs • Apply changes incrementally and follow change control procedures

8.1.1.40 POD_CPU_CONGESTED

Table 8-41 POD_CPU_CONGESTED

Field	Details
Name in Alert Yaml File	PodCPUCongested
Description	The pod congestion status is set to congested for CPU.
Summary	Pod Resource Congestion status of {{$labels.service}} service is congested for CPU type.
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="cpu"} == 4
OID	1.3.6.1.4.1.323.5.3.52.1.2.30
Metric Used	occnp_pod_resource_congestion_state{type="cpu"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-41 (Cont.) POD_CPU_CONGESTED

Field	Details
Recommended Actions	**Cause**: The pod has reached the CONGESTED state based on the CPU Consumption exceeding the active threshold profile. **Diagnostic Information**: • Check occnp_pod_congestion_state (expect 4), pod_resource_congestion_state for type cpu, pod_resource_stress, and occnp_http_congestion_message_reject_total (filter by congestionState, requestUri, requestMethod, priority). **Recovery**: • In CM GUI (PCF → Overload and Congestion Control → Congestion Control), ensure the feature is enabled and the intended Thresholds and Load Shedding profiles are active. • If rejections are excessive: • Raise discard priority for the current state or relax cpu thresholds based on performance baselines. • Consider increasing stateChangeSampleCount and/or the calculation interval to reduce flapping due to short spikes.

8.1.1.41 POD_CPU_DANGER_OF_CONGESTION

Table 8-42 POD_CPU_DANGER_OF_CONGESTION

Field	Details
Description	Pod Resource Congestion status of {{$labels.service}} service is DoC for CPU type.
Summary	Pod Resource Congestion status of {{$labels.service}} service is DoC for CPU type.
Severity	Major
Expression	occnp_pod_resource_congestion_state{type="cpu"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.29
Metric Used	occnp_pod_resource_congestion_state{type="cpu"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-42 (Cont.) POD_CPU_DANGER_OF_CONGESTION

Field	Details
Recommended Actions	**Cause**: This alert is caused when the pod has reached the DANGER_OF_CONGESTION state based on the CPU Utilization exceeding the active threshold profile. **Diagnostic Information**: • Check occnp_pod_congestion_state (expect 1), pod_resource_congestion_state for queue, pod_resource_stress, and occnp_http_congestion_message_reject_total (filter by congestionState, requestUri, requestMethod, priority). **Recovery**: • In CM GUI (PCF → Overload and Congestion Control → Congestion Control), ensure the feature is enabled and the intended Thresholds and Load Shedding profiles are active. • If rejections are excessive: • Lower the load-shedding aggressiveness for Major (if profiles are staged by state): • Raise the discard priority threshold for Danger of Congention state (i.e., be less aggressive in Major). In Major, reject only lower-priority traffic, and allow more mid/high-priority requests through. • Keep Critical/Congested configured to reject more aggressively than Major so escalation still protects the system. • Also validate the rules are not unintentionally catching important traffic: • Check mapping/classification so that critical call flows are assigned higher priority and are not being discarded in Major • If frequent transitions between Normal and Major due to brief spikes: • Increase stateChangeSampleCount (requires more consecutive samples before state changes) • Increase the calculation interval (smooths short spikes) • After changes: • Monitor Major-state duration, rejection rate, latency, and resource utilization • Confirm Major no longer causes excessive rejections, but still escalates to Critical when true overload occurs • Apply changes incrementally and follow change control procedures

8.1.1.42 SERVICE_OVERLOADED

Table 8-43 SERVICE_OVERLOADED

Field	Details
Description	Overload Level of {{$labels.service}} service is L1
Summary	Overload Level of {{$labels.service}} service is L1
Severity	Minor
Expression	load_level == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.40
Metric Used	load_level

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-43 (Cont.) SERVICE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: Possible causes include: CPU: brief CPU spike (burst traffic, short expensive operation) Pending requests: short-lived queue buildup due to bursty arrivals or slight latency increase Failures: small error spike (transient dependency wobble, brief network blip) **Diagnostic Information**: • Identify the signal that triggered L1. • CPU trend across pods (is it widespread or a few pods?) • Gateway pending requests trend (spike vs sustained) • Gateway failures (error codes/timeouts; any single dependency implicated?) • Check the impact: • p95/p99 latency, timeout rate, reject/drop counters • Check stability: • Determine whether load_level fluctuates between 0 and 1. **Recovery**: • Stabilize the calculation to avoid flapping. • Increase stateChangeSampleCount and/or the calculation interval • Ensure hysteresis between Normal -> L1 (entry vs exit thresholds) • Apply load shedding only when necessary. • Priority-based: Configure L1 to discard only lowest-priority traffic. If L1 rejections are too high, make L1 less aggressive by raising the discard cutoff (so fewer requests are discarded). • Percentage-based: Keep L1 reject % minimal; prefer smoothing/hysteresis tuning over increasing shedding. • If CPU usage remains high at L1: • Validate autoscaling (HPA) and check if CPU limits/requests are constraining the service.

Table 8-44 SERVICE_OVERLOADED

Field	Details
Description	Overload Level of {{$labels.service}} service is L2
Summary	Overload Level of {{$labels.service}} service is L2
Severity	Major
Expression	load_level == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.40
Metric Used	load_level

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-44 (Cont.) SERVICE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: Possible causes include: CPU high + pending requests rising: service capacity issue (not enough replicas/CPU), or inefficient code path under current traffic mix. Pending requests high but CPU not that high: waiting on something (downstream latency), thread/connection pool bottleneck, or gateway/service concurrency limit. Failures rising (with or without pending): dependency degradation/outage, timeouts, bad config/release, or a retry storm. **Diagnostic Information**: • CPU check • Is CPU high across most pods? If yes, likely compute/capacity. • Any recent deployment/config changes increasing CPU per request? • Pending request check • Is backlog steadily increasing? If yes, service throughput < arrival rate. • Correlate pending with latency: rising pending usually pairs with rising p95/p99. • Failure check • What failure types dominate (timeouts vs immediate 5xx/4xx)? • Are failures linked to a downstream dependency or a specific endpoint? • Amplification check • Evidence of retries (repeated attempts, rising incoming rate without real user growth). **Recovery**: • Apply stronger overload protection to prevent L3 • Priority-based: • In L2, discard low priority (and if required, some medium priority) traffic to preserve core/high-priority flows. Ensure L3 remains stricter than L2. • Percentage-based: • Increase reject % to a moderate level, ideally targeting non-critical traffic classes/paths first. • Address the dominant limiter • If CPU-driven: scale out replicas (and/or increase CPU limits) within approved capacity. verify node pool can schedule them. • If pending-driven but CPU not high: investigate downstream latency/connection pools; scaling may not help • if you're blocked on a dependency. • If failure-driven: prioritize dependency recovery, rollback recent changes if indicated, and reduce retry amplification.

Table 8-45 SERVICE_OVERLOADED

Field	Details
Description	Overload Level of {{$labels.service}} service is L3
Summary	Overload Level of {{$labels.service}} service is L3
Severity	Critical
Expression	load_level == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.40
Metric Used	load_level

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-45 (Cont.) SERVICE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: Possible causes include: CPU very high + large backlog: hard capacity ceiling reached (service cannot keep up). Backlog extreme + failures rising: downstream outage/major latency event causing timeouts, then retry storm. Failures very high (even if CPU isn't maxed): widespread error condition (network/DNS/certs/routing, bad release, dependency down). **Diagnostic Information**: • Confirm which of the three is worst right now: – CPU saturation? – Pending requests runaway queue? – Failures/timeouts spiking? – Check cluster/platform health (node readiness, network/DNS/CNI, ingress/LB). – Confirm critical traffic classification (so core flows aren't mistakenly treated as low priority). **Recovery**: • Immediate containment (stop cascading failure) • Priority-based: Apply the strictest L3 discard rules—reject low priority and, if needed, some medium priority traffic to keep the highest-priority flows alive. • Percentage-based: Increase reject % aggressively (again, prefer non-critical traffic first if supported). • Then restore stability • If dependency-driven (failures/timeouts): fix/mitigate the dependency first; scaling the service may worsen downstream load. • If compute-driven and dependencies are healthy: scale out rapidly (replicas/nodes) and consider temporarily reducing expensive traffic/features if operationally possible. • Engage relevant platform/dependency owners—L3 is typically a cross-team incident.

8.1.1.43 SERVICE_RESOURCE_OVERLOADED

Alerts when service is in overload state due to memory usage

Table 8-46 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type
Severity	Minor
Expression	service_resource_overload_level{type="memory"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="memory"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-46 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: Service is at overload level L1 specifically for memory. Drivers: memory leak, higher concurrency, cache growth, large payloads, misconfiguration of memory limits/ heap, node memory pressure. **Diagnostic Information**: • Memory usage trend per pod; OOMKilled/restarts. • GC pressure (if applicable), allocation spikes. • Check limits/requests and node memory pressure. • Correlate with traffic and recent changes. **Recovery**: • Reduce memory pressure (tune caches/payloads), fix leaks/rollback regressions. • Scale out to reduce per-pod footprint; adjust memory limits cautiously. • Clears when overload level drops to 0.

Table 8-47 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type
Severity	Major
Expression	service_resource_overload_level{type="memory"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="memory"}
Recommended Actions	**Cause**: Service is at overload level L2 specifically for memory. Drivers: memory leak, higher concurrency, cache growth, large payloads, misconfiguration of memory limits/ heap, node memory pressure. **Diagnostic Information**: • Memory usage trend per pod; OOMKilled/restarts. • GC pressure (if applicable), allocation spikes. • Check limits/requests and node memory pressure. • Correlate with traffic and recent changes. **Recovery**: • Reduce memory pressure (tune caches/payloads), fix leaks/rollback regressions. • Scale out to reduce per-pod footprint; adjust memory limits cautiously. • Clears when overload level drops below 2.

Table 8-48 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type
Severity	Critical
Expression	service_resource_overload_level{type="memory"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="memory"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-48 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: Service is at overload level L3 specifically for memory. Drivers: memory leak, higher concurrency, cache growth, large payloads, misconfiguration of memory limits/ heap, node memory pressure. **Diagnostic Information**: • Memory usage trend per pod; OOMKilled/restarts. • GC pressure (if applicable), allocation spikes. • Check limits/requests and node memory pressure. • Correlate with traffic and recent changes. **Recovery**: • Reduce memory pressure (tune caches/payloads), fix leaks/rollback regressions. • Scale out to reduce per-pod footprint; adjust memory limits cautiously. • Clears when overload level drops below 3.

Alerts when service is in overload state due to CPU usage

Table 8-49 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type
Severity	Minor
Expression	service_resource_overload_level{type="cpu"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="cpu"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-49 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: This alert fires when the metric service_resource_overload_level indicates that a given service is experiencing Level 1 (L1) resource overload for the specified resource type. For this rule, the resource type is CPU, so it indicates CPU pressure at L1 for {{$labels.service}}. Common causes of CPU overload include: • Traffic increase causing higher request processing load • Background workload spikes (GC pressure, housekeeping tasks, batch jobs) • Insufficient CPU limits/requests or reduced node capacity • Node contention if running in a shared cluster • Recent deployment/config change that increased CPU usage L1 (MINOR) is an early warning. If overload persists or worsens (e.g., L2/L3), treat as potentially service impacting. **Diagnostic Information**: • Identify the impacted service/pod(s). Correlate with pod replica count and pod distribution across nodes recent deploys/config changes for that service • Validate CPU usage per pod / container for {{$labels.service}} • Check traffic and latency/error correlation determine if CPU overload correlates with: – Increased ingress traffic rate – p95/p99 latency increases increased – increased error rates / timeouts • Review logs for overload indicator, such as, overload control activation and request rejections **Recovery**: • Recovery Reduce load (short term): Divert traffic or reduce non-critical workloads impacting the service • If a retry storm is suspected, reduce retries/timeouts upstream • Scale the service: – Increase replicas (horizontal scaling) to distribute CPU load – Increase CPU requests/limits if the service is CPU-starved or throttled • Rollback recent changes if CPU increase started after a deployment • Stabilize dependencies: – If CPU is driven by retries or backpressure from downstream slowness, remediate the downstream dependency first (latency/outage can amplify CPU load). • Alert clearance: The alert clears automatically once service_resource_overload_level{type="cpu"} returns to 0 (or below L1) for the service.

Table 8-50 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type
Severity	Major
Expression	The overload level of the service is L2 due to CPU usage.
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="cpu"} == 2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-50 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: This alert fires when the metric service_resource_overload_level indicates that a given service is experiencing Level 2 (L2) resource overload for the specified resource type. For this rule, the resource type is CPU, so it indicates CPU pressure at L2 for {{$labels.service}}. Common causes of CPU overload include: • Traffic increase causing higher request processing load • Background workload spikes (GC pressure, housekeeping tasks, batch jobs) • Insufficient CPU limits/requests or reduced node capacity • Node contention if running in a shared cluster • Recent deployment/config change that increased CPU usage L2 (MAJOR) should generally be treated as service-impacting or at high risk of impact; **Diagnostic Information**: • Identify the impacted service/pod(s). Correlate with pod replica count and pod distribution across nodes recent deploys/config changes for that service • Validate CPU usage per pod / container for {{$labels.service}} • Check traffic and latency/error correlation determine if CPU overload correlates with: – Increased ingress traffic rate – p95/p99 latency increases increased – increased error rates / timeouts • Review logs for overload indicator, such as, overload control activation and request rejections **Recovery**: • Recovery Reduce load (short term): Divert traffic or reduce non-critical workloads impacting the service • If a retry storm is suspected, reduce retries/timeouts upstream • Scale the service: – Increase replicas (horizontal scaling) to distribute CPU load – Increase CPU requests/limits if the service is CPU-starved or throttled • Rollback recent changes if CPU increase started after a deployment • Stabilize dependencies: – If CPU is driven by retries or backpressure from downstream slowness, remediate the downstream dependency first (latency/outage can amplify CPU load). • Alert clearance: The alert clears automatically once service_resource_overload_level{type="cpu"} returns to 0 (or below L2) for the service.

Table 8-51 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type
Severity	Critical
Expression	service_resource_overload_level{type="cpu"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="cpu"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-51 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: This alert fires when the metric service_resource_overload_level indicates that a given service is experiencing Level 3 (L3) resource overload for the specified resource type. For this rule, the resource type is CPU, so it indicates CPU pressure at L3 for {{$labels.service}}. Common causes of CPU overload include: • Traffic increase causing higher request processing load • Background workload spikes (GC pressure, housekeeping tasks, batch jobs) • Insufficient CPU limits/requests or reduced node capacity • Node contention if running in a shared cluster • Recent deployment/config change that increased CPU usage L3 (CRITICAL) often precedes cascading failures; prioritize load shedding + scaling before deep debugging. **Diagnostic Information**: • Identify the impacted service/pod(s). Correlate with pod replica count and pod distribution across nodes recent deploys/config changes for that service • Validate CPU usage per pod / container for {{$labels.service}} • Check traffic and latency/error correlation determine if CPU overload correlates with: – Increased ingress traffic rate – p95/p99 latency increases increased – increased error rates / timeouts • Review logs for overload indicator, such as, overload control activation and request rejections **Recovery**: • Recovery Reduce load (short term): Divert traffic or reduce non-critical workloads impacting the service • If a retry storm is suspected, reduce retries/timeouts upstream • Scale the service: – Increase replicas (horizontal scaling) to distribute CPU load – Increase CPU requests/limits if the service is CPU-starved or throttled • Rollback recent changes if CPU increase started after a deployment • Stabilize dependencies: – If CPU is driven by retries or backpressure from downstream slowness, remediate the downstream dependency first (latency/outage can amplify CPU load). • Alert clearance: The alert clears automatically once service_resource_overload_level{type="cpu"} returns to 0 (or below L3) for the service.

Alerts when service is in overload state due to number of pending messages

Table 8-52 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type
Severity	Minor
Expression	service_resource_overload_level{type="svc_pending_count"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.41

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-52 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Metric Used	service_resource_overload_level{type="svc_pending_count"}
Recommended Actions	**Cause**: svc_pending_count is the number of pending/in-flight work items queued for processing by {{$labels.service}}. L1 indicates an early backlog build-up. Common contributors: • Short traffic spike / bursty arrivals • Sustained traffic above capacity • Temporary downstream slowdown/backpressure/outage • Resource constraints (CPU starvation/throttling, insufficient replicas, node pressure) • Reduced processing capacity (pods not ready, fewer replicas, node contention) • Increased per-request work after a deploy/config change • Database slowness (query latency, lock waits, pool pressure) blocking workers • High istio-proxy CPU and/or throttling increasing proxy/transport overhead and slowing completion **Diagnostic Information**: • Confirm backlog behavior: confirm pending count is high and not draining. • Check impact signals: p95/p99 latency, timeout rate, error rate, retry rate. • Correlate with load: compare ingress/request rate vs completion/throughput. • Pod/service health: restarts, readiness failures, uneven load distribution; check recent deploy/config changes. • MySQL checks: query latency/timeouts, connection count/pool usage, lock waits/deadlocks, slow query log/top slow queries. • Istio-proxy checks: istio-proxy CPU usage and CPU throttling; check whether spikes correlate with queue growth. If available, review Envoy indicators such as upstream timeouts/resets/retries. • Logs: queue buildup warnings, slow-processing messages, DB timeout/retry errors, Envoy upstream timeout/reset patterns. • Recent changes: deployments/config changes in service, Istio policy/telemetry changes, DB parameter changes. **Recovery**: • If transient, monitor; backlog should drain as dependencies/CPU normalize. • If backlog persists: • Remediate MySQL performance (address slow queries/indexing, reduce contention, ensure DB capacity, tune pools/timeouts). • Reduce istio-proxy overhead (right-size CPU requests/limits, tune telemetry/log volume, verify retry policies aren't amplifying load). • Scale out {{$labels.service}} (add replicas) to increase throughput (ensure DB can handle added concurrency). • Apply load shedding if supported to prevent queue growth. • Alert clears when overload level drops below 1.

Table 8-53 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type
Severity	Major
Expression	service_resource_overload_level{type="svc_pending_count"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.41

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-53 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Metric Used	service_resource_overload_level{type="svc_pending_count"}
Recommended Actions	**Cause**: svc_pending_count is the number of pending/in-flight work items queued for processing by {{$labels.service}}. L2 indicates an early backlog build-up. Common contributors: • Short traffic spike / bursty arrivals • Sustained traffic above capacity • Temporary downstream slowdown/backpressure/outage • Resource constraints (CPU starvation/throttling, insufficient replicas, node pressure) • Reduced processing capacity (pods not ready, fewer replicas, node contention) • Increased per-request work after a deploy/config change • Database slowness (query latency, lock waits, pool pressure) blocking workers • High istio-proxy CPU and/or throttling increasing proxy/transport overhead and slowing completion **Diagnostic Information**: • Confirm backlog behavior: confirm pending count is high and not draining. • Check impact signals: p95/p99 latency, timeout rate, error rate, retry rate. • Correlate with load: compare ingress/request rate vs completion/throughput. • Pod/service health: restarts, readiness failures, uneven load distribution; check recent deploy/config changes. • MySQL checks: query latency/timeouts, connection count/pool usage, lock waits/deadlocks, slow query log/top slow queries. • Istio-proxy checks: istio-proxy CPU usage and CPU throttling; check whether spikes correlate with queue growth. If available, review Envoy indicators such as upstream timeouts/resets/retries. • Logs: queue buildup warnings, slow-processing messages, DB timeout/retry errors, Envoy upstream timeout/reset patterns. • Recent changes: deployments/config changes in service, Istio policy/telemetry changes, DB parameter changes. **Recovery**: • If transient, monitor; backlog should drain as dependencies/CPU normalize. • If backlog persists: • Remediate MySQL performance (address slow queries/indexing, reduce contention, ensure DB capacity, tune pools/timeouts). • Reduce istio-proxy overhead (right-size CPU requests/limits, tune telemetry/log volume, verify retry policies aren't amplifying load). • Scale out {{$labels.service}} (add replicas) to increase throughput (ensure DB can handle added concurrency). • Apply load shedding if supported to prevent queue growth. • Alert clears when overload level drops to 0 or below 1.

Table 8-54 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type
Severity	Critical
Expression	service_resource_overload_level{type="svc_pending_count"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.41

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-54 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Metric Used	service_resource_overload_level{type="svc_pending_count"}
Recommended Actions	**Cause**: svc_pending_count is the number of pending/in-flight work items queued for processing by {{$labels.service}}. L3 indicates an early backlog build-up. Common contributors: • Short traffic spike / bursty arrivals • Sustained traffic above capacity • Temporary downstream slowdown/backpressure/outage • Resource constraints (CPU starvation/throttling, insufficient replicas, node pressure) • Reduced processing capacity (pods not ready, fewer replicas, node contention) • Increased per-request work after a deploy/config change • Database slowness (query latency, lock waits, pool pressure) blocking workers • High istio-proxy CPU and/or throttling increasing proxy/transport overhead and slowing completion **Diagnostic Information**: • Confirm backlog behavior: confirm pending count is high and not draining. • Check impact signals: p95/p99 latency, timeout rate, error rate, retry rate. • Correlate with load: compare ingress/request rate vs completion/throughput. • Pod/service health: restarts, readiness failures, uneven load distribution; check recent deploy/config changes. • MySQL checks: query latency/timeouts, connection count/pool usage, lock waits/deadlocks, slow query log/top slow queries. • Istio-proxy checks: istio-proxy CPU usage and CPU throttling; check whether spikes correlate with queue growth. If available, review Envoy indicators such as upstream timeouts/resets/retries. • Logs: queue buildup warnings, slow-processing messages, DB timeout/retry errors, Envoy upstream timeout/reset patterns. • Recent changes: deployments/config changes in service, Istio policy/telemetry changes, DB parameter changes. **Recovery**: • If transient, monitor; backlog should drain as dependencies/CPU normalize. • If backlog persists: • Remediate MySQL performance (address slow queries/indexing, reduce contention, ensure DB capacity, tune pools/timeouts). • Reduce istio-proxy overhead (right-size CPU requests/limits, tune telemetry/log volume, verify retry policies aren't amplifying load). • Scale out {{$labels.service}} (add replicas) to increase throughput (ensure DB can handle added concurrency). • Apply load shedding if supported to prevent queue growth. • Alert clears when overload level drops to 0 or below 3.

Alerts when service is in overload state due to number of failed requests

Table 8-55 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type.
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-55 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Expression	service_resource_overload_level{type="svc_failure_count"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="svc_failure_count"}
Recommended Actions	**Cause**: svc_failure_count indicates elevated service-side failures (internal failures while processing work) reaching overload level L1. Common drivers: • Dependency failures (DB down/slow, peer NF failures) • Timeouts leading to failures and retries • Resource exhaustion (CPU/memory/queue) causing rejections • Misconfiguration or regression after deploy • Network/service mesh issues (upstream resets/timeouts) **Diagnostic Information**: • Identify which failure types dominate (error codes, exception classes, timeout vs non-timeout). • Correlate failures with dependency health (DB latency/errors, connection pool, peer availability). • Check resource saturation signals (CPU, memory, pending queue). • Review service logs for repeated stack traces, “too busy/queue full”, connection failures. • Check recent deployments/config changes. **Recovery**: • Restore dependencies and reduce timeouts/retries amplification. • Scale out service and/or adjust resource limits if saturation is contributing. • Fix misconfig/regression; rollback if needed. • Clears when overload level drops below the level.

Table 8-56 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type.
Severity	Major
Expression	service_resource_overload_level{type="svc_failure_count"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="svc_failure_count"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-56 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: svc_failure_count indicates elevated service-side failures (internal failures while processing work) reaching overload level L2. Common drivers: • Dependency failures (DB down/slow, peer NF failures) • Timeouts leading to failures and retries • Resource exhaustion (CPU/memory/queue) causing rejections • Misconfiguration or regression after deploy • Network/service mesh issues (upstream resets/timeouts) **Diagnostic Information**: • Identify which failure types dominate (error codes, exception classes, timeout vs non-timeout). • Correlate failures with dependency health (DB latency/errors, connection pool, peer availability). • Check resource saturation signals (CPU, memory, pending queue). • Review service logs for repeated stack traces, “too busy/queue full”, connection failures. • Check recent deployments/config changes. **Recovery**: • Restore dependencies and reduce timeouts/retries amplification. • Scale out service and/or adjust resource limits if saturation is contributing. • Fix misconfig/regression; rollback if needed. • Clears when overload level drops below the level.

Table 8-57 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type.
Severity	Critical
Expression	service_resource_overload_level{type="svc_failure_count"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.41
Metric Used	service_resource_overload_level{type="svc_failure_count"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-57 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Recommended Actions	**Cause**: svc_failure_count indicates elevated service-side failures (internal failures while processing work) reaching overload level L3. Common drivers: • Dependency failures (DB down/slow, peer NF failures) • Timeouts leading to failures and retries • Resource exhaustion (CPU/memory/queue) causing rejections • Misconfiguration or regression after deploy • Network/service mesh issues (upstream resets/timeouts) **Diagnostic Information**: • Identify which failure types dominate (error codes, exception classes, timeout vs non-timeout). • Correlate failures with dependency health (DB latency/errors, connection pool, peer availability). • Check resource saturation signals (CPU, memory, pending queue). • Review service logs for repeated stack traces, “too busy/queue full”, connection failures. • Check recent deployments/config changes. **Recovery**: • Restore dependencies and reduce timeouts/retries amplification. • Scale out service and/or adjust resource limits if saturation is contributing. • Fix misconfig/regression; rollback if needed. • L3 should be treated as incident-level if sustained. • Clears when overload level drops below the level.

8.1.1.44 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD

Table 8-58 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the critical threshold limit for a given Subscriber Notification server.
Summary	Transaction Error exceeds the critical threshold limit for a given Subscriber Notification server.
Severity	Critical
Expression	sum by(notificationEndpoint) (increase(http_notification_response_total{responseCode!~"2.*"}[2m])) > 1000
OID	1.3.6.1.4.1.323.5.3.44.1.2.42
Metric Used	http_notification_response_total{responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-58 (Cont.) SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause**: SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD indicates a critical increase in notification transaction failures for a given notificationEndpoint. The alert fires when non-2xx HTTP responses exceed 1000 within 2 minutes (per endpoint), suggesting the Subscriber Notification server is failing to deliver notifications successfully. **Diagnostic Information**: • Identify which response codes dominate (e.g., 4xx vs 5xx vs 429) for the affected notificationEndpoint. • Confirm whether the issue is isolated to one endpoint or widespread across endpoints (compare top failing endpoints). • Correlate with latency and timeout signals (HTTP client timeouts, upstream duration histograms if available). • Check Subscriber Notification server logs for: repeated errors, payload validation failures, auth errors, TLS handshake failures, connection timeouts/resets. • Validate downstream endpoint health: DNS resolution, cert validity, firewall rules, rate limiting (429), maintenance windows. • Check internal dependencies used for notification delivery (DB/queue/service mesh): errors, saturation, connection pool exhaustion. • Review recent deployments/config changes affecting: endpoint routing, auth credentials, payload format, retry policy, timeout policy. **Recovery**: • If failures are 4xx, fix payload/auth/config issues (credentials, headers, schema) and reprocess if applicable. • If failures are 5xx/timeouts, stabilize dependencies and reduce retry amplification (add backoff/jitter, cap concurrency). • If downstream endpoint is unhealthy or rate-limiting (429), coordinate with endpoint owner, apply throttling, and/or pause/retry with backoff. • If resource saturation is contributing, scale out the service and/or adjust resource limits/queues. • Rollback recent changes if a regression is suspected. • Treat sustained CRITICAL as incident-level, especially if impacting multiple endpoints or causing backlog growth. • Clears when non-2xx responses for each notificationEndpoint drop below 1000 over 2 minutes.

Table 8-59 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the major threshold limit for a given Subscriber Notification server
Summary	Transaction Error exceeds the major threshold limit for a given Subscriber Notification server
Severity	Major
Expression	sum by(notificationEndpoint) (increase(http_notification_response_total{responseCode!~"2.*"}[2m])) > 750 and sum by(notificationEndpoint)(increase(http_notification_response_total{responseCode!~"2.*"}[2m])) <= 1000
OID	1.3.6.1.4.1.323.5.3.44.1.2.42
Metric Used	http_notification_response_total{responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-59 (Cont.) SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD indicates a critical increase in notification transaction failures for a given notificationEndpoint. The alert fires when non-2xx HTTP responses exceed 750 but less than1000 within 2 minutes (per endpoint), suggesting the Subscriber Notification server is failing to deliver notifications successfully. **Diagnostic Information**: • Server failures (5xx due to internal errors, dependency failures, timeouts). • Network/service mesh issues (timeouts, resets, MTLS/cert problems, proxy errors). • Retry storms/backpressure (retries amplifying failures; queue buildup increasing error volume). • Deployment/config regression (route changes, endpoint mapping changes, timeout changes). • Identify which response codes dominate (e.g., 4xx vs 5xx vs 429) for the affected notificationEndpoint. • Confirm whether the issue is isolated to one endpoint or widespread across endpoints (compare top failing endpoints). • Correlate with latency and timeout signals (HTTP client timeouts, upstream duration histograms if available). • Check Subscriber Notification server logs for: repeated errors, payload validation failures, auth errors, TLS handshake failures, connection timeouts/resets. • Validate downstream endpoint health: DNS resolution, cert validity, firewall rules, rate limiting (429), maintenance windows. • Check internal dependencies used for notification delivery (DB/queue/service mesh): errors, saturation, connection pool exhaustion. • Review recent deployments/config changes affecting: endpoint routing, auth credentials, payload format, retry policy, timeout policy. **Recovery**: • If failures are 4xx, fix payload/auth/config issues (credentials, headers, schema) and reprocess if applicable. • If failures are 5xx/timeouts, stabilize dependencies and reduce retry amplification (add backoff/jitter, cap concurrency). • If downstream endpoint is unhealthy or rate-limiting (429), coordinate with endpoint owner, apply throttling, and/or pause/retry with backoff. • If resource saturation is contributing, scale out the service and/or adjust resource limits/queues. • Rollback recent changes if a regression is suspected. • Treat sustained CRITICAL as incident-level, especially if impacting multiple endpoints or causing backlog growth. • Clears when non-2xx responses for each notificationEndpoint drop below 1000 over 2 minutes.

Table 8-60 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server
Summary	Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-60 (Cont.) SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD

Field	Details
Expression	sum by(notificationEndpoint) (increase(http_notification_response_total{responseCode!~"2.*"}[2m])) > 500 and sum by(notificationEndpoint)(increase(http_notification_response_total{responseCode!~"2.*"}[2m])) <= 750
OID	1.3.6.1.4.1.323.5.3.44.1.2.42
Metric Used	http_notification_response_total{responseCode!~"2.*"}
Recommended Actions	**Cause**: SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD indicates a critical increase in notification transaction failures for a given notificationEndpoint. The alert fires when non-2xx HTTP responses exceed 500 but remains lesser than 750 within 2 minutes (per endpoint), suggesting the Subscriber Notification server is failing to deliver notifications successfully. **Diagnostic Information**: • Server failures (5xx due to internal errors, dependency failures, timeouts). • Network/service mesh issues (timeouts, resets, MTLS/cert problems, proxy errors). • Retry storms/backpressure (retries amplifying failures; queue buildup increasing error volume). • Deployment/config regression (route changes, endpoint mapping changes, timeout changes). • Identify which response codes dominate (e.g., 4xx vs 5xx vs 429) for the affected notificationEndpoint. • Confirm whether the issue is isolated to one endpoint or widespread across endpoints (compare top failing endpoints). • Correlate with latency and timeout signals (HTTP client timeouts, upstream duration histograms if available). • Check Subscriber Notification server logs for: repeated errors, payload validation failures, auth errors, TLS handshake failures, connection timeouts/resets. • Validate downstream endpoint health: DNS resolution, cert validity, firewall rules, rate limiting (429), maintenance windows. • Check internal dependencies used for notification delivery (DB/queue/service mesh): errors, saturation, connection pool exhaustion. • Review recent deployments/config changes affecting: endpoint routing, auth credentials, payload format, retry policy, timeout policy. **Recovery**: • If failures are 4xx, fix payload/auth/config issues (credentials, headers, schema) and reprocess if applicable. • If failures are 5xx/timeouts, stabilize dependencies and reduce retry amplification (add backoff/jitter, cap concurrency). • If downstream endpoint is unhealthy or rate-limiting (429), coordinate with endpoint owner, apply throttling, and/or pause/retry with backoff. • If resource saturation is contributing, scale out the service and/or adjust resource limits/queues. • Rollback recent changes if a regression is suspected. • Treat sustained CRITICAL as incident-level, especially if impacting multiple endpoints or causing backlog growth. • Clears when non-2xx responses for each notificationEndpoint drop below 1000 over 2 minutes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.45 SYSTEM_IMPAIRMENT_MAJOR

Table 8-61 SYSTEM_IMPAIRMENT_MAJOR

Field	Details
Description	Major Impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage > 80%
Summary	Major impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage must be more than 80% for 10 minutes.
Severity	Major
Expression	(db_tier_replication_status{role="failed"} == 0) or (db_tier_replication_status{role="active"} == 0) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="standby"})) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="failed"})) or (avg_over_time(db_tier_binlog_used_bytes_percentage[5m])>= 80)
OID	1.3.6.1.4.1.323.5.3.52.1.2.43
Metric Used	db_tier_replication_status and db_tier_binlog_used_bytes_percentage

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-61 (Cont.) SYSTEM_IMPAIRMENT_MAJOR

Field	Details
Recommended Actions	**Cause**: SYSTEM_IMPAIRMENT_MAJOR indicates a major site impairment condition related to the DB tier, typically associated with replication health or binlog storage pressure. This alert is intended to fire when one or more of the following major-risk conditions occur (often mapped to REPLICATION_FAILED, REPLICATION_CHANNEL_DOWN, or BINLOG_STORAGE high usage): **Diagnostic Information**: • Replication failure (replication role reported as failed, or replication threads stopped) • Replication channel down / missing standby (expected replication roles are not present for the site, e.g., standby not reporting) • Primary/active not reporting (active role missing/unhealthy from metrics perspective) • Binlog storage growth due to replication lag, blocked purge, or high write rate, resulting in binlog usage 80% (as measured by db_tier_binlog_used_bytes_percentage) • Network issues between DB nodes/sites (timeouts, resets, packet loss) • DB load/resource saturation causing lag (CPU, IO, disk, connection pool) • Misconfiguration/regression after deploy/patch (replication settings, credentials, TLS/certs) • Determine which condition triggered the alert • Check current values and recent history for: – db_tier_replication_status{role="active"}, {role="standby"}, {role="failed"} – db_tier_binlog_used_bytes_percentage • Confirm whether the trigger is replication-related vs binlog-usage-related. • Replication health deep-dive • Identify impacted site_name and which node(s)/roles are missing or in failed. • Check replication lag, SQL/IO thread state, last error, and channel status on the DB nodes. • Channel/network validation • Check connectivity between active and standby. • Look for recent network maintenance, route changes, MTU issues, or service mesh/proxy impacts (if in path). • Binlog storage analysis (if binlog usage is high) • Confirm binlog filesystem utilization and growth rate; determine if purge is blocked. • Correlate with replication lag/backlog (binlogs often accumulate when standby can’t consume). • Check for unusually high write volume or long-running transactions. • Resource saturation / DB health • Check disk IOPS/latency, CPU, memory pressure, and connection pool saturation. • Review DB logs for replication errors, disk-full warnings, corruption, or restart events. • Change correlation • Check recent deploys/patches/config changes (DB parameters, replication config, storage changes). **Recovery**: • If replication failed / channel down: – Restore replication connectivity (network path, DNS, firewall, TLS/certs). – Restart/repair replication channel as per DB runbook; resolve the root error (permissions, missing binlogs, etc.).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-61 (Cont.) SYSTEM_IMPAIRMENT_MAJOR

Field	Details
	– If standby is unhealthy, recover/rebuild standby from a known-good snapshot/backup and rejoin replication. – Consider temporarily reducing write load or enabling throttling to allow the standby to catch up. • If binlog usage 80%: – Treat as urgent to avoid running out of storage (risk of DB outage). – Reduce binlog growth by addressing replication lag (fix channel, improve IO/CPU, reduce write amplification). – Expand binlog storage if needed (short-term mitigation) following capacity change procedures. – Ensure binlog purge/retention settings are correct and purge is not blocked (e.g., by lagging replicas). • Operational guidance: – Escalate as major if sustained, if multiple sites are impacted, or if lag/space continues to worsen. – After remediation, verify: – replication roles return to expected states (active/standby healthy; no failed) – replication lag stabilizes – db_tier_binlog_used_bytes_percentage drops below threshold and continues trending down

8.1.1.46 SYSTEM_IMPAIRMENT_CRITICAL

Table 8-62 SYSTEM_IMPAIRMENT_CRITICAL

Field	Details
Description	Critical Impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage > 80%
Summary	Critical impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage must be more than 80% for 30 minutes.
Severity	Critical
Expression	(db_tier_replication_status{role="failed"} == 0) or (db_tier_replication_status{role="active"} == 0) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="standby"})) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="failed"})) or (avg_over_time(db_tier_binlog_used_bytes_percentage[5m])>= 80)
OID	1.3.6.1.4.1.323.5.3.52.1.2.43
Metric Used	db_tier_replication_status and db_tier_binlog_used_bytes_percentage

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-62 (Cont.) SYSTEM_IMPAIRMENT_CRITICAL

Field	Details
Recommended Actions	**Cause**: SYSTEM_IMPAIRMENT_CRITICAL indicates a critical site impairment related to DB-tier replication health and/or binlog storage pressure. It is the higher-severity escalation of the impairment condition, intended to represent that one of the following has become sustained/critical (per description: replication failed, replication channel down, or binlog storage usage 80% for ~30 minutes). Common drivers: • Sustained replication failure (replication role reported as failed, replication threads stopped, unrecoverable SQL error) • Replication channel down for an extended period (standby missing/unreachable, broken link, auth/TLS failure) • Loss of expected topology (active/standby role metrics missing or inconsistent for a site) • Sustained binlog storage pressure (80%), typically due to replication lag/backlog, blocked purge, or abnormal write volume • Network instability between sites/DB nodes causing persistent disconnects and lag • Resource exhaustion on DB nodes (disk IO saturation, CPU, memory) preventing replication catch-up • Misconfiguration/regression after change (replication config, retention, credentials) **Diagnostic Information**: • Confirm the trigger and impacted site_name • Identify whether the critical is driven by replication status vs binlog usage trend. • Review current and historical values for: • db_tier_replication_status{role="active" | "standby" | "failed"} • db_tier_binlog_used_bytes_percentage (trend over last 30–60 minutes) • Replication failure/channel-down triage • On DB nodes, check replication channel state, IO/SQL thread status, last error, and lag. • Determine whether the standby is unreachable vs reachable-but-failing (auth/TLS/permissions vs data/SQL errors). • Confirm whether the “active” node is healthy and exporting metrics (avoid false positives from missing scrapes). • Topology consistency check • Validate expected number of replication endpoints per site (active + standby) and confirm none are missing. • If the alert logic is based on counts, verify whether a node is down or metrics are absent. • Binlog storage pressure investigation (if 80%) • Check filesystem utilization where binlogs reside and remaining headroom; estimate time-to-full. • Confirm whether binlog purge is blocked by lagging replica(s) or retention settings. • Correlate with write throughput and long transactions. • Dependency and resource saturation • Disk IO latency/queue depth, CPU, memory pressure, network throughput/packet loss. • DB error logs for disk-full warnings, replication errors, restarts, corruption indicators. • Change/event correlation • Look for recent deployments, DB patching, parameter changes, certificate rotations, or network maintenance coinciding with onset.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-62 (Cont.) SYSTEM_IMPAIRMENT_CRITICAL

Field	Details
	Recovery: • Immediate posture (CRITICAL): • Treat as incident-level due to risk of data protection loss (replication down) and/or imminent DB outage (binlog disk exhaustion). • Engage DB/platform/network on-call as required; follow site incident process. • If replication failed / channel down: • Restore connectivity (network/DNS/firewall) and fix auth/TLS/cert issues. • Restart/repair replication channels per runbook; remediate root cause (SQL errors, missing binlogs, GTID divergence). • If standby cannot be repaired quickly, rebuild standby from snapshot/backup and re-establish replication. • Consider temporarily throttling write load to reduce lag/backlog while recovering. • If binlog usage 80% (sustained): • Prevent disk-full: • reduce binlog generation (traffic/load throttling where feasible) • restore replication so binlogs can be consumed and purged • expand binlog storage/capacity as an emergency mitigation (per change controls) • Verify purge/retention settings and ensure purge is not blocked by an unreachable or stuck replica. • Validation or exit criteria: • Replication status returns to expected healthy roles (no failed, standby present and catching up). • Replication lag stabilizes within acceptable bounds. • db_tier_binlog_used_bytes_percentage trends downward and remains below threshold.

8.1.1.47 SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN

Table 8-63 SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN

Field	Details
Description	System Operational State is now in partial shutdown state.
Summary	System Operational State is now in partial shutdown state.
Severity	Major
Expression	system_operational_state == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.44
Metric Used	system_operational_state == 2

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-63 (Cont.) SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN

Field	Details
Recommended Actions	**Cause:** The site has entered the `PARTIAL SHUTDOWN` operational state under the Controlled Shutdown feature. This deliberate isolation mode supports maintenance, such as upgrades or configuration changes, or recovery activities, such as prolonged replication-channel failures or replication delay, while allowing existing sessions to continue. In this state, NRF status is `SUSPENDED` to prevent consumer discovery; the Ingress Gateway and Diameter Gateway permit only in-session messages and reject new session establishment; and the Egress Gateway has no restriction. This state is typically set through the CM GUI or REST API when `enableControlledShutdown` is enabled. **Diagnostic Information**: • Confirm the operational state is truly 2 (PARTIAL) and record transition time (use alert timestamp + metric history). • Verify whether the change was planned (maintenance/recovery activity) and who/what initiated it (CM GUI/REST). • Validate enableControlledShutdown is enabled and configuration is consistent across the site. • Verify expected gateway behavior: • Ingress rejects new session establishment but permits in-session traffic • Diameter permits in-session only • Check NRF to confirm NF status marked SUSPENDED and are not being discovered for new sessions. • Identify the underlying reason for isolation (maintenance, replication channel failures/delay, dependency instability) and correlate with replication metrics/logs. • Assess customer impact: rate of blocked new sessions, admission control counters, error codes returned at ingress/diameter. **Recovery:** For a planned shutdown, proceed with maintenance or recovery activities, such as replication repair or dependency stabilization, while keeping existing sessions stable. For an unplanned shutdown, confirm that no automation or configuration error triggered the change, correct configuration or access controls, and return to `NORMAL` when safe. After recovery, verify that NFs return to `REGISTERED` in NRF and that new session establishment succeeds at Ingress and Diameter. Escalate if the partial shutdown persists unexpectedly or blocks new sessions beyond agreed SLOs.

8.1.1.48 SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN

Table 8-64 SYSTEM_OPERATIONAL_COMPLETE_SHUTDOWN

Field	Details
Description	System Operational State is now in complete shutdown state
Summary	System Operational State is now in complete shutdown state
Severity	Critical
Expression	system_operational_state == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.44
Metric Used	system_operational_state

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-64 (Cont.) SYSTEM_OPERATIONAL_COMPLETE_SHUTDOWN

Field	Details
Recommended Actions	**Cause:** The site has entered the `COMPLETE SHUTDOWN` operational state under the Controlled Shutdown feature. This fully stops load and isolates the site during recovery or severe instability. NRF status is `SUSPENDED`, the Ingress Gateway accepts no requests, the Egress Gateway allows only NRF-bound requests, and Diameter Gateway external-peer connections are closed. **Diagnostic Information**: • Confirm the operational state is 3 (COMPLETE) and capture the exact change time and duration. • Verify whether complete isolation was intended (approved maintenance/incident action) and confirm initiator. • Validate actual enforcement at gateways: • Ingress is refusing all new connections • Diameter external peer sessions are closed • Egress allows only NRF-bound traffic • Confirm NRF state: NFs remain SUSPENDED and are not discoverable by consumers (SMF/AMF/etc.). • Identify the triggering condition that required complete shutdown (e.g., severe replication failure, corruption risk, cascading dependency failures) and gather supporting logs/metrics. • Confirm traffic has drained/failover behavior is functioning (upstream routing, peer sites capacity, no looping retries). • Check for any secondary effects: backlog growth, message queue accumulation, alarms from consumers due to loss of discovery. **Recovery:** Treat an unscheduled shutdown as an incident. Perform the maintenance or recovery procedure while the site is isolated, such as replication rebuild or data-consistency checks. When ready, transition to `PARTIAL` if required for validation, or directly to `NORMAL`; restore gateway connectivity and Egress behavior; update NRF status to `REGISTERED`; and validate discovery, new-session establishment, and clean Diameter-peer reconnection.

8.1.1.49 TDF_CONNECTION_DOWN

Table 8-65 TDF_CONNECTION_DOWN

Field	Details
Description	TDF connection is down.
Summary	TDF connection is down.
Severity	Critical
Expression	occnp_diam_conn_app_network{applicationName="Sd"} == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.48
Metric Used	occnp_diam_conn_app_network

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-65 (Cont.) TDF_CONNECTION_DOWN

Field	Details
Recommended Actions	**Cause**: TDF_CONNECTION_DOWN indicates the Diameter Gateway has lost connectivity to a configured TDF peer node (for the Sd Diameter application). The alert fires when `occnp_diam_conn_app_network{applicationName="Sd"} == 0`, meaning the Diameter GW reports the Sd application network connection is down (peer unreachable/disconnected). • Common drivers: – TDF peer node outage/restart or Diameter service down – Network connectivity loss between Diameter GW and TDF. – TLS/MTLS or certificate issues (expired/rotated certs, truststore mismatch) – Diameter peer configuration mismatch (host/realm, IP/port, capabilities) – Transport-level failures (TCP resets, keepalive failures, packet loss, MTU issues) – Gateway overload/resource pressure causing session drops (CPU/memory/thread starvation) **Diagnostic Information**: • Identify the affected TDF peer(s) from the Diameter GW reported message/alert details (peer host/IP/realm) and confirm it is a configured peer. • Verify whether the connection-down is isolated (single peer) or systemic (multiple peers down simultaneously). • Check Diameter GW logs/events around the disconnect time for: • disconnect reason codes, watchdog timeouts, capability exchange failures (CER/CEA), DPR/DPA • TLS handshake failures / certificate validation errors • connection refused / timeout / reset indications • Validate network path from Diameter GW to the TDF peer: • basic reachability (routing/VLAN/VXLAN), port access, firewall rules • recent network changes/maintenance • Confirm TDF peer health: • process/service status, listener port up, resource saturation • peer logs for rejecting connections, overload, or config errors • Check recent changes on either side: • peer definitions (host/realm/IP), allowed apps (Sd), policy changes • certificate rotations, cipher policy updates • If available, correlate with other metrics: • total active Diameter connections, reconnect attempts, watchdog counters, error rate spikes. **Recovery**: • Restore connectivity to the TDF peer: • bring up/restart TDF Diameter service if down • correct network/firewall/routing issues and confirm port reachability • Fix configuration mismatches (peer host/realm, IP/port, supported application “Sd”). • Resolve TLS/certificate issues (renew/replace certs, update truststores, align MTLS settings). • If gateway resource pressure contributed, scale/relieve load and investigate saturation triggers. • After remediation, verify: • `occnp_diam_conn_app_network{applicationName="Sd"}` returns to 1/up • peer sessions re-establish and remain stable (no flapping) • Diameter GW reports the peer as reachable in status output/logs

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.50 DIAM_CONN_PEER_DOWN

Table 8-66 DIAM_CONN_PEER_DOWN

Field	Details
Description	Diameter connection to peer {{ $labels.peerHost }} is down.
Summary	Diameter connection to peer is down.
Severity	Major
Expression	(sum by (namespace,peerHost)(occnp_diam_conn_network) == 0) and (sum by (namespace,peerHost)(max_over_time(occnp_diam_conn_network[24h])) != 0)
OID	1.3.6.1.4.1.323.5.3.52.1.2.50
Metric Used	occnp_diam_conn_network

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-66 (Cont.) DIAM_CONN_PEER_DOWN

Field	Details
Recommended Actions	**Cause**: DIAM_CONN_PEER_DOWN indicates the Diameter Gateway's network-side connection to a specific external peer (keyed by origHost) is currently down, even though it was successfully connected at least once in the last 24 hours. The alert logic is: • Now: sum by(kubernetes_namespace, origHost)(`occnp_diam_conn_network`) == 0 → no active connections for that peer • History: max_over_time(`occnp_diam_conn_network`[24h]) != 0 → the peer was up recently, so this is not "never configured" • This is a MAJOR condition because it typically impacts one peer (or a subset), not necessarily all external Diameter connectivity. • Common drivers: – Peer node/service down, restarting, or in maintenance – Network path issue specific to that peer (routing/ACL/firewall/NAT/DNS) – Transport instability (packet loss/latency causing watchdog timeouts, TCP resets) – TLS/mTLS handshake failures (cert expiry/rotation mismatch, trust mismatch, hostname/SNI mismatch, cipher/protocol mismatch) – Peer overload/throttling causing disconnects or refused connections – Configuration mismatch (peer IP/port, host/realm, supported applications) – Diameter GW resource pressure leading to selective peer drops/reconnect storms **Diagnostic Information**: • Identify the affected kubernetes_namespace and origHost value(s) and confirm whether this is a single peer or multiple peers. • Validate that the peer was up recently: • Confirm max_over_time(`occnp_diam_conn_network`[24h]) is non-zero for the same origHost. • Check Diameter GW logs/events for the affected peer around the time it went down: • watchdog failures (DWR/DWA), disconnect procedures (DPR/DPA) • CER/CEA negotiation failures • TCP connection refused/timeout/reset messages • TLS handshake/certificate validation failures (if TLS enabled to this peer) • Check the peer-side health: • service/process status, listener port, recent restarts • peer logs for reject/disconnect reasons and overload indicators • Validate network reachability from GW to that peer: • routing, firewall/NAT rules, DNS resolution • confirm whether only this peer path is impacted (vs broader outage). • If TLS is enabled for that peer, validate: • certificate validity/expiry and correct chain • trust bundle alignment on both sides • hostname/SNI and protocol/cipher compatibility • Correlate with recent changes: gateway/peer config updates, peer list changes, certificate rotations, network maintenance. **Recovery**: • Restore peer availability: • restart/repair peer service; coordinate with peer owner if external. • Restore connectivity: • fix routing/firewall/DNS issues affecting that peer; confirm required ports are open.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-66 (Cont.) DIAM_CONN_PEER_DOWN

Field	Details
	• Resolve TLS issues (if enabled): • renew/rotate certificates, update trust bundles, correct hostname/SNI or cipher/protocol settings • Address overload/instability: – scale/relieve load on GW or peer; ensure reconnect backoff is reasonable to avoid storms. • Validate recovery: – `occnp_diam_conn_network` for the affected origHost returns to > 0 – connection remains stable (no repeated flapping) – Diameter transaction success rates normalize for traffic targeting that peer

8.1.1.51 DIAM_CONN_NETWORK_DOWN

Table 8-67 DIAM_CONN_NETWORK_DOWN

Field	Details
Description	All the diameter network connections are down.
Summary	All the diameter network connections are down.
Severity	Critical
Expression	sum by (kubernetes_namespace)(occnp_diam_conn_network) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.51
Metric Used	occnp_diam_conn_network

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-67 (Cont.) DIAM_CONN_NETWORK_DOWN

Field	Details
Recommended Actions	**Cause**: DIAM_CONN_NETWORK_DOWN indicates the Diameter Gateway has no active Diameter network (external peer) connections in a given kubernetes_namespace. The alert fires when: • `sum by (kubernetes_namespace)(occnp_diam_conn_network) == 0`. This means the total count of established/healthy external/network-side Diameter connections reported by the gateway is zero for that namespace. This results in loss of Diameter connectivity to external peers (for example, TDF or other network peer nodes). • Common drivers (TLS may apply for external peers): – External peer outage/restart/maintenance (peer service down, listener not available) – Network path failure affecting all peers (routing/VRF/VLAN, firewall/ACL, NAT, DNS) – TLS/mTLS issues (expired/rotated certificates, CA/trust mismatch, hostname/SNI mismatch, cipher/protocol mismatch) – Peer configuration mismatch (wrong IP/port, host/realm, supported application such as Sd) – Transport instability (packet loss/latency causing watchdog timeouts, TCP resets) – Diameter GW instability/overload causing disconnects and failed reconnect attempts – Controlled shutdown/site isolation actions that intentionally close external peer connections (if applicable) **Diagnostic Information**: • Confirm impacted kubernetes_namespace and whether the issue is isolated or widespread. • Identify which peers are affected (if metrics/logs provide peer labels/details) and whether all external peers are down simultaneously. • Review Diameter GW logs/events around the drop: • watchdog failures (DWR/DWA), disconnect procedures (DPR/DPA) • CER/CEA failures (capabilities mismatch) • TCP timeouts/resets/connection refused • Validate external peer health: • peer process up, port listening, peer-side logs show accept/reject reasons • check whether peers are in maintenance or intentionally isolated. • Network reachability validation: • routing/firewall/NAT/security list correctness to all peers • confirm no recent network maintenance/changes coinciding with onset. • If TLS is enabled for external peers, validate TLS posture: • certificate expiry and correct certificate chain • truststore/CA bundle alignment on both sides • hostname/SNI matching (if used), protocol/cipher compatibility • Correlate with related alerts/metrics: – if backend connections are also down, suspect gateway-wide failure – if controlled shutdown is active, confirm external peer connections are expected to be closed. **Recovery**: • Restore external peer availability (restart/repair peer services; coordinate with peer owner teams). • Restore network connectivity (fix routing/ACL/firewall/NAT/DNS) and confirm required ports are reachable. • If TLS-related:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-67 (Cont.) DIAM_CONN_NETWORK_DOWN

Field	Details
	• renew/rotate certificates and update truststores/CA bundles • correct hostname/SNI/cipher/protocol mismatches • re-establish sessions after cert/config updates • Correct Diameter peer configuration (IP/port, host/realm, application enablement). • If GW resource pressure/instability contributed, scale/repair the gateway and address the underlying saturation. • Validate recovery: • `sum by (kubernetes_namespace)(occnp_diam_conn_network) returns to > 0` • external peer sessions remain stable (no frequent reconnects) • end-to-end Diameter transactions succeed and error rates normalize

8.1.1.52 DIAM_CONN_BACKEND_DOWN

Table 8-68 DIAM_CONN_BACKEND_DOWN

Field	Details
Description	All the diameter backend connections are down.
Summary	All the diameter backend connections are down.
Severity	Critical
Expression	sum by (kubernetes_namespace)(occnp_diam_conn_backend) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.52
Metric Used	occnp_diam_conn_network

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-68 (Cont.) DIAM_CONN_BACKEND_DOWN

Field	Details
Recommended Actions	**Cause**: DIAM_CONN_BACKEND_DOWN indicates the Diameter Gateway has no active connections to any internal backend services (for example, PCRF Core, Diam-Connector) within a given kubernetes_namespace. The alert fires when: • `sum by (kubernetes_namespace)(occnp_diam_conn_backend) == 0` • meaning the gateway reports the total number of established backend connections is zero for that namespace. With no backend connectivity, the Diameter GW will be unable to route/process Diameter requests that depend on those internal services. • Common drivers (no TLS involved for these backend connections): – Internal backend services unavailable (PCRF Core / Diam-Connector pods down, crashlooping, not Ready, rolling restart) – Service discovery issues (K8s Service selectors wrong, Endpoints/ EndpointSlices empty, wrong port/targetPort) – Network connectivity/policy issues inside cluster (NetworkPolicy blocking, CNI/kube-proxy/node networking issues) – Backend overload/backpressure (connection limits reached, listener not accepting, process unhealthy) – Diameter GW overload/resource issues (CPU/memory/file-descriptor exhaustion) causing connection drops/reconnect failures – Misconfiguration/regression after deploy (backend host/port/service name changes) **Diagnostic Information**: • Identify impacted kubernetes_namespace and confirm whether the issue is isolated to one namespace or widespread. • Break down `occnp_diam_conn_backend` by available labels (for example, GW pod/instance, and backend identifier if present) to determine whether: • all GW replicas have zero backend connections, or • only specific GW pods/nodes are affected. • Check backend service health (PCRF Core, Diam-Connector): • pod status, readiness and liveness, restarts, recent rollouts • application logs for “cannot accept connection”, “connection limit”, “listener down”, resource exhaustion • Verify Kubernetes Service/Endpoints for each backend: • Service exists and selectors match expected pods • Endpoints/EndpointSlices are non-empty and point to correct IP:port • port/targetPort configuration matches what the GW expects • Review Diameter GW logs for connection symptoms: • connection refused (backend not listening/not ready) • timeout (network path/policy/CNI issue or backend hung) • frequent reconnect loops / backend unavailable messages • Validate in-cluster networking: • NetworkPolicies allowing GW → backend traffic on required ports • node/CNI/kube-proxy issues if failures correlate to specific nodes • Correlate with recent changes: • deploys/config updates of Diameter GW, PCRF Core, Diam-Connector • service renames, port changes, scaling events. **Recovery**: • Restore backend availability: • fix/restart failing PCRF Core / Diam-Connector pods, ensure they become Ready. • Roll back recent backend changes if a regression is suspected. • scale backends if overloaded or hitting connection limits.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-68 (Cont.) DIAM_CONN_BACKEND_DOWN

Field	Details
	• Fix service discovery wiring: • correct Service selectors/ports/targetPorts; ensure EndpointSlices repopulate • Restore connectivity: • adjust/Roll back NetworkPolicies blocking traffic • remediate node/CNI/kube-proxy issues if connectivity is node-specific • Stabilize gateway/backends if resource pressure is contributing: • scale Diameter GW or increase resources/limits. • address FD exhaustion or excessive reconnect storms. • Validate recovery: • `sum by (kubernetes_namespace)(occnp_diam_conn_backend) returns to > 0` • connections to PCRF Core and Diam-Connector remain stable (no flapping) • Diameter transaction error/timeout rates return to baseline

8.1.1.53 PERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED

Table 8-69 PPERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED

Field	Details
Description	The application fails to get the current active overload level threshold data.
Summary	The application fails to get the current active overload level threshold data.
Severity	Major
Expression	active_overload_threshold_fetch_failed == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.53
Metric Used	active_overload_threshold_fetch_failed

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-69 (Cont.) PPERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED

Field	Details
Recommended Actions	**Cause**: The system has failed to fetch or retrieve the active overload threshold data, as indicated by the flag active_overload_threshold_fetch_failed == 1. This suggests that overload protection parameters are unavailable or not being correctly loaded, which may impact the system ability to handle traffic surges safely. **Diagnostic Information**: • Evaluate the following metric: • active_overload_threshold_fetch_failed == 1 • Trigger condition: Value equals 1 (failure state) • Interpretation: • The system could not fetch active overload threshold configuration/data • Perform the following checks: • Verify connectivity to the configuration source (e.g., database, config service, NMS) • Check if overload threshold data is properly configured and available • Review logs for errors related to config fetch failures or timeouts • Validate credentials and access permissions for configuration retrieval • Inspect recent configuration changes or deployments affecting overload settings • Ensure dependent services providing threshold data are up and responsive • Check for initialization issues during service startup **Recovery**: • Restore connectivity to the configuration or data source • Correct missing or invalid overload threshold configurations • Restart or reinitialize the component responsible for fetching the data • Fix authentication/authorization issues if access is denied • Roll back recent changes impacting configuration retrieval • Ensure high availability of configuration services (failover/replication) • Monitor until the metric returns to normal state (value = 0) • If the issue still persist, please contact the My Oracle Support.

8.1.1.54 SLA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-70 SLA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	SLA Sy fail count exceeds the critical threshold limit
Summary	Alert SLA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD > 90
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.58
Metric Used	occnp_diam_response_local_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-70 (Cont.) SLA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause**: The percentage of failed SLA (Subscriber Location Answer / Service-Level related Answer) Diameter responses has exceeded the critical threshold (greater than 90%). The condition indicates that the majority of SLA transactions are failing, which can significantly impact subscriber-related operations such as location handling, service validation, or policy enforcement depending on the SLA usage context. Likely causes include backend system failures, data unavailability, or signaling issues. **Diagnostic Information**: • Evaluate the following metric: • Failed SLA Responses / Total SLA Responses * 100 over a 5-minute window • Scope: • msgType = "SLA" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 90% • Perform the following checks: • Analyze Diameter response codes (for example, user unknown, system failure, data missing). • Verify connectivity to backend systems (for example, subscriber database, HSS/UDM, policy servers). • Check logs for request processing failures, timeouts, or invalid responses. • Validate subscriber data availability and consistency. • Monitor latency and retransmissions for SLA transactions. • Inspect system resource utilization (CPU, memory, thread pools). • Correlate with recent configuration or schema changes affecting subscriber data. **Recovery**: • Restore connectivity to backend/subscriber data systems. • Fix issues related to missing or inconsistent subscriber data. • Address specific Diameter error codes causing SLA failures. • Restart or scale affected services handling SLA traffic. • Roll back recent configuration or deployment changes if correlated. • Tune timeout and retry mechanisms if applicable • Continue monitoring until failure rate drops below the critical threshold. • For any additional guidance, contact My Oracle Support

8.1.1.55 SLA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-71 SLA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	SLA Sy fail count exceeds the major threshold limit
Summary	Alert SLA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD > 80 and <= 90
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.58

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-71 (Cont.) SLA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of failed SLA (Subscriber Location Answer / Service-Level related Answer) Diameter responses has exceeded the major threshold (greater than 80% and up to 90%). The condition indicates a high rate of SLA transaction failures, suggesting significant service degradation. While not yet critical, this level of failure can impact subscriber-related operations and may escalate if not addressed promptly. Possible causes include backend instability, partial outages, or increasing system load. **Diagnostic Information**: • Evaluate the following metric: • Failed SLA Responses / Total SLA Responses * 100 over a 5-minute window • Scope: • msgType = "SLA" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% and 90% • Perform the following checks: • Analyze response code distribution to identify dominant failure types. • Check for partial failures in backend systems (HSS/UDM, subscriber DB). • Review logs for intermittent errors, timeouts, or invalid responses. • Validate subscriber data availability and consistency. • Monitor system performance (CPU, memory, latency, thread utilization). • Inspect network connectivity and latency for SLA transactions. • Correlate with recent deployments or configuration changes. **Recovery**: • Investigate and stabilize backend systems handling subscriber data. • Resolve identified issues based on specific Diameter error codes. • Optimize or scale system resources to handle load. • Fix data inconsistencies or missing subscriber information. • Roll back recent changes if they correlate with the issue. • Apply retry or failover mechanisms if applicable. • Closely monitor to prevent escalation to the critical threshold • For any additional guidance, contact My Oracle Support.

8.1.1.56 SLA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-72 SLA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	SLA Sy fail count exceeds the minor threshold limit
Summary	Alert SLA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD > 60 <= 80
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.58

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-72 (Cont.) SLA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of failed SLA (Subscriber Location Answer / Service-Level related Answer) Diameter responses has exceeded the minor threshold (greater than 60% and up to 80%). The condition indicates an early stage of service degradation where a significant portion of SLA transactions are failing. While the system may still be functional, this condition signals potential underlying issues such as intermittent backend failures, rising load, or partial data/service unavailability. **Diagnostic Information**: • Evaluate the following metric: • Failed SLA Responses / Total SLA Responses * 100 over a 5-minute window • Scope: • msgType = "SLA" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% and 80% • Perform the following checks: • Observe trends to determine if failure rate is increasing toward major/critical levels • Analyze response code distribution for early error patterns. • Check connectivity and responsiveness of backend systems (HSS/UDM, subscriber DB). • Review logs for intermittent failures, retries, or timeout issues. • Validate subscriber data availability and consistency. • Monitor system performance (CPU, memory, latency, thread utilization). • Identify if failures are isolated to specific request types or scenarios. **Recovery**: • Investigate and address early signs of backend or data-related issues. • Validate and correct configurations or recent changes if applicable. • Optimize system performance or scale resources to handle increasing load. • Resolve identified issues based on Diameter error codes. • Apply preventive measures (retry tuning, connection stability improvements). • Continue close monitoring to prevent escalation to higher severity thresholds. • For any additional guidance, contact My Oracle Support.

8.1.1.57 STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-73 STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	STA Sy fail count exceeds the critical threshold limit.
Summary	Alert STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD >90
Severity	Critical
Expression	The failure rate of Sy STA responses is more than 90% of the total responses.
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 > 90

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-73 (Cont.) STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.59
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of failed STA (Session Termination Answer) Diameter responses for application ID 16777302 has exceeded the critical threshold (greater than 90%). The condition indicates that most session termination requests are failing, which can lead to improper session cleanup, resource leakage, and inconsistencies in subscriber/session state. Likely causes include backend failures, session state mismatches, or signaling issues with peer systems. **Diagnostic Information**: • Evaluate the following metric: • Failed STA Responses / Total STA Responses * 100 over a 5-minute window • Scope: • msgType = "STA" (Session Termination Answer) • appId = "16777302" (specific Diameter application, typically Gx) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 90% • Perform the following checks: • Analyze Diameter response codes (for example, unknown session, unable to comply, system errors). • Verify session state consistency between network elements (for example, PCRF/PCF and gateway). • Check connectivity and health of peer systems handling session termination. • Review logs for session cleanup failures, stale sessions, or timeout issues. • Monitor retransmissions, latency, and signaling errors. • Inspect system resource utilization (CPU, memory, session table capacity). • Correlate with spikes in session terminations (for example, mass disconnect events). **Recovery**: • Restore connectivity and stability with peer systems (for example, PCRF/PCF). • Resolve session state inconsistencies or stale session entries. • Address specific Diameter error codes causing STA failures. • Restart or scale affected components handling session termination. • Clean up orphaned or stuck sessions if required • Roll back recent changes impacting session handling. • Monitor until failure rate drops below the critical threshold. • For any additional guidance, contact My Oracle Support.

8.1.1.58 STA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-74 STA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	STA Sy fail count exceeds the major threshold limit.
Summary	Alert STA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD > 80 and <= 90
Severity	Major
Expression	The failure rate of Sy STA responses is more than 80% and less and or equal to 90% of the total responses.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-74 (Cont.) STA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.59
Metric Used	occnp_diam_response_local_total
Recommended Actions	**Cause**: The percentage of failed STA (Session Termination Answer) Diameter responses for application ID 16777302 has exceeded the major threshold (greater than 80% and up to 90%). The condition indicates a high rate of session termination failures, which can lead to incomplete session cleanup, inconsistent session states, and potential resource buildup. The issue suggests partial service degradation, possibly due to backend instability, signaling issues, or increased load. **Diagnostic Information**: • Evaluate the following metric: • Failed STA Responses / Total STA Responses * 100 over a 5-minute window • Scope: • msgType = "STA" • appId = "16777302" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% and 90% • Perform the following checks: • Analyze response code distribution (for example, unknown session, unable to comply, system errors). • Verify session state synchronization between network elements (for example, PCRF/PCF and gateway). • Check connectivity and health of peer systems handling session termination. • Review logs for intermittent session cleanup failures or timeout issues. • Monitor signaling performance (latency, retransmissions). • Inspect system resource usage (CPU, memory, session table capacity). • Correlate with spikes in session termination requests (for example, bulk disconnect events). **Recovery**: • Investigate and stabilize communication with peer systems. • Resolve session state inconsistencies or stale session entries. • Address specific Diameter error codes contributing to failures. • Optimize or scale system resources to handle load. • Restart affected components if necessary. • Roll back recent configuration or deployment changes if correlated. • Closely monitor to prevent escalation to the critical threshold • For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.59 STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-75 STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	STA Sy fail count exceeds the minor threshold limit.
Summary	Alert STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD > 60 and <= 80
Severity	Minor
Expression	The failure rate of Sy STA responses is more than 60% and less and or equal to 80% of the total responses.
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.59
Metric Used	occnp_diam_response_local_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-75 (Cont.) STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: The percentage of failed STA (Session Termination Answer) Diameter responses for application ID 16777302 has exceeded the minor threshold (greater than 60% and up to 80%). The condition indicates an early stage of degradation in session termination handling. While the system may still be operational, a significant portion of session termination requests are failing, potentially leading to delayed cleanup, partial session inconsistencies, or buildup of stale sessions. **Diagnostic Information**: • Evaluate the following metric: • Failed STA Responses / Total STA Responses * 100 over a 5-minute window • Scope: • msgType = "STA" • appId = "16777302" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% and 80% • Perform the following checks: • Observe trends to determine if failure rate is increasing toward major/critical levels • Analyze response codes for early indicators (for example, unknown session, temporary failures). • Verify session state consistency between network elements. • Check connectivity and responsiveness of peer systems (for example, PCRF/PCF). • Review logs for intermittent session termination or cleanup issues. • Monitor system performance (CPU, memory, session table usage). • Identify if failures are linked to specific traffic patterns or events. **Recovery**: • Investigate and address early signs of session handling or backend issues. • Validate session state synchronization across systems. • Resolve identified issues based on Diameter error codes. • Optimize or scale system resources to handle load. • Apply preventive measures (for example, retry tuning, session cleanup mechanisms). • Review and correct recent configuration or deployment changes if applicable. • Continue close monitoring to prevent escalation to higher severity thresholds. • For any additional guidance, contact My Oracle Support.

8.1.1.60 STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-76 STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	The failure rate of Rx STA responses is more than 90% of the total responses.
Summary	Alert STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD >90
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 > 90

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-76 (Cont.) STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.64
Metric Used	occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}
Recommended Actions	**Cause**: The percentage of failed STA (Session Termination Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the critical threshold (greater than 90%). The condition indicates that most session termination operations on the Rx interface are failing, which can lead to improper session cleanup, policy inconsistencies, and potential resource leakage. Likely causes include failures in communication with AF (Application Function), signaling issues, or backend instability. **Diagnostic Information**: • Evaluate the following metric: • Failed STA (Rx) Responses / Total STA (Rx) Responses * 100 over a 5-minute window • Scope: • msgType = "STA" • appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 90% • Perform the following checks: • Analyze Diameter response codes (for example, unknown session, authorization failures, unable to comply). • Verify connectivity and health of AF (Application Function) or related Rx peers. • Check session state consistency between PCRF/PCF and AF. • Review logs for session termination failures, timeouts, or invalid requests. • Monitor signaling metrics (latency, retransmissions, error rates). • Inspect system resource utilization (CPU, memory, session tables). • Correlate with spikes in Rx signaling or session termination events. **Recovery**: • Restore connectivity and stability with AF or Rx peer systems. • Resolve session state inconsistencies or stale sessions. • Address specific Diameter error codes causing failures. • Restart or scale affected components handling Rx traffic. • Clean up orphaned or stuck sessions if required • Roll back recent configuration or deployment changes if correlated. • Monitor until failure rate drops below the critical threshold.

8.1.1.61 STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-77 STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	The failure rate of Rx STA responses is more than 80% and less and or equal to 90% of the total responses.
Summary	Alert STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD > 80 and <= 90
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-77 (Cont.) STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.64
Metric Used	occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}
Recommended Actions	**Cause**: The percentage of failed STA (Session Termination Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the major threshold (greater than 80% and up to 90%). The condition indicates a high failure rate in session termination over the Rx interface, leading to partial service degradation. It may result in delayed or incomplete session cleanup, inconsistent policy enforcement, and increased resource utilization. The issue is likely due to instability in communication with the Application Function (AF), backend issues, or increased signaling load. **Diagnostic Information**: • Evaluate the following metric: • Failed STA (Rx) Responses / Total STA (Rx) Responses * 100 over a 5-minute window • Scope: • msgType = "STA" • appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% and 90% • Perform the following checks: • Analyze response code distribution (for example, unknown session, temporary failures, system errors). • Verify connectivity and health of AF (Application Function) peers. • Check session state synchronization between PCRF/PCF and AF. • Review logs for intermittent failures, timeouts, or malformed requests. • Monitor signaling performance (latency, retransmissions, error trends). • Inspect system resource usage (CPU, memory, session tables). • Correlate with spikes in Rx traffic or session termination events. **Recovery**: • Investigate and stabilize connectivity with AF/Rx peer systems. • Resolve session state inconsistencies or stale session entries. • Address identified Diameter error codes contributing to failures. • Optimize or scale system resources to handle load. • Restart affected components if necessary. • Roll back recent configuration or deployment changes if correlated. • Closely monitor to prevent escalation to the critical threshold

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.62 STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-78 STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	The failure rate of Rx STA responses is more than 60% and less and or equal to 80% of the total responses.
Summary	STA Rx fail count exceeds the minor threshold limit.
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.64
Metric Used	occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-78 (Cont.) STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: The percentage of failed STA (Session Termination Answer) Diameter responses for application ID 16777236 (Rx interface) has exceeded the minor threshold (greater than 60% and up to 80%). The condition indicates an early stage of degradation in handling session termination over the Rx interface. While the system may still be functioning, a notable portion of session terminations are failing, which can lead to delayed cleanup, partial session inconsistencies, and potential buildup of stale sessions. **Diagnostic Information**: • Evaluate the following metric: • Failed STA (Rx) Responses / Total STA (Rx) Responses * 100 over a 5-minute window • Scope: • msgType = "STA" • appId = "16777236" (Rx interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% and 80% • Perform the following checks: • Observe trends to see if failure rate is increasing toward major/critical levels • Analyze response codes for early indicators (for example, unknown session, temporary/system errors). • Verify connectivity and responsiveness of AF (Application Function) peers. • Check session state synchronization between PCRF/PCF and AF. • Review logs for intermittent failures, retries, or timeout issues. • Monitor system performance (CPU, memory, session table utilization). • Identify if failures correlate with specific traffic patterns or events. **Recovery**: • Investigate and address early signs of issues in Rx signaling or AF connectivity. • Validate session state consistency across involved systems. • Resolve identified issues based on Diameter error codes. • Optimize or scale system resources to handle load. • Apply preventive measures (retry tuning, improved session cleanup mechanisms). • Review and correct recent configuration or deployment changes if applicable. • Continue close monitoring to prevent escalation to higher severity thresholds.

8.1.1.63 SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-79 SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	The failure rate of Sy SNA responses is more than 90% of the total responses.
Summary	Alert SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD > 90
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.65

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-79 (Cont.) SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Metric Used	occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}
Recommended Actions	**Cause**: The percentage of failed SNA (Subscriber Notification Answer) Diameter responses has exceeded the critical threshold (greater than 90%). The condition indicates a severe failure in handling subscriber notification responses, which may impact event notifications, policy updates, or subscriber state synchronization. The issue is likely due to backend system failures, signaling issues, or data inconsistencies. **Diagnostic Information**: • Evaluate the following metric: • Failed SNA Responses / Total SNA Responses * 100 over a 5-minute window • Scope: • msgType = "SNA" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 90% • Perform the following checks: • Analyze Diameter response codes (for example, user unknown, unable to comply, system errors). • Verify connectivity and health of backend systems (for example, HSS/UDM, notification handlers). • Check logs for notification delivery failures, timeouts, or processing errors. • Validate subscriber data availability and correctness. • Monitor signaling performance (latency, retransmissions, error spikes). • Inspect system resources (CPU, memory, thread pools). • Correlate with spikes in notification events or subscriber activity. **Recovery**: • Restore connectivity and stability with backend/subscriber systems. • Resolve data inconsistencies or missing subscriber information. • Address specific Diameter error codes causing failures. • Restart or scale affected components handling notification traffic. • Roll back recent configuration or deployment changes if correlated. • Tune timeout and retry mechanisms if applicable • Monitor until failure rate drops below the critical threshold. • For any additional guidance, contact My Oracle Support.

8.1.1.64 SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-80 SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	The failure rate of Sy SNA responses is more than 80% and less and or equal to 90% of the total responses.
Summary	Alert SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD > 80 and <= 90
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-80 (Cont.) SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.65
Metric Used	occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}
Recommended Actions	**Cause**: The percentage of failed SNA (Subscriber Notification Answer) Diameter responses has exceeded the major threshold (greater than 80% and up to 90%). The condition indicates a high rate of failures in subscriber notification handling, leading to partial service degradation. It may impact timely delivery of notifications, subscriber state synchronization, and policy updates. The issue could stem from backend instability, signaling issues, or increased system load. **Diagnostic Information**: • Evaluate the following metric: • Failed SNA Responses / Total SNA Responses * 100 over a 5-minute window • Scope: • msgType = "SNA" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% and 90% • Perform the following checks: • Analyze response code distribution to identify dominant failure types. • Verify connectivity and health of backend systems (for example, HSS/UDM, notification handlers). • Check logs for intermittent notification failures, timeouts, or processing errors. • Validate subscriber data availability and correctness. • Monitor signaling performance (latency, retransmissions, error trends). • Inspect system resource usage (CPU, memory, thread pools). • Correlate with spikes in notification events or subscriber activity. **Recovery**: • Investigate and stabilize backend systems handling notifications. • Resolve issues based on specific Diameter error codes. • Optimize or scale system resources to handle load. • Fix data inconsistencies or missing subscriber information. • Restart affected components if necessary. • Roll back recent configuration or deployment changes if correlated. • Closely monitor to prevent escalation to the critical threshold • For any additional guidance, contact My Oracle Support.

8.1.1.65 SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-81 SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	The failure rate of Sy STA responses is more than 60% and less and or equal to 80% of the total responses.
Summary	Alert SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD > 60 <= 80

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-81 (Cont.) SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.65
Metric Used	occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}
Recommended Actions	**Cause**: The percentage of failed SNA (Subscriber Notification Answer) Diameter responses has exceeded the minor threshold (greater than 60% and up to 80%). The condition indicates an early stage of degradation in subscriber notification handling. While the system may still be operational, a noticeable portion of notification responses are failing, potentially affecting timely updates to subscriber state and policy enforcement. **Diagnostic Information**: • Evaluate the following metric: • Failed SNA Responses / Total SNA Responses * 100 over a 5-minute window • Scope: • msgType = "SNA" • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% and 80% • Perform the following checks: • Observe trends to determine if failure rate is increasing toward major/critical levels • Analyze response code distribution for early failure patterns. • Verify connectivity and responsiveness of backend systems (for example, HSS/UDM, notification handlers). • Review logs for intermittent errors, retries, or timeout issues. • Validate subscriber data availability and correctness. • Monitor system performance (CPU, memory, thread pools, latency). • Identify if failures are linked to specific traffic spikes or events. **Recovery**: • Investigate and address early signs of backend or signaling issues. • Validate and correct configurations or recent changes. • Optimize or scale system resources to handle load. • Resolve issues based on observed Diameter error codes. • Apply preventive measures (retry tuning, connection stability improvements). • Continue close monitoring to prevent escalation to higher severity thresholds. • For any additional guidance, contact My Oracle Support.

8.1.1.66 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

Table 8-82 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

Field	Details
Description	Certificate expiry in less than 6 months.
Summary	Certificate expiry in less than 6 months.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-82 (Cont.) DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

Field	Details
Severity	Minor
Expression	dgw_tls_cert_expiration_seconds - time() <= 15724800
OID	1.3.6.1.4.1.323.5.3.52.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds
Recommended Actions	**Cause**: Diameter Gateway TLS certificate approaching expiry; risk of future connection failures if not rotated. **Diagnostic Information**: • Identify which cert/instance is expiring (labels on metric, if present). • `min by (instance,cert_subject,cert_name) (dgw_tls_cert_expiration_seconds - time()) (adjust labels to your environment)` **Recovery**: • Start certificate renewal process: create/approve new cert, validate chain/SANs, and schedule rotation before major window. Confirm DGW can load the new cert in staging/non-prod first.

8.1.1.67 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR

Table 8-83 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR

Field	Details
Description	Certificate expiry in less than 3 months.
Summary	Certificate expiry in less than 3 months.
Severity	Major
Expression	dgw_tls_cert_expiration_seconds - time() <= 7862400
OID	1.3.6.1.4.1.323.5.3.52.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-83 (Cont.) DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR

Field	Details
Recommended Actions	**Cause**: Diameter Gateway TLS certificate approaching expiry; risk of future connection failures if not rotated. **Diagnostic Information**: • Identify which cert/instance is expiring (labels on metric, if present). • `min by (instance,cert_subject,cert_name) (dgw_tls_cert_expiration_seconds - time()) (adjust labels to your environment)` • Confirm the dependent peers trust the issuing CA and that intermediate certificate are correct. **Recovery**: • Execute rotation plan: deploy new cert + key via approved secret management, reload/ restart DGW as per runbook, and verify successful TLS handshakes with peers.

8.1.1.68 DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

Table 8-84 DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

Field	Details
Description	Certificate expiry in less than 1 month.
Summary	Certificate expiry in less than 1 month.
Severity	Critical
Expression	dgw_tls_cert_expiration_seconds - time() <= 2592000
OID	1.3.6.1.4.1.323.5.3.52.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-84 (Cont.) DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

Field	Details
Recommended Actions	**Cause**: Imminent expiry; high risk of production outage when cert expires. **Diagnostic Information**: • Identify which cert/instance is expiring (labels on metric, if present). • `min by (instance,cert_subject,cert_name) (dgw_tls_cert_expiration_seconds - time()) (adjust labels to your environment)` • Confirm the dependent peers trust the issuing CA and that intermediate certificate are correct. • Verify exact expiry timestamp and whether multiple instances are impacted. **Recovery**: • Expedite renewal/rotation immediately. After deployment, validate with: • Peer connection stability (no TLS alerts/ handshake failures) • DGW logs show new cert loaded • Metric resets to a larger time-to-expiry.

8.1.1.69 DGW_TLS_CONNECTION_FAILURE

Table 8-85 DGW_TLS_CONNECTION_FAILURE

Field	Details
Description	Alert for TLS connection establishment.
Summary	TLS Connection failure when Diam gateway is an initiator.
Severity	Major
Expression	sum by (namespace,reason) (occnp_diam_failed_conn_network) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.81
Metric Used	occnp_diam_failed_conn_network

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-85 (Cont.) DGW_TLS_CONNECTION_FAILURE

Field	Details
Recommended Actions	**Cause**: Diameter Gateway (DGW) is failing to establish TLS connections as a client due to handshake exceptions. Common causes: expired/rotated certs, missing intermediate chain, truststore mismatch/unknown CA, SAN/CN mismatch, TLS policy/cipher mismatch, clock skew, or network middlebox interference. **Diagnostic Information**: • Identify the reason breakdown and where it occurs. • `sum by(namespace,reason) (occnp_diam_failed_conn_network)` • If labels exist for peer/endpoint, isolate the target • Example: sum by(namespace,reason,destHost,destRealm) (`occnp_diam_failed_conn_network`) • Correlate with cert-expiry alerts and validate time sync (NTP) on DGW nodes. • Check DGW logs around handshake failures to confirm: unknown_ca, bad_certificate, certificate_expired, handshake_failure, protocol_version, etc. **Recovery**: • If cert/trust issue: renew/rotate DGW client cert or update truststores/CA bundles (include intermediates), then reload/restart DGW per runbook. • If TLS policy mismatch: align TLS versions/ciphers on both sides according to approved security standards. • If endpoint-specific: remediate the server cert/config or failover to an alternate server/peer. • Validate: handshake failures stop increasing and DGW peer connections remain established.

8.1.1.70 POLICY_CONNECTION_FAILURE

Table 8-86 POLICY_CONNECTION_FAILURE

Field	Details
Description	Connection failure on Egress and Ingress Gateways for incoming and outgoing connections.
Summary	Connection failure on Egress and Ingress Gateways for incoming and outgoing connections.
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-86 (Cont.) POLICY_CONNECTION_FAILURE

Field	Details
Expression	sum(increase(occnp_oc_ingressgateway_connection_failure_total[5m]) >0 or (occnp_oc_ingressgateway_connection_failure_total unless occnp_oc_ingressgateway_connection_failure_total offset 5m)) by (namespace,app, error_reason) > 0 or sum(increase(occnp_oc_egressgateway_connection_failure_total[5m]) >0 or (occnp_oc_egressgateway_connection_failure_total unless occnp_oc_egressgateway_connection_failure_total offset 5m)) by (namespace,app, error_reason) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.76
Metric Used	occnp_oc_ingressgateway_connection_failure_total
Recommended Actions	**Cause**: Gateway is experiencing incoming/ outgoing connection failures, typically due to: downstream endpoint down, DNS issues, TLS handshake failures, network ACL/firewall changes, certificate/CA problems, or resource exhaustion causing connect timeouts/refusals. **Diagnostic Information**: • Break down failures by gateway and reason: – - Ingress: sum by (namespace,app,error_reason) (increase(occnp_oc_ingressgateway_connection_failure_total[5m])) – - Egress: sum by (namespace,app,error_reason) (increase(occnp_oc_egressgateway_connection_failure_total[5m])) • Identify affected destination(s) if labeled (e.g., host/cluster/route). • Correlate with cert expiry alerts, DNS metrics, and network error logs. **Recovery**: • If TLS/cert-related (error_reason indicates handshake/unknown CA): rotate/fix cert chain and truststores; confirm mTLS policies. • If network/DNS: restore name resolution, routes, firewall rules, service endpoints; validate connectivity from gateway pods. • If downstream outage/overload: restore downstream service or failover; consider backoff/rate limit to reduce retry storms. • Validate recovery by observing failure increases return to ~0 and connections stabilize.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.71 AUDIT_NOT_RUNNING

Table 8-87 AUDIT_NOT_RUNNING

Field	Details
Description	Audit has not been running for at least 1 hour.
Summary	Audit has not been running for at least 1 hour.
Severity	CRITICAL
Expression	(increase(data_repository_invocations_seconds_count{method="getQueuedTablesToAudit",state="SUCCESS"}[1h])) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.78
Metric Used	data_repository_invocations_seconds_count
Recommended Actions	**Cause**: No successful executions of getQueuedTablesToAudit have been recorded for at least 1 hour (increase(...[1h]) == 0). This condition indicates the audit job in the application is not running, is stuck, or is failing before it records a SUCCESS. **Diagnostic Information**: • Check in Prometheus/Grafana: • Graph data_repository_invocations_seconds_count{method="getQueuedTablesToAudit"} by state to see if attempts are happening but failing (for example, ERROR/FAILURE) vs not happening at all. • Confirm the metric series exists for the pod; if missing, verify Prometheus scrape health/target status for that pod. • Check pod health and logs around the last hour: • Recent restarts/OOMKills, readiness and liveness failures. • Application logs for audit scheduler/worker thread issues, DB connectivity, timeouts, deadlocks, or queue starvation. **Recovery**: • If the pod is unhealthy or the audit worker is stuck: restart/roll the pod (following your team's change/restart procedures). • If failures are present (non-success states): remediate the underlying error (for example, restore DB connectivity, fix credentials, address timeouts/locks, clear blocking conditions), then verify SUCCESS invocations resume. • If metrics are missing but the service is healthy: fix scraping/metrics emission (Prometheus target, service monitor, endpoint auth), then confirm the counter is increasing. • Validate recovery by confirming the metric increases over a short window (for example, increase(...[5m]) > 0) and the audit backlog/health indicators return to normal.

8.1.1.72 DIAMETER_POD_ERROR_RESPONSE_MINOR

Table 8-88 DIAMETER_POD_ERROR_RESPONSE_MINOR

Field	Details
Description	At least 1% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Summary	At least 1% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Severity	MINOR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-88 (Cont.) DIAMETER_POD_ERROR_RESPONSE_MINOR

Field	Details
Expression	(sum by (pod) (rate(occnp_diam_response_network_total{responseCode="3002"}[2m])))/ (sum by (pod) (rate(occnp_diam_response_network_total[2m]))) * 100 >=1
OID	1.3.6.1.4.1.323.5.3.52.1.2.79
Metric Used	ocbsf_diam_response_network_total
Recommended Actions	**Cause**: At least one pod is returning/observing an elevated rate of Diameter result code 3002 (DIAMETER_UNABLE_TO_DELIVER). Typically indicates routing/peer selection problems, destination realm/host not reachable, peer connection down, invalid/missing route, or transient network issues. Can also occur during rolling restarts when peer tables/routes are not stable. **Diagnostic Information**: • Identify the worst pod (the alert is already topk(1); list all pods). • % by pod: ((sum by(pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) / sum by(pod)(rate(ocbsf_diam_response_network_total[2m]))) * 100) • Confirm whether it's a volume issue vs ratio artifact. • Total by pod: sum by(pod)(rate(ocbsf_diam_response_network_total[2m])) • 3002 by pod: sum by(pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) • Break down by any available routing labels (commonly destHost, destRealm, peer, appId, msgType—use what exists in your metric) • Example: sum by(pod,destRealm,destHost) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) • Correlate with peer connection state / disconnects (Diameter stack metrics/logs) and recent deploy/restart events for the affected pod. **Recovery**: • If isolated to one pod: drain/replace the pod (after confirming no broader peer outage) and validate routing tables/peer connections on the new instance. • If isolated to a destination realm/host: fix routing configuration, realm definitions, and peer reachability; restore the peer connection. • If caused by peer downtime: failover/reroute traffic to alternate peers where supported. • Validate: 3002 rate returns to baseline and success (2xxx) responses dominate.

8.1.1.73 DIAMETER_POD_ERROR_RESPONSE_MAJOR

Table 8-89 DIAMETER_POD_ERROR_RESPONSE_MAJOR

Field	Details
Description	At least 5% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Summary	At least 5% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Severity	MAJOR
Expression	(sum by (pod) (rate(occnp_diam_response_network_total{responseCode="3002"}[2m])))/ (sum by (pod) (rate(occnp_diam_response_network_total[2m]))) * 100 >=5
OID	1.3.6.1.4.1.323.5.3.52.1.2.79
Metric Used	ocbsf_diam_response_network_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-89 (Cont.) DIAMETER_POD_ERROR_RESPONSE_MAJOR

Field	Details
Recommended Actions	**Cause**: At least one pod is returning/observing an elevated rate of Diameter result code 3002 (DIAMETER_UNABLE_TO_DELIVER). Typically indicates routing/peer selection problems, destination realm/host not reachable, peer connection down, invalid/missing route, or transient network issues. Can also occur during rolling restarts when peer tables/routes are not stable. Indicates significant delivery failures likely impacting sessions/transactions. **Diagnostic Information**: • Identify the worst pod (the alert is already topk(1); list all pods) - % by pod: ((sum by(pod)(rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) / sum by(pod)(rate(ocbsf_diam_response_network_total[2m]))) * 100) • Confirm whether multiple pods are impacted: – `count( ((sum by(pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) / sum by(pod) (rate(ocbsf_diam_response_network_total[2m]))) * 100) >= 5 )` • Confirm whether it's a volume issue vs ratio artifact. • Total by pod: sum by(pod)(rate(ocbsf_diam_response_network_total[2m])) • 3002 by pod: sum by(pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) • Break down by any available routing labels (commonly destHost, destRealm, peer, appId, msgType—use what exists in your metric) • Example: sum by(pod,destRealm,destHost) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) • Correlate with peer connection state / disconnects (Diameter stack metrics/logs) and recent deploy/restart events for the affected pod. • Same as MINOR, plus confirm whether multiple pods are impacted: • `count( ((sum by(pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) / sum by(pod) (rate(ocbsf_diam_response_network_total[2m]))) * 100) >= 5 )` **Recovery**: • Prioritize restoring reachability/routing: failover peers, fix realm/route config, and mitigate pod-level issues (restart/replace) if localized. Treat as incident if sustained.

8.1.1.74 DIAMETER_POD_ERROR_RESPONSE_CRITICAL

Table 8-90 DIAMETER_POD_ERROR_RESPONSE_CRITICAL

Field	Details
Description	At least 10% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER
Summary	At least 10% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER
Severity	CRITICAL
Expression	(sum by (pod) (rate(occnp_diam_response_network_total{responseCode="3002"}[2m])))/ (sum by (pod) (rate(occnp_diam_response_network_total[2m]))) * 100 >=10
OID	1.3.6.1.4.1.323.5.3.52.1.2.79
Metric Used	occnp_diam_response_network_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-90 (Cont.) DIAMETER_POD_ERROR_RESPONSE_CRITICAL

Field	Details
Recommended Actions	**Cause**: Severe unable-to-deliver condition. Typically indicates major peer/routing outage, widespread disconnects, or a bad configuration rollout. **Diagnostic Information**: • Identify the worst pod (the alert is already topk(1); list all pods) - % by pod: ((sum by(pod)(rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) / sum by(pod)(rate(ocbsf_diam_response_network_total[2m]))) * 100) • Confirm whether multiple pods are impacted: – `count( ((sum by(pod) (rate(ocbsf_diam_response_network_total{responseCode="3002" }[2m])) / sum by(pod) (rate(ocbsf_diam_response_network_total[2m]))) * 100) >= 5 )` • Confirm whether it's a volume issue vs ratio artifact. • Total by pod: sum by(pod)(rate(ocbsf_diam_response_network_total[2m])) • 3002 by pod: sum by(pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) • Break down by any available routing labels (commonly destHost, destRealm, peer, appId, msgType—use what exists in your metric) • Example: sum by(pod,destRealm,destHost) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])) • Correlate with peer connection state / disconnects (Diameter stack metrics/logs) and recent deploy/restart events for the affected pod. • identify dominant destination(s) and whether this correlates with connection failures / peer-down alarms. **Recovery**: • Immediately restore routing/peer connectivity or Roll back recent routing/ configuration changes. • Fail traffic over to healthy peers/realms. • Replace unhealthy pods if issue is pod-local. • Validate stabilization: 3002 drops well below 10% and end-to-end transaction success recovers.

8.1.1.75 CERTIFICATE_EXPIRY_MINOR

Table 8-91 CERTIFICATE_EXPIRY_MINOR

Field	Details
Description	Certificate expiry in less than 6 months
Summary	Certificate expiry in less than 6 months
Severity	MINOR
Expression	security_cert_x509_expiration_seconds - time() <= 15724800
OID	1.3.6.1.4.1.323.5.3.52.1.2.77
Metric Used	security_cert_x509_expiration_seconds

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-91 (Cont.) CERTIFICATE_EXPIRY_MINOR

Field	Details
Recommended Actions	**Cause**: Some certificate monitored by the security exporter is approaching expiry. **Diagnostic Information**: • Find the minimum time-to-expiry and impacted certs (labels vary) • `min by (namespace,secret,cert_subject) (security_cert_x509_expiration_seconds - time())` **Recovery**: • Plan renewal/rotation via the approved cert/PKI process; update Kubernetes secrets or keystores; schedule rollout before MAJOR window; verify post-rotation metric increases.

8.1.1.76 CERTIFICATE_EXPIRY_MAJOR

Table 8-92 CERTIFICATE_EXPIRY_MAJOR

Field	Details
Description	Certificate expiry in less than 3 months
Summary	Certificate expiry in less than 3 months
Severity	MAJOR
Expression	security_cert_x509_expiration_seconds - time() <= 7862400
OID	1.3.6.1.4.1.323.5.3.52.1.2.77
Metric Used	security_cert_x509_expiration_seconds
Recommended Actions	**Cause**: Same as above with higher urgency. **Diagnostic Information**: • Find the minimum time-to-expiry and impacted certs (labels vary) • `min by (namespace,secret,cert_subject) (security_cert_x509_expiration_seconds - time())` • Ensure which workload(s) consume the cert (ingress, egress, internal service, database, etc.). **Recovery**: • Rotate certificate and confirm dependent clients trust the new chain. Consider staged rollout to avoid widespread handshake failures.

8.1.1.77 CERTIFICATE_EXPIRY_CRITICAL

Table 8-93 CERTIFICATE_EXPIRY_CRITICAL

Field	Details
Description	Certificate expiry in less than 1 months
Summary	Certificate expiry in less than 1 months
Severity	CRITICAL
Expression	security_cert_x509_expiration_seconds - time() <= 2592000
OID	1.3.6.1.4.1.323.5.3.52.1.2.77
Metric Used	security_cert_x509_expiration_seconds

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-93 (Cont.) CERTIFICATE_EXPIRY_CRITICAL

Field	Details
Recommended Actions	**Cause**: Imminent expiry; high likelihood of service disruption at expiry. **Diagnostic Information**: • Find the minimum time-to-expiry and impacted certs (labels vary) • `min by (namespace,secret,cert_subject) (security_cert_x509_expiration_seconds - time())` • Ensure which workload(s) consume the cert (ingress, egress, internal service, database, etc.). • Validate exact expiry and blast radius (which services/peers rely on it). **Recovery**: • Emergency rotation: Renew cert, deploy via approved secrets process, reload/restart impacted workloads per runbook, validate: successful TLS handshakes, no connection-failure alerts, and expiration metric resets.

8.1.1.78 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MINOR

Table 8-94 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Description	More than 10% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 10% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MINOR
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m])))/(sum by (namespace) (rate(occnp_userservice_inbound_count_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.85
Metric Used	occnp_late_processing_rejection_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-94 (Cont.) UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Recommended Actions	**Cause**: UDR-connector is rejecting a notable share of requests because they are stale on arrival or become stale during processing. Typical causes: request queueing/ backlog, downstream UDR slowness/timeouts, connector CPU saturation, threadpool exhaustion, GC pauses, network latency, or burst traffic causing requests to miss SLA/TTL. **Diagnostic Information**: • Split “late arrival” vs “late processing” to locate the bottleneck • - Late arrival: sum by(namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m])) • - Late processing: sum by(namespace) (rate(occnp_late_processing_rejection_total{mode="UDR-C"}[5m])) • Check inbound traffic rate and burstiness • - sum by(namespace) (rate(ocpm_userservice_inbound_count_total{service_resource="udr-service"} [5m])) • Correlate with connector/pod congestion signals (CPU/queue) if available • - occnp_pod_resource_congestion_state{type="cpu"} / {type="queue"} • Check downstream UDR latency/errors (UDR service metrics/logs) and network latency to UDR. **Recovery**: • If “late arrival” dominant: reduce upstream burstiness (rate limiting/backpressure), scale ingress/connector, and investigate network path delays. • If “late processing” dominant: scale out connector, increase resources, tune threadpools, and fix hotspots; restore downstream UDR performance. • Validate: stale rejection % drops below 10% and end-to-end latency normalizes.

8.1.1.79 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Table 8-95 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Description	More than 20% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 20% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MAJOR
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="UDR-C"} [5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m])))/(sum by (namespace) (rate(occnp_userservice_inbound_count_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m]))) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.85
Metric Used	occnp_late_processing_rejection_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-95 (Cont.) UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Recommended Actions	**Cause**: Same as MINOR but indicates material service degradation; often sustained backlog or downstream impairment. **Diagnostic Information**: • Same diagnostics, with urgency: confirm whether this is isolated to a namespace/ cluster and whether it aligns with CPU/queue congestion and UDR latency spikes. **Recovery**: • Immediate mitigation: scale out UDR-connector and/or apply temporary rate limits to protect the system. • Restore UDR/downstream dependency health. • Validate rejection % < 20% quickly, then drive to baseline.

8.1.1.80 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Table 8-96 UDR_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	More than 30% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 30% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	CRITICAL
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m])))/(sum by (namespace) (rate(occnp_userservice_inbound_count_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.85
Metric Used	occnp_late_processing_rejection_total
Recommended Actions	**Cause**: Severe backlog/latency condition; many requests miss TTL/SLA. Likely causes: UDR outage/slowness, connector saturation, or systemic platform/network issue. **Diagnostic Information**: • Same as above, plus check for cascading failures: retries, connection failures, pod restarts/OOM, and saturation across multiple services. **Recovery**: • Treat as incident: immediate traffic shaping/load shedding and rapid scale-out. • If downstream UDR is unhealthy, failover if available or restore service urgently. • Consider rollback of recent changes if correlated with onset. • Validate: stale rejection % < 30% then continue until stable baseline; confirm queues drain and latency normalizes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.81 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MINOR

Table 8-97 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Description	More than 10% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 10% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MINOR
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m])))/(sum by (namespace) (rate(occnp_userservice_inbound_count_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.86
Metric Used	occnp_late_processing_rejection_total
Recommended Actions	**Cause**: - CHF-C stale-request rejection ratio >10% over 5m. - Caused by requests arriving late or becoming late during processing. - Common triggers: tight caller timeout budget, high CHF/UDR/backend latency, or pod backlog/overload. **Diagnostic Information**: • Metrics involved: `occnp_late_processing_rejection_total{mode="CHF-C"}`, `occnp_late_arrival_rejection_total{mode="CHF-C"}`, `ocpm_userservice_inbound_count_total{service_resource="chf-service"}`. • - Error observed: `504 Gateway Timeout`, cause `TIMED_OUT_REQUEST`, internal `FAILURE_STALE_REQUEST_REJECT`. • Cause value: `((late_processing + late_arrival) / (chf_inbound + late_arrival)) * 100 > 10` over 5m by namespace. • Condition: CHF-C only; late-processing can be localized by `stage` (`PRE_PROCESS|PRE_UDR|POST_UDR|PRE_CHF|POST_CHF`) and `operation`. • Verification steps: confirm rejection counters rising; check 504/TIMED_OUT_REQUEST logs; break down late-processing by `stage`/`operation`; compare inbound vs rejects; inspect pod saturation and CHF/UDR latency; verify timeout headers/config. • Monitoring recommendations: monitor the ratio and raw counters, split by `stage`/`operation`, and correlate with pod health, backlog, downstream latency, and 504s. **Recovery**: • Restore CHF-C latency/backlog: scale pods, relieve load, and recover CHF/UDR dependencies. • Increase caller timeout/max-response-time if requests are expiring too early. • Verify recovery when rejection rates drop, 504/TIMED_OUT_REQUEST logs stop, and the ratio falls below 10%.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.82 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Table 8-98 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Description	More than 20% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 20% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MAJOR
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m])))/(sum by (namespace) (rate(occnp_userservice_inbound_count_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m]))) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.86
Metric Used	occnp_late_processing_rejection_total
Recommended Actions	**Cause**: - CHF-C stale-request rejection ratio >20% over 5m. - Caused by requests arriving late or becoming late during processing. - Common triggers: tight caller timeout budget, high CHF/UDR/backend latency, or pod backlog/overload. **Diagnostic Information**: • Metrics involved: `occnp_late_processing_rejection_total{mode="CHF-C"}`, `occnp_late_arrival_rejection_total{mode="CHF-C"}`, `ocpm_userservice_inbound_count_total{service_resource="chf-service"}`. • - Error observed: `504 Gateway Timeout`, cause `TIMED_OUT_REQUEST`, internal `FAILURE_STALE_REQUEST_REJECT`. • Cause value: `((late_processing + late_arrival) / (chf_inbound + late_arrival)) * 100 > 10` over 5m by namespace. • Condition: CHF-C only; late-processing can be localized by `stage` (`PRE_PROCESS|PRE_UDR|POST_UDR|PRE_CHF|POST_CHF`) and `operation`. • Verification steps: confirm rejection counters rising; check 504/TIMED_OUT_REQUEST logs; break down late-processing by `stage`/`operation`; compare inbound vs rejects; inspect pod saturation and CHF/UDR latency; verify timeout headers/config. • Monitoring recommendations: monitor the ratio and raw counters, split by `stage`/`operation`, and correlate with pod health, backlog, downstream latency, and 504s. **Recovery**: • Restore CHF-C latency/backlog: scale pods, relieve load, and recover CHF/UDR dependencies. • Increase caller timeout/max-response-time if requests are expiring too early. • Verify recovery when rejection rates drop, 504/TIMED_OUT_REQUEST logs stop, and the ratio falls below 10%.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.83 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Table 8-99 CHF_CONNECTOR_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	More than 30% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 30% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	CRITICAL
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m])))/(sum by (namespace) (rate(occnp_userservice_inbound_count_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.86
Metric Used	occnp_late_processing_rejection_total
Recommended Actions	**Cause**: - CHF-C stale-request rejection ratio >30% over 5m. - Caused by requests arriving late or becoming late during processing. - Common triggers: tight caller timeout budget, high CHF/UDR/backend latency, or pod backlog/overload. **Diagnostic Information**: • Metrics involved: `occnp_late_processing_rejection_total{mode="CHF-C"}`, `occnp_late_arrival_rejection_total{mode="CHF-C"}`, `ocpm_userservice_inbound_count_total{service_resource="chf-service"}`. • - Error observed: `504 Gateway Timeout`, cause `TIMED_OUT_REQUEST`, internal `FAILURE_STALE_REQUEST_REJECT`. • Cause value: `((late_processing + late_arrival) / (chf_inbound + late_arrival)) * 100 > 10` over 5m by namespace. • Condition: CHF-C only; late-processing can be localized by `stage` (`PRE_PROCESS|PRE_UDR|POST_UDR|PRE_CHF|POST_CHF`) and `operation`. • Verification steps: confirm rejection counters rising; check 504/TIMED_OUT_REQUEST logs; break down late-processing by `stage`/`operation`; compare inbound vs rejects; inspect pod saturation and CHF/UDR latency; verify timeout headers/config. • Monitoring recommendations: monitor the ratio and raw counters, split by `stage`/`operation`, and correlate with pod health, backlog, downstream latency, and 504s. **Recovery**: • Restore CHF-C latency/backlog: scale pods, relieve load, and recover CHF/UDR dependencies. • Increase caller timeout/max-response-time if requests are expiring too early. • Verify recovery when rejection rates drop, 504/TIMED_OUT_REQUEST logs stop, and the ratio falls below 10%.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.84 STALE_BINDING_REQUEST_REJECTION_CRITICAL

Table 8-100 STALE_BINDING_REQUEST_REJECTION_CRITICAL

Field	Details
Description	This alert is triggered when more than 30 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	More than 30% of the Binding requests failed with error TIMED_OUT_REQUEST
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*binding"}[5m]))+ sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m])))/ (sum by (namespace) (rate(ocpm_binding_inbound_request_total{microservice=~".*binding"}[5m])))*100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.87
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_binding_inbound_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-100 (Cont.) STALE_BINDING_REQUEST_REJECTION_CRITICAL

Field	Details
Recommended Actions	**Cause**: Binding service is rejecting timed-out/stale requests. The alert fires when the 5-minute rate of `occnp_late_processing_rejection_total + occnp_late_arrival_rejection_total` reaches __>= 30%__ of `ocpm_binding_inbound_request_total` in a namespace. In code this occurs when late-arrival or late-processing protection is enabled and `TimeoutHelper.isRequestOnTime(httpHeaders)` returns false, typically meaning requests arrive already expired or become expired during processing (for example while waiting on BSF/DB/internal work). **Diagnostic Information**: • The following metrics are used: – `occnp_late_processing_rejection_total` – `occnp_late_arrival_rejection_total` – `ocpm_binding_inbound_request_total` • Error observed: – Binding rejects timed-out requests; code throws `ContextBindingTimedOutRequest` – Typical response path is `504 Gateway Timeout` • Cause value: – `cause="TIMED_OUT_REQUEST"` • Condition: – `((rate(occnp_late_processing_rejection_total) +rate(occnp_late_arrival_rejection_total))/ rate(ocpm_binding_inbound_request_total))*100 >= 10` over 5m by `namespace` • Verification steps: – Check rejection ratio and split by metric: late-arrival vs late-processing. – Break down by labels on rejection metrics: `cause`, `operationType`; for late-processing also `stage` – Confirm inbound traffic volume with `ocpm_binding_inbound_request_total`. – Check binding logs for `Timed out request` / `ContextBindingTimedOutRequest`. – Verify whether `lateArrival` / `lateProcessing` handling is enabled in config. – If late-processing dominates, inspect slow dependencies/processing around BSF and DB paths; `POST_BSF` stage is explicitly pegged in code • Monitoring recommendations: – Add dashboards for rejection ratio, absolute rejection rate, and split by `operationType` and `stage` – Correlate with `ocpm_binding_inbound_response_total` 5xx/504, HTTP latency metrics, DB latency, and BSF dependency errors/latency. – Alert separately on sustained late-arrival and late-processing so upstream timeout issues and internal slowness are distinguishable **Recovery**: • If late-arrival is high: investigate upstream callers/network delay and timeout/ header propagation; ensure requests are not reaching binding already expired. • If late-processing is high: reduce processing latency in binding and dependencies (especially BSF/DB), check pod saturation, latency spikes, thread starvation, and downstream timeout/error conditions. • Review recent config or traffic changes that enabled/shifted late request handling or increased request latency. • After mitigation, verify the rejection metrics fall and the ratio drops below 10% for the namespace.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.85 STALE_BINDING_REQUEST_REJECTION_MAJOR

Table 8-101 STALE_BINDING_REQUEST_REJECTION_MAJOR

Field	Details
Description	This alert is triggered when more than 20 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	More than 20% of the Binding requests failed with error TIMED_OUT_REQUEST
Severity	Major
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*binding"}[5m]))+ sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m])))/ (sum by (namespace) (rate(ocpm_binding_inbound_request_total{microservice=~".*binding"}[5m])))*100 >= 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.87
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_binding_inbound_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-101 (Cont.) STALE_BINDING_REQUEST_REJECTION_MAJOR

Field	Details
Recommended Actions	**Cause**: Binding service is rejecting timed-out/stale requests. The alert fires when the 5-minute rate of `occnp_late_processing_rejection_total + occnp_late_arrival_rejection_total` reaches __>= 20%__ of `ocpm_binding_inbound_request_total` in a namespace. In code this occurs when late-arrival or late-processing protection is enabled and `TimeoutHelper.isRequestOnTime(httpHeaders)` returns false, typically meaning requests arrive already expired or become expired during processing (for example while waiting on BSF/DB/internal work). **Diagnostic Information**: • The following metrics are used: – `occnp_late_processing_rejection_total` – `occnp_late_arrival_rejection_total` – `ocpm_binding_inbound_request_total` • Error observed: – Binding rejects timed-out requests; code throws `ContextBindingTimedOutRequest` – Typical response path is `504 Gateway Timeout` • Cause value: – `cause="TIMED_OUT_REQUEST"` • Condition: – `((rate(occnp_late_processing_rejection_total) +rate(occnp_late_arrival_rejection_total))/ rate(ocpm_binding_inbound_request_total))*100 >= 10` over 5m by `namespace` • Verification steps: – Check rejection ratio and split by metric: late-arrival vs late-processing. – Break down by labels on rejection metrics: `cause`, `operationType`; for late-processing also `stage` – Confirm inbound traffic volume with `ocpm_binding_inbound_request_total`. – Check binding logs for `Timed out request` / `ContextBindingTimedOutRequest`. – Verify whether `lateArrival` / `lateProcessing` handling is enabled in config. – If late-processing dominates, inspect slow dependencies/processing around BSF and DB paths; `POST_BSF` stage is explicitly pegged in code • Monitoring recommendations: – Add dashboards for rejection ratio, absolute rejection rate, and split by `operationType` and `stage` – Correlate with `ocpm_binding_inbound_response_total` 5xx/504, HTTP latency metrics, DB latency, and BSF dependency errors/latency. – Alert separately on sustained late-arrival and late-processing so upstream timeout issues and internal slowness are distinguishable **Recovery**: • If late-arrival is high: investigate upstream callers/network delay and timeout/ header propagation; ensure requests are not reaching binding already expired. • If late-processing is high: reduce processing latency in binding and dependencies (especially BSF/DB), check pod saturation, latency spikes, thread starvation, and downstream timeout/error conditions. • Review recent config or traffic changes that enabled/shifted late request handling or increased request latency. • After mitigation, verify the rejection metrics fall and the ratio drops below 10% for the namespace.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.86 STALE_BINDING_REQUEST_REJECTION_MINOR

Table 8-102 STALE_BINDING_REQUEST_REJECTION_MINOR

Field	Details
Description	This alert is triggered when more than 10 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	More than 10% of the Binding requests failed with error TIMED_OUT_REQUEST
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*binding"}[5m]))+ sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m])))/ (sum by (namespace) (rate(ocpm_binding_inbound_request_total{microservice=~".*binding"}[5m])))*100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.87
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_binding_inbound_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-102 (Cont.) STALE_BINDING_REQUEST_REJECTION_MINOR

Field	Details
Recommended Actions	**Cause**: Binding service is rejecting timed-out/stale requests. The alert fires when the 5-minute rate of `occnp_late_processing_rejection_total + occnp_late_arrival_rejection_total` reaches __>= 10%__ of `ocpm_binding_inbound_request_total` in a namespace. In code this occurs when late-arrival or late-processing protection is enabled and `TimeoutHelper.isRequestOnTime(httpHeaders)` returns false, typically meaning requests arrive already expired or become expired during processing (for example while waiting on BSF/DB/internal work). **Diagnostic Information**: • The following metrics are used: – `occnp_late_processing_rejection_total` – `occnp_late_arrival_rejection_total` – `ocpm_binding_inbound_request_total` • Error observed: – Binding rejects timed-out requests; code throws `ContextBindingTimedOutRequest` – Typical response path is `504 Gateway Timeout` • Cause value: – `cause="TIMED_OUT_REQUEST"` • Condition: – `((rate(occnp_late_processing_rejection_total) +rate(occnp_late_arrival_rejection_total))/ rate(ocpm_binding_inbound_request_total))*100 >= 10` over 5m by `namespace` • Verification steps: – Check rejection ratio and split by metric: late-arrival vs late-processing. – Break down by labels on rejection metrics: `cause`, `operationType`; for late-processing also `stage` – Confirm inbound traffic volume with `ocpm_binding_inbound_request_total`. – Check binding logs for `Timed out request` / `ContextBindingTimedOutRequest`. – Verify whether `lateArrival` / `lateProcessing` handling is enabled in config. – If late-processing dominates, inspect slow dependencies/processing around BSF and DB paths; `POST_BSF` stage is explicitly pegged in code • Monitoring recommendations: – Add dashboards for rejection ratio, absolute rejection rate, and split by `operationType` and `stage` – Correlate with `ocpm_binding_inbound_response_total` 5xx/504, HTTP latency metrics, DB latency, and BSF dependency errors/latency. – Alert separately on sustained late-arrival and late-processing so upstream timeout issues and internal slowness are distinguishable **Recovery**: • If late-arrival is high: investigate upstream callers/network delay and timeout/ header propagation; ensure requests are not reaching binding already expired. • If late-processing is high: reduce processing latency in binding and dependencies (especially BSF/DB), check pod saturation, latency spikes, thread starvation, and downstream timeout/error conditions. • Review recent config or traffic changes that enabled/shifted late request handling or increased request latency. • After mitigation, verify the rejection metrics fall and the ratio drops below 10% for the namespace.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.87 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MINOR

Table 8-103 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MINOR

Field	Details
Description	If 30% to 50% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Summary	If 30% to 50% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Severity	Minor
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY",response!~"2.*"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY"}[5m]))) * 100 > 30 <= 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.129
Metric Used	occnp_policy_data_resubscription_response_total
Recommended Actions	• The alert will be raised if policy data subscription is eligible for re-subscription but during resubscription errors observed. Could be due to timeout/ any other error from UDR or UDR-Connector. • If 4xx (check occnp_policy_data_resubscription_response_total metrics) is received it can be due to subscription deleted from UDR. Check the communication between PDS and UDR. • The alert will be cleared after resusbcription succeess rate > 70%

8.1.1.88 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MAJOR

Table 8-104 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MAJOR

Field	Details
Description	If 50% to 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Summary	If 50% to 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY",response!~"2.*"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY"}[5m]))) * 100 > 50 <= 70

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-104 (Cont.) POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MAJOR

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.129
Metric Used	occnp_policy_data_resubscription_response_total
Recommended Actions	• The alert will be raised if policy data subscription is eligible for re-subscription but during resubscription errors observed. Could be due to timeout/ any other error from UDR or UDR-Connector. • If 4xx (check occnp_policy_data_resubscription_response_total metrics) is received it can be due to subscription deleted from UDR. Check the communication between PDS and UDR. • The alert will be cleared after resusbcription succeess rate > 50%

8.1.1.89 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_CRITICAL

Table 8-105 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_CRITICAL

Field	Details
Description	If 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Summary	If 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY",response!~"2.*"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY"}[5m]))) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.129
Metric Used	occnp_policy_data_resubscription_response_total
Recommended Actions	• The alert will be raised if policy data subscription is eligible for re-subscription but during resubscription errors observed. Could be due to timeout/ any other error from UDR or UDR-Connector. • If 4xx (check occnp_policy_data_resubscription_response_total metrics) is received it can be due to subscription deleted from UDR. Check the communication between PDS and UDR. • The alert will be cleared after resusbcription succeess rate > 30%

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.90 POLICYDS_EXPIRED_SUBSCRIPTION

Table 8-106 POLICYDS_EXPIRED_SUBSCRIPTION

Field	Details
Description	If more than 10% of audited subscriptions are expired, this alert will be raised.
Summary	If more than 10% of audited subscriptions are expired, this alert will be raised.
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_request_total{expiryStatus="EXPIRED"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_request_total[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.130
Metric Used	occnp_policy_data_resubscription_request_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

8.1.1.91 LDAP_PEER_CONNECTION_LOST

Table 8-107 LDAP_PEER_CONNECTION_LOST

Field	Details
Name in Alert Yaml File	LDAP_PEER_CONNECTION_LOST
Description	This alert is triggered when the LDAP Gateway loses connection to its LDAP peer(s). It is based on the value of the occnp_ldap_conn_total metric falling to zero. The connection re-attempt and alert clearance behavior is governed by a new configuration parameter, LDAP_CONNECTION_REVERT_DELAY.
Summary	LDAP Gateway loses connection to its LDAP peer(s).
Severity	major
Expression	sum by (namespace,peer)(occnp_ldap_conn_total) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.113
Metric Used	occnp_ldap_conn_total
Recommended Actions	• Verify that the LDAP server is running and connectivity between the PCF and LDAP peers is available. • If LDAP is reachable, check the configured **LDAP_CONNECTION_REVERT_DELAY** value since reconnection attempts and alert clearance depend on this setting.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.92 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_MINOR

Table 8-108 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_MINOR

Field	Details
Description	Memory usage for PRE Service Pod {{$labels.namespace}}-{{$labels.container}}-{{$labels.pod}} is above 75. Current value is: {{ $value }}'
Summary	Memory usage for PRE Service Pod {{$labels.namespace}}-{{$labels.container}}-{{$labels.pod}} service is above 75
Severity	Minor
Expression	(100 * max by (container, pod, namespace) (container_memory_working_set_bytes{container=~".*pre-service.*"})/ sum by (container, pod, namespace) (kube_pod_container_resource_limits{resource="memory",container=~".*pre-service.*"})) >= 75 < 85
OID	1.3.6.1.4.1.323.5.3.52.1.2.131
Recommended Actions	This is a PRE pod level alert which fires when memory usage of PRE pod equals to or is greater than 75 but less than 85%. The alert will be cleared once the memory usage reduces below the threshold.

8.1.1.93 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_MAJOR

Table 8-109 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_MAJOR

Field	Details
Description	Memory usage for PRE Service Pod {{$labels.namespace}}-{{$labels.container}}-{{$labels.pod}} service is above 85. Current value is: {{ $value }}
Summary	Memory usage for PRE Service Pod {{$labels.namespace}}-{{$labels.container}}-{{$labels.pod}} service is above 85
Severity	Major
Expression	(100 * max by (container, pod, namespace) (container_memory_working_set_bytes{container=~".*pre-service.*"})/ sum by (container, pod, namespace) (kube_pod_container_resource_limits{resource="memory",container=~".*pre-service.*"})) >= 85 < 95
OID	1.3.6.1.4.1.323.5.3.52.1.2.131
Recommended Actions	This is a PRE pod level alert which fires when memory usage of PRE pod equals to or is greater than 85 but less than 95%. The alert will be cleared once the memory usage reduces below the threshold.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.94 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_CRITICAL

Table 8-110 MEMORY_USAGE_PER_PRE_POD_ABOVE_THRESHOLD_CRITICAL

Field	Details
Description	Memory usage for PRE Service Pod {{$labels.namespace}}-{{$labels.container}}-{{$labels.pod}} service is above 95. Current value is: {{ $value }}
Summary	Memory usage for PRE Service Pod {{$labels.namespace}}-{{$labels.container}}-{{$labels.pod}} service is above 95
Severity	Critical
Expression	(100 * max by (container, pod, namespace) (container_memory_working_set_bytes{container=~".*pre-service.*"})/ sum by (container, pod, namespace) (kube_pod_container_resource_limits{resource="memory",container=~".*pre-service.*"})) >= 95
OID	1.3.6.1.4.1.323.5.3.52.1.2.131
Recommended Actions	This is a PRE pod level alert which fires when memory usage of PRE pod equals to or is greater than 95%. The alert will be cleared once the memory usage reduces below the threshold.

8.1.1.95 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD

Table 8-111 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server.
Summary	Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server.
Severity	Minor
Expression	sum by(notificationEndpoint) (increase(http_notification_response_total{responseCode!~"2.*"}[2m])) > 500 and sum by(notificationEndpoint) (increase(http_notification_response_total{responseCode!~"2.*"}[2m])) <= 750
OID	1.3.6.1.4.1.323.5.3.44.1.2.42

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-111 (Cont.)
SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD indicates a critical increase in notification transaction failures for a given notificationEndpoint. The alert fires when non-2xx HTTP responses exceed 500 but remains lesser than 750 within 2 minutes (per endpoint), suggesting the Subscriber Notification server is failing to deliver notifications successfully. **Diagnostic Information**: • Identify which response codes dominate (for example, 4xx vs 5xx vs 429) for the affected notificationEndpoint. • Confirm whether the issue is isolated to one endpoint or widespread across endpoints (compare top failing endpoints). • Correlate with latency and timeout signals (HTTP client timeouts, upstream duration histograms if available). • Check Subscriber Notification server logs for: repeated errors, payload validation failures, auth errors, TLS handshake failures, connection timeouts/resets. • Validate downstream endpoint health: DNS resolution, cert validity, firewall rules, rate limiting (429), maintenance windows. • Check internal dependencies used for notification delivery (DB/queue/service mesh): errors, saturation, connection pool exhaustion. • Review recent deployments/configuration changes affecting: endpoint routing, auth credentials, payload format, retry policy, timeout policy. **Recovery**: • If failures are 4xx, fix payload/auth/configuration issues (credentials, headers, schema) and reprocess if applicable. • If failures are 5xx/timeouts, stabilize dependencies and reduce retry amplification (add backoff/jitter, cap concurrency). • If downstream endpoint is unhealthy or rate-limiting (429), coordinate with endpoint owner, apply throttling, or pause/retry with backoff. • If resource saturation is contributing, scale out the service or adjust resource limits/queues. • Roll back recent changes if a regression is suspected. • Clears when non-2xx responses for each notificationEndpoint drop below 500 over 2 minutes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.96 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD

Table 8-112 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the major threshold limit for a given Subscriber Notification server
Summary	Transaction Error exceeds the major threshold limit for a given Subscriber Notification server
Severity	Major
Expression	sum by(notificationEndpoint) (increase(http_notification_response_total{responseCode!~"2.*"}[2m])) > 750 and sum by(notificationEndpoint) (increase(http_notification_response_total{responseCode!~"2.*"}[2m])) <= 1000
OID	1.3.6.1.4.1.323.5.3.44.1.2.42

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-112 (Cont.)
SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD indicates a critical increase in notification transaction failures for a given notificationEndpoint. The alert fires when non-2xx HTTP responses exceed 750 but less than1000 within 2 minutes (per endpoint), suggesting the Subscriber Notification server is failing to deliver notifications successfully. **Diagnostic Information**: • Identify which response codes dominate (for example, 4xx vs 5xx vs 429) for the affected notificationEndpoint. • Confirm whether the issue is isolated to one endpoint or widespread across endpoints (compare top failing endpoints). • Correlate with latency and timeout signals (HTTP client timeouts, upstream duration histograms if available). • Check Subscriber Notification server logs for: repeated errors, payload validation failures, auth errors, TLS handshake failures, connection timeouts/resets. • Validate downstream endpoint health: DNS resolution, cert validity, firewall rules, rate limiting (429), maintenance windows. • Check internal dependencies used for notification delivery (DB/queue/service mesh): errors, saturation, connection pool exhaustion. • Review recent deployments/configuration changes affecting: endpoint routing, auth credentials, payload format, retry policy, timeout policy. **Recovery**: • If failures are 4xx, fix payload/auth/ configuration issues (credentials, headers, schema) and reprocess if applicable. • If failures are 5xx/timeouts, stabilize dependencies and reduce retry amplification (add backoff/jitter, cap concurrency). • If downstream endpoint is unhealthy or rate-limiting (429), coordinate with endpoint owner, apply throttling, or pause/retry with backoff. • If resource saturation is contributing, scale out the service or adjust resource limits/queues. • Roll back recent changes if a regression is suspected. • Treat sustained MAJOR as incident-level, especially if impacting multiple endpoints or causing backlog growth. • Clears when non-2xx responses for each notificationEndpoint drop below 750 over 2 minutes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.97 RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-113 RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Rx timeout count exceeds the critical threshold limit
Summary	Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"} [5m])) * 100 > 90
Condition	The timeout rate of RAA Rx messages has exceeded the configured threshold limit.
OID	1.3.6.1.4.1.323.5.3.52.1.2.36
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode! ~"timeout"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-113 (Cont.) RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause:** Rx RAA timeouts are near-total, meaning most RAR→RAA transactions are not completing within timer. Typical causes: Rx peer AF unreachable/slow, network loss/latency, Diameter connection instability, routing/realm misroute, or local saturation/backlog causing timeouts. **Diagnostic Information**: • Validate ratio + ensure meaningful traffic volume. • Total RAA(Rx): sum(rate(`occnp_diam_response_local_total{appId="16777236",msgType="RAA"}`[5m])) • Timeout RAA(Rx): sum(rate(`occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode="timeout"}`[5m])) • Identify top affected peers (use labels you have: destHost, destRealm, reqDestHost, reqDestRealm, origHost). • `sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode="timeout"}[5m]))` • Confirm whether timeouts are specific to Rx/RAA or broader - sum by (msgType,appId) (rate(`occnp_diam_response_local_total{responseCode="timeout"}`[5m])). • Check backlog/congestion indicators. • `occnp_diam_pending_requests` (or equivalent) • `sum(rate(occnp_stale_diam_request_cleanup_total[5m])) (or equivalent)` • Correlate with peer connectivity signals (Diameter stack logs/metrics): watchdog failures, disconnect/reconnect loops, send failures. **Recovery**: • If isolated to one AF/peer: failover/reroute Rx traffic if supported; restore peer/network health. • If local saturation/backlog: scale out, reduce load, fix CPU/memory/thread pool/queue bottlenecks; ensure pending drains. • If network/transport issue: remediate SCTP/TCP stability, latency/loss, ACL/firewall, MTU/TLS settings; stabilize sessions. • Only adjust timers after confirming the peer is healthy and latency SLOs justify it. • Validate: Rx RAA timeout % drops < threshold and success responses recover.

8.1.1.98 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-114 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Rx timeout count exceeds the major threshold limit
Summary	Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-114 (Cont.) RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.36
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!~"timeout"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-114 (Cont.) RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** Rx RAA timeouts are near-total, meaning most RAR→RAA transactions are not completing within timer. Typical causes: Rx peer AF unreachable/slow, network loss/latency, Diameter connection instability, routing/realm misroute, or local saturation/backlog causing timeouts. Partial outage/degradation trending toward critical (intermittent peer slowness, emerging congestion, routing instability). **Diagnostic Information**: • Validate ratio + ensure meaningful traffic volume. • Total RAA(Rx): sum(rate(`occnp_diam_response_local_total{appId="16777236",msgType="RAA"}`[5m])) • Timeout RAA(Rx): sum(rate(`occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode="timeout"}`[5m])) • Identify top affected peers (use labels you have: destHost, destRealm, reqDestHost, reqDestRealm, origHost). • `sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode="timeout"}[5m]))` • Confirm whether timeouts are specific to Rx/RAA or broader - sum by (msgType,appId) (rate(`occnp_diam_response_local_total{responseCode="timeout"}`[5m])). • Check backlog/congestion indicators. • `occnp_diam_pending_requests` (or equivalent) • `sum(rate(occnp_stale_diam_request_cleanup_total[5m])) (or equivalent)` • Correlate with peer connectivity signals (Diameter stack logs/metrics): watchdog failures, disconnect/reconnect loops, send failures. • Trend by peer to find the first reason: – - topk(5, sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA", responseCode="timeout"}[5m]))) **Recovery**: • If isolated to one AF/peer: failover/reroute Rx traffic if supported; restore peer/network health. • If local saturation/backlog: scale out, reduce load, fix CPU/memory/thread pool/queue bottlenecks; ensure pending drains. • If network/transport issue: remediate SCTP/TCP stability, latency/loss, ACL/firewall, MTU/TLS settings; stabilize sessions. • Only adjust timers after confirming the peer is healthy and latency SLOs justify it. • Validate: Rx RAA timeout % drops < threshold and success responses recover. • Emphasis on preventing escalation: restore degraded peer, preemptive reroute, relieve load, confirm timeouts return to baseline.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.99 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-115 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Rx timeout count exceeds the minor threshold limit
Summary	Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.36
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!~"timeout"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-115 (Cont.) RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** Early warning of Rx RAA timeout increase; may be bursty, peer-specific, or correlated with traffic spikes. **Diagnostic Information**: • Validate ratio + ensure meaningful traffic volume. • Total RAA(Rx): sum(rate(`occnp_diam_response_local_total{appId="16777236",msgType="RAA"}`[5m])) • Timeout RAA(Rx): sum(rate(`occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode="timeout"}`[5m])) • Identify top affected peers (use labels you have: destHost, destRealm, reqDestHost, reqDestRealm, origHost). • `sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode="timeout"}[5m]))` • Confirm whether timeouts are specific to Rx/RAA or broader - sum by (msgType,appId) (rate(`occnp_diam_response_local_total{responseCode="timeout"}`[5m])). • Check backlog/congestion indicators. • `occnp_diam_pending_requests` (or equivalent) • `sum(rate(occnp_stale_diam_request_cleanup_total[5m])) (or equivalent)` • Correlate with peer connectivity signals (Diameter stack logs/metrics): watchdog failures, disconnect/reconnect loops, send failures. • Trend by peer to find the first reason: – - topk(5, sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA", responseCode="timeout"}[5m]))) • Compare 5m vs 30m to see persistence: - (example) avg_over_time((sum(rate(…timeout…[5m])) / sum(rate(…total…[5m])) * 100)[30m:]) **Recovery**: • If isolated to one AF/peer: failover/reroute Rx traffic if supported; restore peer/network health. • If local saturation/backlog: scale out, reduce load, fix CPU/memory/thread pool/queue bottlenecks; ensure pending drains. • If network/transport issue: remediate SCTP/TCP stability, latency/loss, ACL/firewall, MTU/TLS settings; stabilize sessions. • Only adjust timers after confirming the peer is healthy and latency SLOs justify it. • Validate: Rx RAA timeout % drops < threshold and success responses recover. • Emphasis on preventing escalation: restore degraded peer, preemptive reroute, relieve load, confirm timeouts return to baseline. **Recovery:** Proactive checks: peer health/connectivity, reroute if one peer is degrading, address rising resource use/backlog before MAJOR/CRITICAL.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.100 PCF_STATE_NON_FUNCTIONAL_CRITICAL

Table 8-116 PCF_STATE_NON_FUNCTIONAL_CRITICAL

Field	Details
Description	Policy is in non functional state due to DB cluster state down.
Summary	Policy is in non functional state due to DB cluster state down.
Severity	Critical
Expression	appinfo_nfDbFunctionalState_current{nfDbFunctionalState="Not_Running"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.102
Metric Used	appinfo_nfDbFunctionalState_current
Recommended Actions	For any additional guidance, contact My Oracle Support.

8.1.1.101 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST_EGW

Table 8-117 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST_EGW

Field	Details
Description	Egress Gateway traffic is getting rejected more than 1% because of ratelimiting.
Summary	EGW traffic getting rejected more than 1% because of ratelimiting
Severity	Major
Expression	(sum by (namespace, pod) (rate(oc_egressgateway_http_request_ratelimit_values_total{Allowed="false",microservice="occnp-occnp-egress-gateway"}[5m]))) / sum by (namespace, pod) (rate(oc_egressgateway_http_request_ratelimit_values_total{microservice="occnp-occnp-egress-gateway"}[5m])) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.114
Metric Used	oc_egressgateway_http_request_ratelimit_values_total
Recommended Actions	The alert is cleared when the failure rate goes below 1% of total tps.

8.1.1.102 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Table 8-118 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Description	UDR returning with POST subscribe response but without user data for SM as part of immediate reporting occurring above 10% for service {{$labels.microservice}} in {{$labels.namespace}} (current value: {{ $value }} %)
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-118 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.127
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-118 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing SM user data check is based on: * `service_subresource = "sm-data"` (indicates the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `imm_reports_present = "false"` (indicates no SM user data was returned from UDR as part of the Immediate Reporting capability) – If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response without SM user data as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (e.g., `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved, inform the UDR operators to verify whether the Immediate Reporting feature is working and negotiated from their end.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-118 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

8.1.1.103 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Table 8-119 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.127
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-119 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing SM user data check is based on: * `service_subresource = "sm-data"` (to indicate the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no SM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response **without** user data for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and still no SM user data is retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-119 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

8.1.1.104 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Table 8-120 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Description	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx", immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-120 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Recommended Actions	**Cause**: UDR profile/capability mismatch, partial rollout/config drift across UDR instances, or negotiation disabled/missing in returned `supportedFeatures`. **Diagnostic Information**: • Verification steps: • Query `occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}` split by `immediate_report_pcc`, `nf_name`, and `namespace`. • Check whether one/few UDR `nf_name` values dominate the `immediate_report_pcc="false"` bucket. • Review PCF logs around `handleSuccessResponseForImmRep` / UDR POST response for messages showing returned `supportedFeatures` does not set ImmediateReportPcc. • Confirm PCF-side enablement: `optimizeSubscribe=true`, global `UDR.IMMREP` enabled, and Helm `enable.immediate.reporting.sm-data=true`. • Compare UDR profile capability / returned `supportedFeatures` across healthy vs affected UDRs. • Monitoring recommendations: • Break down the metric by `nf_name` to isolate bad UDR instances. • Also watch `occnp_immrep_request_total` vs `occnp_immrep_response_total` for request/response symmetry. • Track `imm_reports_present` and `error_cause` for adjacent degradation patterns. • Alert separately if the ratio increases beyond 30% or becomes concentrated on a single UDR. **Recovery**: • Verify and correct UDR capability/config so returned `supportedFeatures` includes ImmediateReportPcc for `sm-data` subscriptions. • If only specific UDR instances are affected, drain/remove or fix those instances and confirm the `immediate_report_pcc="false"` ratio drops. • If intentional/not supported in the environment, disable `sm-data` immediate reporting consistently to avoid mixed negotiation behavior. • After change, confirm the alert ratio returns below threshold and

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-120 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
	`immediate_report_pcc="true"` dominates successful POST responses.

8.1.1.105 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Table 8-121 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Minor
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx", immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-121 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Recommended Actions	**Cause**: UDR profile/capability mismatch, partial rollout/config drift across UDR instances, or negotiation disabled/missing in returned `supportedFeatures`. **Diagnostic Information**: • Verification steps: • Query `occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}` split by `immediate_report_pcc`, `nf_name`, and `namespace`. • Check whether one/few UDR `nf_name` values dominate the `immediate_report_pcc="false"` bucket. • Review PCF logs around `handleSuccessResponseForImmRep` / UDR POST response for messages showing returned `supportedFeatures` does not set ImmediateReportPcc. • Confirm PCF-side enablement: `optimizeSubscribe=true`, global `UDR.IMMREP` enabled, and Helm `enable.immediate.reporting.sm-data=true`. • Compare UDR profile capability / returned `supportedFeatures` across healthy vs affected UDRs. • Monitoring recommendations: • Break down the metric by `nf_name` to isolate bad UDR instances. • Also watch `occnp_immrep_request_total` vs `occnp_immrep_response_total` for request/response symmetry. • Track `imm_reports_present` and `error_cause` for adjacent degradation patterns. • Alert separately if the ratio increases beyond 20% or becomes concentrated on a single UDR. **Recovery**: • Verify and correct UDR capability/config so returned `supportedFeatures` includes ImmediateReportPcc for `sm-data` subscriptions. • If only specific UDR instances are affected, drain/remove or fix those instances and confirm the `immediate_report_pcc="false"` ratio drops. • If intentional/not supported in the environment, disable `sm-data` immediate reporting consistently to avoid mixed negotiation behavior. • After change, confirm the alert ratio returns below threshold and

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-121 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
	`immediate_report_pcc="true"` dominates successful POST responses.

8.1.1.106 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Table 8-122 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx",immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-122 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Recommended Actions	**Cause**: UDR profile/capability mismatch, partial rollout/config drift across UDR instances, or negotiation disabled/missing in returned `supportedFeatures`. **Diagnostic Information**: • Verification steps: • Query `occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}` split by `immediate_report_pcc`, `nf_name`, and `namespace`. • Check whether one/few UDR `nf_name` values dominate the `immediate_report_pcc="false"` bucket. • Review PCF logs around `handleSuccessResponseForImmRep` / UDR POST response for messages showing returned `supportedFeatures` does not set ImmediateReportPcc. • Confirm PCF-side enablement: `optimizeSubscribe=true`, global `UDR.IMMREP` enabled, and Helm `enable.immediate.reporting.sm-data=true`. • Compare UDR profile capability / returned `supportedFeatures` across healthy vs affected UDRs. • Monitoring recommendations: • Break down the metric by `nf_name` to isolate bad UDR instances. • Also watch `occnp_immrep_request_total` vs `occnp_immrep_response_total` for request/response symmetry. • Track `imm_reports_present` and `error_cause` for adjacent degradation patterns. • Alert separately if the ratio increases beyond 20% to 30% or becomes concentrated on a single UDR. **Recovery**: • Verify and correct UDR capability/config so returned `supportedFeatures` includes ImmediateReportPcc for `sm-data` subscriptions. • If only specific UDR instances are affected, drain/remove or fix those instances and confirm the `immediate_report_pcc="false"` ratio drops. • If intentional/not supported in the environment, disable `sm-data` immediate reporting consistently to avoid mixed negotiation behavior. • After change, confirm the alert ratio returns below threshold and

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-122 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
	`immediate_report_pcc="true"` dominates successful POST responses.

8.1.1.107 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Table 8-123 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Description	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-123 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "sm-data"` (indicates the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `immediate_report_pcc = "false"` (indicates that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-123 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
	working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

8.1.1.108 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MINOR_PERCENT

Table 8-124 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MINOR_PERCENT

Field	Details
Description	20% or more but less than 50% of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control
Summary	20% or more but less than 50% of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_dnn_replacement_total{mandatory_ie_missing!=""}[5m]))) / (sum by (namespace) (rate(occnp_dnn_replacement_total[5m]))) * 100 >= 20 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.137
Metric Used	occnp_dnn_replacement_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-124 (Cont.) DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MINOR_PERCENT

Field	Details
Recommended Actions	Cause: This alert is triggered when the percentage of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control. When occnp_dnn_replacement_total{mandatory_ie_missing!=""} increases, it indicates: AMF is sending invalid request body with PCRT (SMF_SELECT_CH or ALLOWED_NSSAI_CH) but allowedSnssais and/or snssai/dnn it's missing. Diagnostics Information: Verification steps: • Send a valid AM Update request including all mandatory IEs for DnnReplacement. • Ensure allowedSnssais/snssai/dnn are present and that DnnReplacement is negotiated. • Confirm the request succeeds. • Verify that the 400/ MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. Recovery: • Check AMF configuration and behavior as why invalid values are sent. • Investigate configuration mismatch between PCF and AMF. • Escalate if sustained at Major or Critical level.

8.1.1.109 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MAJOR_PERCENT

Table 8-125 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MAJOR_PERCENT

Field	Details
Description	50% or more but less than 75% of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control
Summary	50% or more but less than 75% of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control
Severity	Major
Expression	(sum by (namespace) (rate(occnp_dnn_replacement_total{mandatory_ie_missing!=""}[5m]))) / (sum by (namespace) (rate(occnp_dnn_replacement_total[5m]))) * 100 >= 50 < 75

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-125 (Cont.) DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_MAJOR_PERCENT

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.137
Metric Used	occnp_dnn_replacement_total
Recommended Actions	Cause: This alert is triggered when the percentage of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control. When occnp_dnn_replacement_total{mandatory_ie_missing!=""} increases, it indicates: AMF is sending invalid request body with PCRT (SMF_SELECT_CH or ALLOWED_NSSAI_CH) but allowedSnssais and/or snssai/dnn it's missing. Diagnostics Information: Verification steps: • Send a valid AM Update request including all mandatory IEs for DnnReplacement. • Ensure allowedSnssais/snssai/dnn are present and that DnnReplacement is negotiated. • Confirm the request succeeds. • Verify that the 400/ MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. Recovery: • Check AMF configuration and behavior as why invalid values are sent. • Investigate configuration mismatch between PCF and AMF. • Escalate if sustained at Major or Critical level.

8.1.1.110 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_CRITICAL_PERCENT

Table 8-126 DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_CRITICAL_PERCENT

Field	Details
Description	More than 75% of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control
Summary	More than 75% of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-126 (Cont.)
DNN_REPLACEMENT_MANDATORY_IE_MISSING_ABOVE_CRITICAL_PERCENT

Field	Details
Expression	(sum by (namespace) (rate(occnp_dnn_replacement_total{mandatory_ie_missing!=""}[5m]))) / (sum by (namespace) (rate(occnp_dnn_replacement_total[5m]))) * 100 >= 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.137
Metric Used	occnp_dnn_replacement_total
Recommended Actions	Cause: This alert is triggered when the percentage of AM Update requests are rejected due to Mandatory IE Missing for DNN Replacement Control. When occnp_dnn_replacement_total{mandatory_ie_missing!=""} increases, it indicates: AMF is sending invalid request body with PCRT (SMF_SELECT_CH or ALLOWED_NSSAI_CH) but allowedSnssais and/or snssai/dnn it's missing. Diagnostics Information: Verification steps: • Send a valid AM Update request including all mandatory IEs for DnnReplacement. • Ensure allowedSnssais/snssai/dnn are present and that DnnReplacement is negotiated. • Confirm the request succeeds. • Verify that the 400/ MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. Recovery: • Check AMF configuration and behavior as why invalid values are sent. • Investigate configuration mismatch between PCF and AMF. • Escalate if sustained at Major or Critical level.

8.1.1.111 QOS_MON_MISSING_ATTRIBUTES_ABOVE_CRITICAL_PERCENT

Table 8-127 QOS_MON_MISSING_ATTRIBUTES_ABOVE_CRITICAL_PERCENT

Field	Description
Description	More than 70% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring
Summary	More than 70% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring
Severity	CRITICAL

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-127 (Cont.) QOS_MON_MISSING_ATTRIBUTES_ABOVE_CRITICAL_PERCENT

Field	Description
Expression	(sum by (namespace) (rate(occnp_pa_qosmon_request_total{incompleteQosMonAttr="true"}[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.134
Metric Used	occnp_pa_qosmon_request_total
Recommended Actions	More than 70% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring.The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.112 QOS_MON_MISSING_ATTRIBUTES_ABOVE_MAJOR_PERCENT

Table 8-128 QOS_MON_MISSING_ATTRIBUTES_ABOVE_MAJOR_PERCENT

Field	Details
Description	More than 50% but less than 70% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring
Summary	More than 50% but less than 70% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring
Severity	MAJOR
Expression	(sum by (namespace) (rate(occnp_pa_qosmon_request_total{incompleteQosMonAttr="true"}[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.134
Metric Used	occnp_pa_qosmon_request_total
Recommended Actions	More than 50% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring. The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.113 QOS_MON_MISSING_ATTRIBUTES_ABOVE_MINOR_PERCENT

Table 8-129 QOS_MON_MISSING_ATTRIBUTES_ABOVE_MINOR_PERCENT

Field	Description
Description	More than 30% but less than 50% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring
Summary	More than 30% but less than 50% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring
Severity	MINOR

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-129 (Cont.) QOS_MON_MISSING_ATTRIBUTES_ABOVE_MINOR_PERCENT

Field	Description
Expression	(sum by (namespace) (rate(occnp_pa_qosmon_request_total{incompleteQosMonAttr="true"}[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.134
Metric Used	occnp_pa_qosmon_request_total
Recommended Actions	More than 30% of Npcf_PolicyAuthorization Create requests are missing at least 1 attribute for QosMonitoring. The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.114 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT

Table 8-130 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_CRITICAL_PERCENT

Field	Description
Description	More than 70% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Summary	More than 70% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Severity	CRITICAL
Expression	sum by (namespace) (rate(occnp_sm_qosmon_decs_error_total[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.133
Metric Used	occnp_sm_qosmon_decs_error_total, occnp_pa_qosmon_request_total
Recommended Actions	The number of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF with QOS_MON_DECS_ERR represents 70% or more of the total app sessions. The alert will be cleared once the reject rate reduces below the threshold.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.1.115 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MAJOR_PERCENT

Table 8-131 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MAJOR_PERCENT

Field	Description
Description	More than 50% but less than 70% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Summary	More than 50% but less than 70% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Severity	MAJOR
Expression	(sum by (namespace) (rate(occnp_sm_qosmon_decs_error_total[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.133
Metric Used	occnp_sm_qosmon_decs_error_total, occnp_pa_qosmon_request_total
Recommended Actions	The number of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF with QOS_MON_DECS_ERR represents 50% or more of the total app sessions. The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.116 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MINOR_PERCENT

Table 8-132 QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MINOR_PERCENT

Field	Description
Description	More than 30% but less than 50% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Summary	More than 30% but less than 50% of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF contains QOS_MON_DECS_ERR
Severity	MINOR
Expression	(sum by (namespace) (rate(occnp_sm_qosmon_decs_error_total[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.133
Metric Used	occnp_sm_qosmon_decs_error_total, occnp_pa_qosmon_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-132 (Cont.)
QOS_MON_SMF_POLICY_FAILURE_CODE_ABOVE_MINOR_PERCENT

Field	Description
Recommended Actions	The number of SMF updateNotify responses and/or Npcf_SMPolicyControl_Update requests from SMF with QOS_MON_DECS_ERR represents 30% or more of the total app sessions. The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.117 QOS_MON_FAILED_AUTH_ABOVE_CRITICAL_PERCENT

Table 8-133 QOS_MON_FAILED_AUTH_ABOVE_CRITICAL_PERCENT

Field	Description
Description	More than 70% of PA Create got rejected due to QosMonitoring
Summary	More than 70% of PA Create got rejected due to QosMonitoring
Severity	CRITICAL
Expression	(sum by (namespace) (rate(occnp_pa_qosmon_response_total{cause=~"MISSING_ATTR|FEATURE_UNSUPPORTED|REJECTED"}[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.132
Metric Used	occnp_pa_qosmon_response_total, occnp_pa_qosmon_request_total
Recommended Actions	The percentage of Npcf_PolicyAuthorization Create requests that get rejected by policy because of QosMonitoring is equal or greater than 70%. The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.118 QOS_MON_FAILED_AUTH_ABOVE_MAJOR_PERCENT

Table 8-134 QOS_MON_FAILED_AUTH_ABOVE_MAJOR_PERCENT

Field	Description
Description	More than 50% but less than 70% of PA Create got rejected due to QosMonitoring
Summary	More than 50% but less than 70% of PA Create got rejected due to QosMonitoring
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-134 (Cont.) QOS_MON_FAILED_AUTH_ABOVE_MAJOR_PERCENT

Field	Description
Expression	(sum by (namespace) (rate(occnp_pa_qosmon_response_total{cause=~"MISSING_ATTR|FEATURE_UNSUPPORTED|REJECTED"}[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.132
Metric Used	occnp_pa_qosmon_response_total, occnp_pa_qosmon_request_total
Recommended Actions	The percentage of Npcf_PolicyAuthorization Create requests that get rejected by policy because of QosMonitoring is equal or greater than 50%. The alert will be cleared once the reject rate reduces below the threshold.

8.1.1.119 QOS_MON_FAILED_AUTH_ABOVE_MINOR_PERCENT

Table 8-135 QOS_MON_FAILED_AUTH_ABOVE_MINOR_PERCENT

Field	Description
Description	More than 30% but less than 50% of PA Create got rejected due to QosMonitoring
Summary	More than 30% but less than 50% of PA Create got rejected due to QosMonitoring
Severity	MINOR
Expression	(sum by (namespace) (rate(occnp_pa_qosmon_response_total{cause=~"MISSING_ATTR|FEATURE_UNSUPPORTED|REJECTED"}[5m]))) / (sum by (namespace) (rate(occnp_pa_qosmon_request_total[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.132
Metric Used	occnp_pa_qosmon_response_total
Recommended Actions	The percentage of Npcf_PolicyAuthorization Create requests that get rejected by policy because of QosMonitoring is equal or greater than 30%. The alert will be cleared once the reject rate reduces below the threshold.

8.1.2 PCF Alerts

This section provides information on PCF alerts.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.1 EGRESS_GATEWAY_DNS_RESOLUTION_FAILURE

Table 8-136 EGRESS_GATEWAY_DNS_RESOLUTION_FAILURE

Field	Details
Description	Egress Gateway encountered DNS SRV resolution failure.
Summary	"{{$labels.microservice}} is unable to route to SCP in namespace {{$labels.namespace}} due to DNS-SRV lookup failure for the FQDN {{$labels.vfqdn}}"
Severity	MAJOR
Expression	(increase(occnp_oc_egressgateway_resolve_fqdn_from_ars_failure_total[2m])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.138
Metric Used	occnp_oc_egressgateway_resolve_fqdn_from_ars_failure_total
Recommended Actions	**Cause:** Due to misconfiguration, the Egress Gateway was not routing to the SCP properly because of a DNS-SRV lookup failure. **Diagnostic Information:** 1. Check whether `sbirouting` is enabled in the egress gateway ConfigMap. 2. Check the configured FQDN or vFQDN value in the egress gateway ConfigMap. 3. Verify the FQDN or vFQDN, value in custom values file. **Recovery:** If you configure the correct FQDN or vFQDN, the alert is cleared.

8.1.2.2 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Table 8-137 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Description	UDR returning with POST subscribe response but without user data for SM as part of immediate reporting occurring above 10% for service {{$labels.microservice}} in {{$labels.namespace}} (current value: {{ $value }} %)
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-137 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.127
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-137 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing SM user data check is based on: * `service_subresource = "sm-data"` (indicates the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `imm_reports_present = "false"` (indicates no SM user data was returned from UDR as part of the Immediate Reporting capability) – If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response without SM user data as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (e.g., `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved, inform the UDR operators to verify whether the Immediate Reporting feature is working and negotiated from their end.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-137 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

8.1.2.3 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Table 8-138 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.127
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-138 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing SM user data check is based on: * `service_subresource = "sm-data"` (to indicate the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no SM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response **without** user data for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and still no SM user data is retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-138 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

8.1.2.4 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Table 8-139 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Description	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx", immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-139 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Recommended Actions	**Cause**: UDR profile/capability mismatch, partial rollout/config drift across UDR instances, or negotiation disabled/missing in returned `supportedFeatures`. **Diagnostic Information**: • Verification steps: • Query `occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}` split by `immediate_report_pcc`, `nf_name`, and `namespace`. • Check whether one/few UDR `nf_name` values dominate the `immediate_report_pcc="false"` bucket. • Review PCF logs around `handleSuccessResponseForImmRep` / UDR POST response for messages showing returned `supportedFeatures` does not set ImmediateReportPcc. • Confirm PCF-side enablement: `optimizeSubscribe=true`, global `UDR.IMMREP` enabled, and Helm `enable.immediate.reporting.sm-data=true`. • Compare UDR profile capability / returned `supportedFeatures` across healthy vs affected UDRs. • Monitoring recommendations: • Break down the metric by `nf_name` to isolate bad UDR instances. • Also watch `occnp_immrep_request_total` vs `occnp_immrep_response_total` for request/response symmetry. • Track `imm_reports_present` and `error_cause` for adjacent degradation patterns. • Alert separately if the ratio increases beyond 30% or becomes concentrated on a single UDR. **Recovery**: • Verify and correct UDR capability/config so returned `supportedFeatures` includes ImmediateReportPcc for `sm-data` subscriptions. • If only specific UDR instances are affected, drain/remove or fix those instances and confirm the `immediate_report_pcc="false"` ratio drops. • If intentional/not supported in the environment, disable `sm-data` immediate reporting consistently to avoid mixed negotiation behavior. • After change, confirm the alert ratio returns below threshold and

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-139 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
	`immediate_report_pcc="true"` dominates successful POST responses.

8.1.2.5 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Table 8-140 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Minor
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx", immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-140 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Recommended Actions	**Cause**: UDR profile/capability mismatch, partial rollout/config drift across UDR instances, or negotiation disabled/missing in returned `supportedFeatures`. **Diagnostic Information**: • Verification steps: • Query `occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}` split by `immediate_report_pcc`, `nf_name`, and `namespace`. • Check whether one/few UDR `nf_name` values dominate the `immediate_report_pcc="false"` bucket. • Review PCF logs around `handleSuccessResponseForImmRep` / UDR POST response for messages showing returned `supportedFeatures` does not set ImmediateReportPcc. • Confirm PCF-side enablement: `optimizeSubscribe=true`, global `UDR.IMMREP` enabled, and Helm `enable.immediate.reporting.sm-data=true`. • Compare UDR profile capability / returned `supportedFeatures` across healthy vs affected UDRs. • Monitoring recommendations: • Break down the metric by `nf_name` to isolate bad UDR instances. • Also watch `occnp_immrep_request_total` vs `occnp_immrep_response_total` for request/response symmetry. • Track `imm_reports_present` and `error_cause` for adjacent degradation patterns. • Alert separately if the ratio increases beyond 20% or becomes concentrated on a single UDR. **Recovery**: • Verify and correct UDR capability/config so returned `supportedFeatures` includes ImmediateReportPcc for `sm-data` subscriptions. • If only specific UDR instances are affected, drain/remove or fix those instances and confirm the `immediate_report_pcc="false"` ratio drops. • If intentional/not supported in the environment, disable `sm-data` immediate reporting consistently to avoid mixed negotiation behavior. • After change, confirm the alert ratio returns below threshold and

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-140 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
	`immediate_report_pcc="true"` dominates successful POST responses.

8.1.2.6 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Table 8-141 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx", immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-141 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Recommended Actions	**Cause**: UDR profile/capability mismatch, partial rollout/config drift across UDR instances, or negotiation disabled/missing in returned `supportedFeatures`. **Diagnostic Information**: • Verification steps: • Query `occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",response_code="2xx"}` split by `immediate_report_pcc`, `nf_name`, and `namespace`. • Check whether one/few UDR `nf_name` values dominate the `immediate_report_pcc="false"` bucket. • Review PCF logs around `handleSuccessResponseForImmRep` / UDR POST response for messages showing returned `supportedFeatures` does not set ImmediateReportPcc. • Confirm PCF-side enablement: `optimizeSubscribe=true`, global `UDR.IMMREP` enabled, and Helm `enable.immediate.reporting.sm-data=true`. • Compare UDR profile capability / returned `supportedFeatures` across healthy vs affected UDRs. • Monitoring recommendations: • Break down the metric by `nf_name` to isolate bad UDR instances. • Also watch `occnp_immrep_request_total` vs `occnp_immrep_response_total` for request/response symmetry. • Track `imm_reports_present` and `error_cause` for adjacent degradation patterns. • Alert separately if the ratio increases beyond 20% to 30% or becomes concentrated on a single UDR. **Recovery**: • Verify and correct UDR capability/config so returned `supportedFeatures` includes ImmediateReportPcc for `sm-data` subscriptions. • If only specific UDR instances are affected, drain/remove or fix those instances and confirm the `immediate_report_pcc="false"` ratio drops. • If intentional/not supported in the environment, disable `sm-data` immediate reporting consistently to avoid mixed negotiation behavior. • After change, confirm the alert ratio returns below threshold and

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-141 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
	`immediate_report_pcc="true"` dominates successful POST responses.

8.1.2.7 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Table 8-142 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Description	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-142 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "sm-data"` (indicates the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `immediate_report_pcc = "false"` (indicates that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-142 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
	working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

8.1.2.8 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MINOR

Table 8-143 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MINOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 10% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Summary	More than 10% of the Diam Connector requests failed with error DIAMETER_ERROR_TIMED_OUT_REQUEST.
Severity	Minor
Expression	(sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]))) / ((sum by (namespace, pod) (rate(ocpm_ingress_request_total{msgType!~"DWR|CER", microservice=~".*diam-connector"}[5m])) or sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]) * 0)) + sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.88
Metric Used	• `occnp_stale_diam_request_cleanup_total` • `ocpm_ingress_request_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-143 (Cont.) STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MINOR

Field	Details
Recommended Actions	**Cause**: At least 10 % of the processed requests by Diameter Connector have gone stale before being completed. That means that PCF is taking too long to process the given requests. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between micro-services. Maybe a particular micro-service is slower. • **Review Logs**: Check PCF's Diameter logs to further investigate on why requests are taking too long; take special attention to the timestamps. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: If system is slow, please increase timeout values to consider these latencies. **Recovery**: As soon as Diameter processes incoming requests on time the Alert will turn off by itself.

8.1.2.9 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MAJOR

Table 8-144 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MAJOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 20% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Summary	More than 20% of the Diam Connector requests failed with error DIAMETER_ERROR_TIMED_OUT_REQUEST.
Severity	Major
Expression	(sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]))) / ((sum by (namespace, pod) (rate(ocpm_ingress_request_total{msgType!~"DWR|CER", microservice=~".*diam-connector"}[5m])) or sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]) * 0)) + sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.88
Metric Used	• `ocpm_ingress_request_total` • `occnp_stale_diam_request_cleanup_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-144 (Cont.) STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MAJOR

Field	Details
Recommended Actions	**Cause**: At least 20 % of the processed requests by Diameter Connector have gone stale before being completed. That means that PCF is taking too long to process the given requests. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between micro-services. Maybe a particular micro-service is slower. • **Review Logs**: Check PCF's Diameter logs to further investigate on why requests are taking too long; take special attention to the timestamps. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: If system is slow, please increase timeout values to consider these latencies. **Recovery**: As soon as Diameter processes incoming requests on time the Alert will turn off by itself.

8.1.2.10 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL

Table 8-145 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 30% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Summary	More than 30% of the Diam Connector requests failed with error DIAMETER_ERROR_TIMED_OUT_REQUEST.
Severity	Critical
Expression	(sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]))) / ((sum by (namespace, pod) (rate(ocpm_ingress_request_total{msgType!~"DWR|CER", microservice=~".*diam-connector"}[5m])) or sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]) * 0)) + sum by (namespace, pod) (rate(occnp_stale_diam_request_cleanup_total{microservice=~".*diam-connector"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.88
Metric Used	• `ocpm_ingress_request_total` • `occnp_stale_diam_request_cleanup_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-145 (Cont.) STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL

Field	Details
Recommended Actions	**Cause**: At least 30 % of the processed requests by Diameter Connector have gone stale before being completed. That means that PCF is taking too long to process the given requests. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between micro-services. Maybe a particular micro-service is slower. • **Review Logs**: Check PCF's Diameter logs to further investigate on why requests are taking too long; take special attention to the timestamps. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: If system is slow, please increase timeout values to consider these latencies. **Recovery**: As soon as Diameter processes incoming requests on time the Alert will turn off by itself.

8.1.2.11 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_CRITICAL_THRESHOLD

Table 8-146 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	Number of revalidation responses indicated the binding was missing but restored from BSF over all valid session sessions being audited is equal or above 70% of total revalidation responses.
Summary	70% or more of binding were missing but restored from BSF over all bindings being audited.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code="2xx",action="restored"} [5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.89
Metric Used	occnp_session_binding_revalidation_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-146 (Cont.) SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause**: At least 70 % of the PCF Bindings registered in Binding Service were missing in the registered BSF and had to be recovered. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and BSF. Maybe the Binding registration requests are not being sent, or taking too long to reach. • **Review Logs**: Check BSF's BSF MGMT logs to further investigate on why it isn't registering the sent PCF Bindings. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check BSF's Audit configurations to confirm if they Query to PCF is enabled. **Recovery**: Once PCF Bindings are properly registered (and not deleted in its lifetime), the percentage of missing bindings will decrease, and the Alert will turn off by itself.

8.1.2.12 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MAJOR_THRESHOLD

Table 8-147 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	Number of revalidation responses indicated the binding was missing but restored from BSF over all valid session sessions being audited is equal or above 50% but less than 70% of total revalidation responses.
Summary	50% to 70% of binding were missing but restored from BSF over all bindings being audited
Severity	Major
Expression	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx",action="restored"}[5m])) / sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.89

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-147 (Cont.) SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	**Cause**: At least 50 % of the PCF Bindings registered in Binding Service were missing in the registered BSF and had to be recovered. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and BSF. Maybe the Binding registration requests are not being sent, or taking too long to reach. • **Review Logs**: Check BSF's BSF MGMT logs to further investigate on why it isn't registering the sent PCF Bindings. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check BSF's Audit configurations to confirm if they Query to PCF is enabled. **Recovery**: Once PCF Bindings are properly registered (and not deleted in its lifetime), the percentage of missing bindings will decrease, and the Alert will turn off by itself.

8.1.2.13 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD

Table 8-148 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	Number of revalidation responses indicated the binding was missing but restored from BSF over all valid session sessions being audited is equal or above 30% but less than 50% of total revalidation responses.
Summary	30% to 50% of binding were missing but restored from BSF over all bindings being audited.
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-148 (Cont.)
SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD

Field	Details
Expression	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx",action="restored"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.89
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	**Cause**: At least 30 % of the PCF Bindings registered in Binding Service were missing in the registered BSF and had to be recovered. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and BSF. Maybe the Binding registration requests are not being sent, or taking too long to reach. • **Review Logs**: Check BSF's BSF MGMT logs to further investigate on why it isn't registering the sent PCF Bindings. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check BSF's Audit configurations to confirm if they Query to PCF is enabled. **Recovery**: Once PCF Bindings are properly registered (and not deleted in its lifetime), the percentage of missing bindings will decrease, and the Alert will turn off by itself.

8.1.2.14 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_CRITICAL_THRESHOLD

Table 8-149 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	Number of unsuccessful revalidation responses with error received from BSF when in PCF the binding association is valid session sessions is equal or above 70% of total revalidation responses.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-149 (Cont.)
SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Summary	70% or more of failed Revalidation Responses received from BSF over total Revalidation Responses
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code!~"2.*"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.90
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	**Cause**: At least 70 % of the sent bindings revalidation requests failed with a non-2xx response. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and BSF. Maybe the Binding registration requests are not being sent, or taking too long to reach. • **Review Logs**: Check BSF's IGW and BSF MGMT logs to further investigate on why it isn't receiving its Binding Registration requests. • **Scale System Resources**: High CPU or memory usage may lead to some Binding Registration requests to not be processed. Scale pods as required by the traffic. **Recovery**: Once binding revalidation requests are properly processed, the percentage of non-2xx responses will decrease, and the Alert will turn off by itself.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.15 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MAJOR_THRESHOLD

Table 8-150 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	Number of unsuccessful Revalidation Responses with error received from BSF when in PCF the binding association is valid session sessions is equal or above 50% but less than 70% of total Revalidation Responses.
Summary	50% to 70% of failed Revalidation Responses received from BSF over total Revalidation Responses
Severity	Major
Expression	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code!~"2.*"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.90
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	**Cause**: At least 50 % of the sent bindings revalidation requests failed with a non-2xx response. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and BSF. Maybe the Binding registration requests are not being sent, or taking too long to reach. • **Review Logs**: Check BSF's IGW and BSF MGMT logs to further investigate on why it isn't receiving its Binding Registration requests. • **Scale System Resources**: High CPU or memory usage may lead to some Binding Registration requests to not be processed. Scale pods as required by the traffic. **Recovery**: Once binding revalidation requests are properly processed, the percentage of non-2xx responses will decrease, and the Alert will turn off by itself.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.16 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MINOR_THRESHOLD

Table 8-151 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	Number of unsuccessful Revalidation Responses with error received from BSF when in PCF the binding association is valid session sessions is equal or above 30% but less than 50% of total Revalidation Responses
Summary	30% to 50% of failed Revalidation Responses received from BSF over total Revalidation Responses
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code!~"2.*"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.90
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	**Cause**: At least 30 % of the sent bindings revalidation requests failed with a non-2xx response. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and BSF. Maybe the Binding registration requests are not being sent, or taking too long to reach. • **Review Logs**: Check BSF's IGW and BSF MGMT logs to further investigate on why it isn't receiving its Binding Registration requests. • **Scale System Resources**: High CPU or memory usage may lead to some Binding Registration requests to not be processed. Scale pods as required by the traffic. **Recovery**: Once binding revalidation requests are properly processed, the percentage of non-2xx responses will decrease, and the Alert will turn off by itself.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.17 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT

Table 8-152 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Description	Primary Key lookup failed is equal or above 10% but less than 50% of total PA create.
Summary	Primary Key lookup failed is equal or above 10% but less than 50% of total PA create.
Severity	Minor
Expression	sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total{status="failed"}[30m])) / sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total[30m])) * 100 >= 10 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.124
Metric Used	occnp_optimized_smpolicyassociation_lookup_query_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-152 (Cont.)
N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Recommended Actions	**Cause**: Metric `occnp_optimized_smpolicyassociation_lookup_query_total` will increment only when **ENABLE_N7_SESSION_LOOKUP_COOKIE** flag is enabled at SM service and AAR-I comes with custom AVP and primary key lookup happens. • Metrics: `occnp_optimized_smpolicyassociation_lookup_query_total` – This will increment only when ENABLE_N7_SESSION_LOOKUP_COOKIE flag is enabled at SM service and AAR-I comes with custom AVP and primary key lookup happens. • Alarm Condition: – If Primary lookup fails for more than or equal to 10% but less than 50% of the total PA Create received. **Diagnostic Information**: • Check Network Latency – Investigate possible delays in network between PCF/BSF/AF • Verify sender information – Verify if PA Create (from AF) is sending the correct information in the headers (cookies) • Verify NFs that are affected by the flow – Verify healthy status of BSF and AF – Verify E2E flow if BSF is receiving from PCF(SM) the headers cookie, if AF is sending in Rx-Create/PaCreate the headers cookie • Review application – Verify if Sm/Diam-Connector/Diam-Gw are not congested – Signs like constant error logs are showing in services – Monitor System/resource utilization (CPU, Memory, queues) • Monitor Dashboard – Monitor the following metric `occnp_optimized_smpolicyassociation_lookup_query_total` • Monitor DB – Verify healthy status of DB – Latency in DB operation **Recover**: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF (BSF or AF) and SM Service, Diam-Connector and Diam-Gw at PCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-152 (Cont.) N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
	– Resolve any high latency or packet loss immediately if detected. • Review SM Service and Diam-Connector Application and Resources – Restart or scale up resources temporarily if the system is overloaded • Disable feature – If this flow is the only one affected, disable this feature as a last option.

8.1.2.18 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT

Table 8-153 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Description	Primary Key lookup failed is equal or above 50% but less than 75% of total PA create.
Summary	Primary Key lookup failed is equal or above 50% but less than 75% of total PA create.
Severity	Major
Expression	sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total{status="failed"}[30m])) / sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total[30m])) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.124
Metric Used	occnp_optimized_smpolicyassociation_lookup_query_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-153 (Cont.)
N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Recommended Actions	**Cause**: Metric `occnp_optimized_smpolicyassociation_lookup_query_total` will increment only when **ENABLE_N7_SESSION_LOOKUP_COOKIE** flag is enabled at SM service and AAR-I comes with custom AVP and primary key lookup happens. • Metrics: `occnp_optimized_smpolicyassociation_lookup_query_total` – This will increment only when ENABLE_N7_SESSION_LOOKUP_COOKIE flag is enabled at SM service and AAR-I comes with custom AVP and primary key lookup happens. • Alarm Condition: – If Primary lookup fails for more than or equal to 50% but less than 75% of the total PA Create received. **Diagnostic Information**: • Check Network Latency – Investigate possible delays in network between PCF/BSF/AF • Verify sender information – Verify if PA Create (from AF) is sending the correct information in the headers (cookies) • Verify NFs that are affected by the flow – Verify healthy status of BSF and AF – Verify E2E flow if BSF is receiving from PCF(SM) the headers cookie, if AF is sending in Rx-Create/PaCreate the headers cookie • Review application – Verify if Sm/Diam-Connector/Diam-Gw are not congested – Signs like constant error logs are showing in services – Monitor System/resource utilization (CPU, Memory, queues) • Monitor Dashboard – Monitor the following metric `occnp_optimized_smpolicyassociation_lookup_query_total` • Monitor DB – Verify healthy status of DB – Latency in DB operation **Recover**: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF (BSF or AF) and SM Service, Diam-Connector and Diam-Gw at PCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-153 (Cont.) N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
	– Resolve any high latency or packet loss immediately if detected. • Review SM Service and Diam-Connector Application and Resources – Restart or scale up resources temporarily if the system is overloaded • Disable feature – If this flow is the only one affected, disable this feature as a last option.

8.1.2.19 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

Table 8-154 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Description	Primary Key lookup failed is equal or above 75% of total PA create.
Summary	Primary Key lookup failed is equal or above 75% of total PA create
Severity	Critical
Expression	sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total{status="failed"}[30m])) / sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total[30m])) * 100 >= 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.124
Metric Used	occnp_optimized_smpolicyassociation_lookup_query_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-154 (Cont.)
N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Recommended Actions	**Cause**: Metric `occnp_optimized_smpolicyassociation_lookup_query_total` will increment only when **ENABLE_N7_SESSION_LOOKUP_COOKIE** flag is enabled at SM service and AAR-I comes with custom AVP and primary key lookup happens. • Metrics: `occnp_optimized_smpolicyassociation_lookup_query_total` – This will increment only when ENABLE_N7_SESSION_LOOKUP_COOKIE flag is enabled at SM service and AAR-I comes with custom AVP and primary key lookup happens. • Alarm Condition: – If Primary lookup fails for more than or equal to 75% of the total PA Create received. **Diagnostic Information**: • Check Network Latency – Investigate possible delays in network between PCF/BSF/AF • Verify sender information – Verify if PA Create (from AF) is sending the correct information in the headers (cookies) • Verify NFs that are affected by the flow – Verify healthy status of BSF and AF – Verify E2E flow if BSF is receiving from PCF(SM) the headers cookie, if AF is sending in Rx-Create/PaCreate the headers cookie • Review application – Verify if Sm/Diam-Connector/Diam-Gw are not congested – Signs like constant error logs are showing in services – Monitor System/resource utilization (CPU, Memory, queues) • Monitor Dashboard – Monitor the following metric `occnp_optimized_smpolicyassociation_lookup_query_total` • Monitor DB – Verify healthy status of DB – Latency in DB operation **Recover**: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF (BSF or AF) and SM Service, Diam-Connector and Diam-Gw at PCF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-154 (Cont.)
N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
	– Resolve any high latency or packet loss immediately if detected. • Review SM Service and Diam-Connector Application and Resources – Restart or scale up resources temporarily if the system is overloaded • Disable feature – If this flow is the only one affected, disable this feature as a last option.

8.1.2.20 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MINOR

Table 8-155 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MINOR

Field	Details
Description	At least 10% of the received requests have been cancelled due to Overload state of PCF-SM service.
Summary	At least 10% of the received Requests have been rejected due to Overload state of pcf-sm service in namespace {{$labels.namespace}}
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_enhanced_overload_reject_total{microservice=~".*pcf_sm"}[2m])) / (sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0) + (sum by (namespace) (rate(session_oam_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0)))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.125
Metric Used	• occnp_enhanced_overload_reject_total • ocpm_ingress_request_total • session_oam_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-155 (Cont.) SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MINOR

Field	Details
Recommended Actions	**Cause**: occnp_enhanced_overload_reject_total metric gets pegged whenever a rejection is performed by sm-service. This alert accounts all the incoming traffic and tells the extent of rejection. If, for a given namespace, any of the metric is absent in denominator (that is, session_oam_request_total/ ocpm_ingress_request_total), it's value will be considered zero(0) by default as per "or on(namespace) {...}" clause used in the expression. **Diagnostic information**: To monitor the individual rejection percentage by each interface type and operation type, please monitor the grafana dashboard with metric `occnp_enhanced_overload_reject_total` and dimensions operationType, interfaceType and loadLevel. **Recovery**: Whenever the alert is raised, please go to grafana to check which interfaceType/operationType is being rejected the most. If that extent of rejection is not desired for the given interfaceType/ operationType and current load level, customer may need to update the overload profile configurations accordingly.

8.1.2.21 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR

Table 8-156 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR

Field	Details
Description	At least 20 % of the received requests have been cancelled due to Overload state of PCF-SM service.
Summary	At least 20% of the received Requests have been rejected due to Overload state of pcf-sm service in namespace {{$labels.namespace}}
Severity	Major
Expression	(sum by (namespace) (rate(occnp_enhanced_overload_reject_total{microservice=~".*pcf_sm"}[2m])) / (sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0) + (sum by (namespace) (rate(session_oam_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0)))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.125

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-156 (Cont.) SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR

Field	Details
Metric Used	• occnp_enhanced_overload_reject_total • ocpm_ingress_request_total • session_oam_request_total
Recommended Actions	**Cause**: occnp_enhanced_overload_reject_total metric gets pegged whenever a rejection is performed by sm-service. This alert accounts all the incoming traffic and tells the extent of rejection. If, for a given namespace, any of the metric is absent in denominator (that is, session_oam_request_total/ ocpm_ingress_request_total), it's value will be considered zero(0) by default as per "or on(namespace) {...}" clause used in the expression. **Diagnostic information**: To monitor the individual rejection percentage by each interface type and operation type, please monitor the grafana dashboard with metric `occnp_enhanced_overload_reject_total` and dimensions operationType, interfaceType and loadLevel. **Recovery**: Whenever the alert is raised, please go to grafana to check which interfaceType/operationType is being rejected the most. If that extent of rejection is not desired for the given interfaceType/ operationType and current load level, customer may need to update the overload profile configurations accordingly.

8.1.2.22 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_CRITICAL

Table 8-157 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_CRITICAL

Field	Details
Description	At least 30 % of the received requests have been cancelled due to Overload state of PCF-SM service.
Summary	At least 30% of the received Requests have been rejected due to Overload state of pcf-sm service in namespace {{$labels.namespace}}.
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-157 (Cont.) SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_CRITICAL

Field	Details
Expression	(sum by (namespace) (rate(occnp_enhanced_overload_reject_total{microservice=~".*pcf_sm"}[2m])) / (sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0) + (sum by (namespace) (rate(session_oam_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0)))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.125
Metric Used	• occnp_enhanced_overload_reject_total • ocpm_ingress_request_total • session_oam_request_total
Recommended Actions	**Cause**: occnp_enhanced_overload_reject_total metric gets pegged whenever a rejection is performed by sm-service. This alert accounts all the incoming traffic and tells the extent of rejection. If, for a given namespace, any of the metric is absent in denominator (that is, session_oam_request_total/ ocpm_ingress_request_total), it's value will be considered zero(0) by default as per "or on(namespace) {...}" clause used in the expression. **Diagnostic information**: To monitor the individual rejection percentage by each interface type and operation type, please monitor the grafana dashboard with metric `occnp_enhanced_overload_reject_total` and dimensions operationType, interfaceType and loadLevel. **Recovery**: Whenever the alert is raised, please go to grafana to check which interfaceType/operationType is being rejected the most. If that extent of rejection is not desired for the given interfaceType/ operationType and current load level, customer may need to update the overload profile configurations accordingly.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.23 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MINOR

Table 8-158 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MINOR

Field	Details
Description	At least 10 % of the received requests have been treated as Assume Positive due to Overload state of PCF-SM service.
Summary	For at least 10% of the received Requests, various service interactions(including UserData, SpendingLimit, PRE interaction) were skipped due to Overload state of pcf-sm service in namespace {{$labels.namespace}}
Severity	Minor
Expression	((sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm",interfaceType="Npcf_SMPolicyControl"}[5m])) - (sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm",interfaceType="Npcf_SMPolicyControl",userData="true",spendingLimitData="true",policyEvaluation="true"}[5m])) or sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm"}[5m])) * 0))) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm",servicename_3gpp="npcf-smpolicycontrol"}[5m])) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.126
Metric Used	• occnp_enhanced_overload_service_interaction_total • ocpm_ingress_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-158 (Cont.)
SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MINOR

Field	Details
Recommended Actions	**Cause**: This alert gets triggered when the percentage of requests processed with "assume positive" actions, due to system overload, exceeds a certain threshold percentage(say 30%). Specifically, it tracks instances where calls to UserData, SpendingLimit, or PolicyService are skipped by smservice because of overload conditions. When `occnp_enhanced_overload_service_skipped_total` increases, it indicates a higher frequency of assume-positive actions—meaning service interactions are being bypassed to maintain performance under heavy load. While this prevents complete service failure, excessive use indicates significant service degradation. **Diagnostic Steps**: 1. **Use Grafana Dashboard**: Check the `occnp_enhanced_overload_service_skipped_total` metric in Grafana. 2. **Review Dimensions**: Filter by operationType, interfaceType, loadLevel, and skipped operations (for example, userData, spendingLimitData, policyEvaluation). Also, review relevant message attributes such as dnn, snssai, and serviceUrn. 3. **Identify Patterns**: Note which specific operations and interface types are most affected. Use the gauge metric `occnp_service_load_level` to get the current load level of the service. Check Grafana to identify which interfaceType/ operationType has the highest skip rate. **Recovery**: • Assess if the skip rate is acceptable for the current load level. • Adjust configuration if needed: – Tune overload reject/assume-positive percentages – Enable/disable service interactions in the service profile • Disable feature entirely from SM service screen (last option).

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.24 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MAJOR

Table 8-159 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MAJOR

Field	Details
Description	At least 20 % of the received requests have been treated as Assume Positive due to Overload state of PCF-SM service.
Summary	For at least 20% of the received Requests, various service interactions(including UserData, SpendingLimit, PRE interaction) were skipped due to Overload state of pcf-sm service in namespace {{$labels.namespace}}
Severity	Major
Expression	((sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm",interfaceType="Npcf_SMPolicyControl"}[5m])) - (sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm",interfaceType="Npcf_SMPolicyControl",userData="true",spendingLimitData="true",policyEvaluation="true"}[5m])) or sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm"}[5m])) * 0))) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm",servicename_3gpp="npcf-smpolicycontrol"}[5m])) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.126
Metric Used	• occnp_enhanced_overload_service_interaction_total • ocpm_ingress_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-159 (Cont.)
SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_MAJOR

Field	Details
Recommended Actions	**Cause**: This alert gets triggered when the percentage of requests processed with "assume positive" actions, due to system overload, exceeds a certain threshold percentage(say 30%). Specifically, it tracks instances where calls to UserData, SpendingLimit, or PolicyService are skipped by smservice because of overload conditions. When `occnp_enhanced_overload_service_skipped_total` increases, it indicates a higher frequency of assume-positive actions—meaning service interactions are being bypassed to maintain performance under heavy load. While this prevents complete service failure, excessive use indicates significant service degradation. **Diagnostic Steps**: 1. **Use Grafana Dashboard**: Check the `occnp_enhanced_overload_service_skipped_total` metric in Grafana. 2. **Review Dimensions**: Filter by operationType, interfaceType, loadLevel, and skipped operations (for example, userData, spendingLimitData, policyEvaluation). Also, review relevant message attributes such as dnn, snssai, and serviceUrn. 3. **Identify Patterns**: Note which specific operations and interface types are most affected. Use the gauge metric `occnp_service_load_level` to get the current load level of the service. Check Grafana to identify which interfaceType/ operationType has the highest skip rate. **Recovery**: • Assess if the skip rate is acceptable for the current load level. • Adjust configuration if needed: – Tune overload reject/assume-positive percentages – Enable/disable service interactions in the service profile • Disable feature entirely from SM service screen (last option).

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.25 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_CRITICAL

Table 8-160 SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_CRITICAL

Field	Details
Description	At least 30 % of the received Requests have been treated as Assume Positive due to Overload state of PCF-SM service
Summary	For at least 30% of the received Requests, various service interactions(including UserData, SpendingLimit, PRE interaction) were skipped due to Overload state of pcf-sm service in namespace {{$labels.namespace}}
Severity	Critical
Expression	((sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm",interfaceType="Npcf_SMPolicyControl"}[5m])) - (sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm",interfaceType="Npcf_SMPolicyControl",userData="true",spendingLimitData="true",policyEvaluation="true"}[5m])) or sum by (namespace) (rate(occnp_enhanced_overload_service_interaction_total{microservice=~".*pcf_sm"}[5m])) * 0))) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm",servicename_3gpp="npcf-smpolicycontrol"}[5m])) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.126
Metric Used	• occnp_enhanced_overload_service_interaction_total • ocpm_ingress_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-160 (Cont.)
SM_SVC_REQ_ENHANCED_OVERLOAD_SERVICE_INTERACTION_SKIPPED_CRITICAL

Field	Details
Recommended Actions	**Cause**: This alert gets triggered when the percentage of requests processed with "assume positive" actions, due to system overload, exceeds a certain threshold percentage(say 30%). Specifically, it tracks instances where calls to UserData, SpendingLimit, or PolicyService are skipped by smservice because of overload conditions. When `occnp_enhanced_overload_service_skipped_total` increases, it indicates a higher frequency of assume-positive actions—meaning service interactions are being bypassed to maintain performance under heavy load. While this prevents complete service failure, excessive use indicates significant service degradation. **Diagnostic Steps**: 1. **Use Grafana Dashboard**: Check the `occnp_enhanced_overload_service_skipped_total` metric in Grafana. 2. **Review Dimensions**: Filter by operationType, interfaceType, loadLevel, and skipped operations (for example, userData, spendingLimitData, policyEvaluation). Also, review relevant message attributes such as dnn, snssai, and serviceUrn. 3. **Identify Patterns**: Note which specific operations and interface types are most affected. Use the gauge metric `occnp_service_load_level` to get the current load level of the service. Check Grafana to identify which interfaceType/ operationType has the highest skip rate. **Recovery**: • Assess if the skip rate is acceptable for the current load level. • Adjust configuration if needed: – Tune overload reject/assume-positive percentages – Enable/disable service interactions in the service profile • Disable feature entirely from SM service screen (last option).

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.26 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Table 8-161 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timer capacity has been occupied for n1n2 transfer failure notification
Summary	More than 70% of timer capacity has been occupied for n1n2 transfer failure notification
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2TransferFailure"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.107
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-161 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer failure notification reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer failure notification and possibly enable re-transmission. **Cause:** This alert indicates sustained high utilization of the UE N1N2 Transfer Failure Notification timer pool. The occnp_timer_capacity gauge tracks the current number of outstanding timers per timerName, updated every timer scan. • These timers are created when the UE cannot deliver URSP rules and the system initiates a reattempt flow using backoff with a timer. High utilization suggests many failures are triggering the N1N2 transfer failure notification flow. • The alert notifies when utilization for timerName "UE_N1N2TransferFailure" exceeds 70% of a baseline capacity of 360,000. Dimensions: timerName: UE_N1N2TransferFailure namespace: as per Prometheus label used in aggregation siteId: underlying metric label; rule aggregates with max by (namespace) **Diagnostic Information:** 1. **Validate the alert metric:** Inspect occnp_timer_capacity{timerName="UE_N1N2TransferFailure"} in Prometheus/Grafana (and /actuator/prometheus) and review trends around the alert window. 2. **Correlate with triggering failures:** Check for spikes in N1N2 transfer failure notifications and URSP delivery failures within the same time window. 3. **Review logs around the alert window:** In PCF-UE and related components/egress, look for errors leading to N1N2 transfer failure notifications; align timestamps with the alert period. 4. **Verify retransmission/backoff settings:** Ensure retransmission is enabled; confirm backoff parameters are appropriate (not overly conservative). 5. **Check downstream/egress health:** Validate connectivity and response health for AMF or upstream endpoints; look for elevated error rates/timeouts. 6. **Confirm processing throughput:** Verify rate_per_second for this timerName, worker thread health, and pod readiness/liveness; ensure backlog is draining. 7. **Watch for capacity rejections:** Observe occnp_timer_create_failure_total{timerName="UE_N1N2TransferFailure", errorCause="TIMER_CAPACITY_EXCEEDS"} for signs of hard-cap hits. **Recovery:** 1. **Resolve underlying failures:**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-161 (Cont.) AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Field	Details
	Work with upstream/AMF and correct misconfigurations causing the flow to trigger N1N2 transfer failure notifications at high rates. 2. **Enable or optimize retransmission:** Turn on retransmission if disabled; tune backoff to improve success while avoiding downstream overload. 3. **Increase draining capacity:** Temporarily raise rate_per_second and/or scale pods to drain outstanding timers faster. 4. **Adjust capacity if needed:** Temporarily increase the registered timer_capacity baseline for this timerName while addressing root causes. 5. **Reduce new load temporarily:** Throttle or defer non-critical timer creates for this timerName until utilization drops. 6. **Monitor until recovered:** Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold.

8.1.2.27 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Table 8-162 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for n1n2 transfer failure notification
Summary	More than 80% of timer capacity has been occupied for n1n2 transfer failure notification
Severity	Major
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2TransferFailure"})/360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.107
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-162 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer failure notification reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer failure notification and possibly enable re-transmission. **Cause:** This alert indicates sustained high utilization of the UE N1N2 Transfer Failure Notification timer pool. The occnp_timer_capacity gauge tracks the current number of outstanding timers per timerName, updated every timer scan. - These timers are created when the UE cannot deliver URSP rules and the system initiates a reattempt flow using backoff with a timer. High utilization suggests many failures are triggering the N1N2 transfer failure notification flow. - The alert notifies when utilization for timerName "UE_N1N2TransferFailure" exceeds 80% of a baseline capacity of 360000. Dimensions: timerName : UE_N1N2TransferFailure namespace : as per Prometheus label used in aggregation siteId : underlying metric label; rule aggregates with max by (namespace) **Diagnostic Information :** 1. **Validate the alert metric:** Inspect occnp_timer_capacity{timerName="UE_N1N2TransferFailure"} in Prometheus/Grafana (and /actuator/prometheus) and review trends around the alert window. 2. **Correlate with triggering failures:** Check for spikes in N1N2 transfer failure notifications and URSP delivery failures within the same time window. 3. **Review logs around the alert window:** In PCF-UE and related components/egress, look for errors leading to N1N2 transfer failure notifications; align timestamps with the alert period. 4. **Verify retransmission/backoff settings:** Ensure retransmission is enabled; confirm backoff parameters are appropriate (not overly conservative). 5. **Check downstream/egress health:** Validate connectivity and response health for AMF or upstream endpoints; look for elevated error rates/timeouts. 6. **Confirm processing throughput:** Verify rate_per_second for this timerName, worker thread health, and pod readiness/liveness; ensure backlog is draining. 7. **Watch for capacity rejections:** Observe occnp_timer_create_failure_total{timerName="UE_N1N2TransferFailure",errorCause="TIMER_CAPACITY_EXCEEDS"} for signs of hard-cap hits. **Recovery :**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-162 (Cont.) AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Field	Details
	1. **Resolve underlying failures:** Work with upstream/AMF and correct misconfigurations causing the flow to trigger N1N2 transfer failure notifications at high rates. 2. **Enable or optimize retransmission:** Turn on retransmission if disabled; tune backoff to improve success while avoiding downstream overload. 3. **Increase draining capacity:** Temporarily raise rate_per_second and/or scale pods to drain outstanding timers faster. 4. **Adjust capacity if needed:** Temporarily increase the registered timer_capacity baseline for this timerName while addressing root causes. 5. **Reduce new load temporarily:** Throttle or defer non-critical timer creates for this timerName until utilization drops. 6. **Monitor until recovered:** Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold.

8.1.2.28 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Table 8-163 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD
Description	More than 90% of timer capacity has been occupied for n1n2 transfer failure notification
Summary	More than 90% of timer capacity has been occupied for n1n2 transfer failure notification
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2TransferFailure"})/360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.107
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-163 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer failure notification reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer failure notification and possibly enable re-transmission. **Cause:** This alert indicates sustained high utilization of the UE N1N2 Transfer Failure Notification timer pool. The occnp_timer_capacity gauge tracks the current number of outstanding timers per timerName, updated every timer scan. - These timers are created when the UE cannot deliver URSP rules and the system initiates a reattempt flow using backoff with a timer. High utilization suggests many failures are triggering the N1N2 transfer failure notification flow. - The alert notifies when utilization for timerName "UE_N1N2TransferFailure" exceeds 90% of a baseline capacity of 360000. Dimensions: timerName : UE_N1N2TransferFailure namespace : as per Prometheus label used in aggregation siteId : underlying metric label; rule aggregates with max by (namespace) **Diagnostic Information :** 1. **Validate the alert metric:** Inspect occnp_timer_capacity{timerName="UE_N1N2TransferFailure"} in Prometheus/Grafana (and /actuator/prometheus) and review trends around the alert window. 2. **Correlate with triggering failures:** Check for spikes in N1N2 transfer failure notifications and URSP delivery failures within the same time window. 3. **Review logs around the alert window:** In PCF-UE and related components/egress, look for errors leading to N1N2 transfer failure notifications; align timestamps with the alert period. 4. **Verify retransmission/backoff settings:** Ensure retransmission is enabled; confirm backoff parameters are appropriate (not overly conservative). 5. **Check downstream/egress health:** Validate connectivity and response health for AMF or upstream endpoints; look for elevated error rates/timeouts. 6. **Confirm processing throughput:** Verify rate_per_second for this timerName, worker thread health, and pod readiness/liveness; ensure backlog is draining. 7. **Watch for capacity rejections:** Observe occnp_timer_create_failure_total{timerName="UE_N1N2TransferFailure",errorCause="TIMER_CAPACITY_EXCEEDS"} for signs of hard-cap hits. **Recovery :**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-163 (Cont.) AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Field	Details
	1. **Resolve underlying failures:** Work with upstream/AMF and correct misconfigurations causing the flow to trigger N1N2 transfer failure notifications at high rates. 2. **Enable or optimize retransmission:** Turn on retransmission if disabled; tune backoff to improve success while avoiding downstream overload. 3. **Increase draining capacity:** Temporarily raise rate_per_second and/or scale pods to drain outstanding timers faster. 4. **Adjust capacity if needed:** Temporarily increase the registered timer_capacity baseline for this timerName while addressing root causes. 5. **Reduce new load temporarily:** Throttle or defer non-critical timer creates for this timerName until utilization drops. 6. **Monitor until recovered:** Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold.

8.1.2.29 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD

Table 8-164 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timers capacity has been occupied for amf discovery.
Summary	More than 70% of timers capacity has been occupied for amf discovery.
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_AMFDiscovery"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.95
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-164 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to AMF discovery reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with NRF discovery and possibly enable direct or indirect alternate routing from NRF client. **Cause:** More than 70% of timer capacity has been occupied for AMF discovery. The `occnp_timer_capacity` metric records the current timer count. These timers are created when the User Equipment (UE) cannot deliver URSP rules, retries with a back-off, and creates a timer. This alert is triggered when capacity for timers corresponding to AMF Discovery reaches a certain percent (over 70%) of the total 360K capacity. **Diagnostic Information:** • **High Rate of UE Failures**: Many User Equipment (UE) devices are unable to deliver URSP (User Route Selection Policy) rules, causing increased retries and timer creation for AMF discovery. • **Network Function (NRF or AMF) Issues**: Problems or instability with the AMF (Access and Mobility Management Function) or related NRF (Network Repository Function) components might prevent successful discovery or rule delivery, resulting in more timer retries. • **Resource Bottlenecks**: Network resource constraints or congestion could delay or prevent successful URSP rule delivery, again resulting in repeated retries and high timer usage. • **Excessively Short Timer Values**: If the back-off or retry timers are set too short, UEs may repeat attempts too rapidly, compounding timer consumption. **Recovery:** • Review the logs and monitor for trends in UE failures with AMF discovery. • Consider enabling direct or indirect alternate routing from the NRF-client to mitigate timer capacity issues. • Investigate any recent configuration or software changes, check for network health (especially AMF and NRF), and verify timer-related configurations. • If the issue persists, please check with Support team.

8.1.2.30 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD

Table 8-165 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for amf discovery.
Summary	More than 80% of timer capacity has been occupied for amf discovery.
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-165 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD

Field	Details
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_AMFDiscovery"})/ 360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.95
Metric Used	occnp_timer_capacity
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to AMF discovery reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with NRF discovery and possibly enable direct or indirect alternate routing from NRF client. **Cause:** More than 80% of timer capacity has been occupied for AMF discovery. The `occnp_timer_capacity` metric records the current timer count. These timers are created when the User Equipment (UE) cannot deliver URSP rules, retries with a back-off, and creates a timer. This alert is triggered when capacity for timers corresponding to AMF Discovery reaches a certain percent (over 80%) of the total 360K capacity. **Diagnostic Information:** • **High Rate of UE Failures**: Many User Equipment (UE) devices are unable to deliver URSP (User Route Selection Policy) rules, causing increased retries and timer creation for AMF discovery. • **Network Function (NRF or AMF) Issues**: Problems or instability with the AMF (Access and Mobility Management Function) or related NRF (Network Repository Function) components might prevent successful discovery or rule delivery, resulting in more timer retries. • **Resource Bottlenecks**: Network resource constraints or congestion could delay or prevent successful URSP rule delivery, again resulting in repeated retries and high timer usage. • **Excessively Short Timer Values**: If the back-off or retry timers are set too short, UEs may repeat attempts too rapidly, compounding timer consumption. **Recovery:** • Review the logs and monitor for trends in UE failures with AMF discovery. • Consider enabling direct or indirect alternate routing from the NRF-client to mitigate timer capacity issues. • Investigate any recent configuration or software changes, check for network health (especially AMF and NRF), and verify timer-related configurations. • If the issue persists, please check with Support team.

8.1.2.31 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Table 8-166 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-166 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	More than 90% of timer capacity has been occupied for amf discovery.
Summary	More than 90% of timer capacity has been occupied for amf discovery.
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_AMFDiscovery"})/ 360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.95
Metric Used	occnp_timer_capacity
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to AMF discovery reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with NRF discovery and possibly enable direct or indirect alternate routing from NRF client. **Cause:** More than 90% of timer capacity has been occupied for AMF discovery. The `occnp_timer_capacity` metric records the current timer count. These timers are created when the User Equipment (UE) cannot deliver URSP rules, retries with a back-off, and creates a timer. This alert is triggered when capacity for timers corresponding to AMF Discovery reaches a certain percent (over 90%) of the total 360K capacity. **Diagnostic Information:** • **High Rate of UE Failures**: Many User Equipment (UE) devices are unable to deliver URSP (User Route Selection Policy) rules, causing increased retries and timer creation for AMF discovery. • **Network Function (NRF or AMF) Issues**: Problems or instability with the AMF (Access and Mobility Management Function) or related NRF (Network Repository Function) components might prevent successful discovery or rule delivery, resulting in more timer retries. • **Resource Bottlenecks**: Network resource constraints or congestion could delay or prevent successful URSP rule delivery, again resulting in repeated retries and high timer usage. • **Excessively Short Timer Values**: If the back-off or retry timers are set too short, UEs may repeat attempts too rapidly, compounding timer consumption. **Recovery:** • Review the logs and monitor for trends in UE failures with AMF discovery. • Consider enabling direct or indirect alternate routing from the NRF-client to mitigate timer capacity issues. • Investigate any recent configuration or software changes, check for network health (especially AMF and NRF), and verify timer-related configurations. • If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.32 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD

Table 8-167 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timer capacity has been occupied for n1n2 subscribe.
Summary	More than 70% of timer capacity has been occupied for n1n2 subscribe.
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageSubscribe"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.96
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-167 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 subscribe reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 subscription or on the AMF side and possibly enable the direct/indirect alternate routing. **Cause:** More than 70% of timer capacity has been occupied for N1N2 subscription. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after back-off, and creates a new timer. This alert is triggered when timer capacity for N1N2 subscription exceeds 70% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Subscription Flows:** Multiple User Equipment (UE) devices may be repeatedly failing to complete N1N2 subscription actions, resulting in retries and new timer creations. • **Persistent Delivery or Communication Issues:** Failures in delivering URSP rules or problems communicating with the AMF or other network functions might cause UEs to retrigger the N1N2 subscription flow. • **Underlying AMF or Network Instability:** Instability, health issues, or misconfigurations in the AMF (Access and Mobility Management Function) could prevent successful subscription completion, leading to increased timers. • **High Traffic Volume or Spikes:** Unexpectedly high volumes of N1N2 subscription requests can cause a large number of timers to be in use concurrently. • **Resource Limitations or Performance Bottlenecks:** Processing delays or resource bottlenecks (CPU, memory, network) within the UE-service or supporting backend could slow down or block subscription handling, causing timers to accumulate. • **Improper Timer or Retry Configuration:** Short retry intervals or misconfigured back-off could lead to rapid, repeated subscription attempts and excessive timer usage. **Recovery:** • Review logs and N1N2 subscription flow metrics for unusual error patterns. • Investigate AMF and related network function health and recent changes. • Check configuration for timer parameters and adjust if necessary. • Monitor for spikes in traffic or unusual load patterns. • If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.33 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD

Table 8-168 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for n1n2 subscribe.
Summary	More than 80% of timer capacity has been occupied for n1n2 subscribe.
Severity	Major
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageSubscribe"})/360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.96
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-168 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 subscribe reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 subscription or on the AMF side and possibly enable the direct/indirect alternate routing. **Cause:** More than 80% of timer capacity has been occupied for N1N2 subscription. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after back-off, and creates a new timer. This alert is triggered when timer capacity for N1N2 subscription exceeds 80% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Subscription Flows:** Multiple User Equipment (UE) devices may be repeatedly failing to complete N1N2 subscription actions, resulting in retries and new timer creations. • **Persistent Delivery or Communication Issues:** Failures in delivering URSP rules or problems communicating with the AMF or other network functions might cause UEs to retrigger the N1N2 subscription flow. • **Underlying AMF or Network Instability:** Instability, health issues, or misconfigurations in the AMF (Access and Mobility Management Function) could prevent successful subscription completion, leading to increased timers. • **High Traffic Volume or Spikes:** Unexpectedly high volumes of N1N2 subscription requests can cause a large number of timers to be in use concurrently. • **Resource Limitations or Performance Bottlenecks:** Processing delays or resource bottlenecks (CPU, memory, network) within the UE-service or supporting backend could slow down or block subscription handling, causing timers to accumulate. • **Improper Timer or Retry Configuration:** Short retry intervals or misconfigured back-off could lead to rapid, repeated subscription attempts and excessive timer usage. **Recovery:** • Review logs and N1N2 subscription flow metrics for unusual error patterns. • Investigate AMF and related network function health and recent changes. • Check configuration for timer parameters and adjust if necessary. • Monitor for spikes in traffic or unusual load patterns. • If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.34 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD

Table 8-169 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD
Description	More than 90% of timer capacity has been occupied for n1n2 subscribe.
Summary	More than 90% of timer capacity has been occupied for n1n2 subscribe.
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageSubscribe"})/360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.96
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-169 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 subscribe reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 subscription or on the AMF side and possibly enable the direct/indirect alternate routing. **Cause:** More than 90% of timer capacity has been occupied for N1N2 subscription. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after back-off, and creates a new timer. This alert is triggered when timer capacity for N1N2 subscription exceeds 90% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Subscription Flows:** Multiple User Equipment (UE) devices may be repeatedly failing to complete N1N2 subscription actions, resulting in retries and new timer creations. • **Persistent Delivery or Communication Issues:** Failures in delivering URSP rules or problems communicating with the AMF or other network functions might cause UEs to retrigger the N1N2 subscription flow. • **Underlying AMF or Network Instability:** Instability, health issues, or misconfigurations in the AMF (Access and Mobility Management Function) could prevent successful subscription completion, leading to increased timers. • **High Traffic Volume or Spikes:** Unexpectedly high volumes of N1N2 subscription requests can cause a large number of timers to be in use concurrently. • **Resource Limitations or Performance Bottlenecks:** Processing delays or resource bottlenecks (CPU, memory, network) within the UE-service or supporting backend could slow down or block subscription handling, causing timers to accumulate. • **Improper Timer or Retry Configuration:** Short retry intervals or misconfigured back-off could lead to rapid, repeated subscription attempts and excessive timer usage. **Recovery:** • Review logs and N1N2 subscription flow metrics for unusual error patterns. • Investigate AMF and related network function health and recent changes. • Check configuration for timer parameters and adjust if necessary. • Monitor for spikes in traffic or unusual load patterns. If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.35 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD

Table 8-170 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timer capacity has been occupied for n1n2 transfer.
Summary	More than 70% of timer capacity has been occupied for n1n2 transfer.
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageTransfer"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.97
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-170 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer subscribe reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer and possibly enable direct/ indirect alternate routing. **Cause:** More than 70% of timer capacity has been occupied for N1N2 transfer. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after a back-off, and creates a new timer. This alert is triggered when the timer capacity for N1N2 transfer exceeds 70% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Transfer Flows:** Many User Equipment (UE) devices are failing to complete N1N2 transfer operations successfully. Each failure leads to retries and the creation of new timers. • **Delivery or Communication Issues:** Persistent network issues preventing successful URSP rule delivery or failures in communication between the UE, AMF (Access and Mobility Management Function), or other relevant network functions can result in repeated N1N2 transfer attempts. • **Resource Constraints or Performance Bottlenecks:** Limited processing resources, high latency, or overload conditions (e.g., CPU/memory/network contention) can slow down or block the completion of transfer requests, causing timers to accumulate. • **High Volume of Requests:** An increased volume of N1N2 transfer requests due to network events or abnormal UE behavior can lead to a rapid consumption of available timer capacity. • **Improper Timer Configuration:** Short back-off intervals or aggressive retry settings can cause repeated rapid reattempts, increasing the number of concurrent timers. • **AMF or Other NF Instability:** Outages or instability in the AMF or related network functions may cause requests to go unprocessed, triggering continual retries from UEs. **Recovery:** • Review recent logs and metrics related to N1N2 transfer failures. • Investigate the health status of the AMF and other supporting NFs. • Check resource utilization and adjust timer back-off/retry configuration if needed. • Look for recent network changes or spikes in request volume. If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.36 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD

Table 8-171 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for n1n2 transfer.
Summary	More than 80% of timer capacity has been occupied for n1n2 transfer.
Severity	Major
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageTransfer"})/360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.97
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-171 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer subscribe reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer and possibly enable direct/ indirect alternate routing. **Cause:** More than 80% of timer capacity has been occupied for N1N2 transfer. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after a back-off, and creates a new timer. This alert is triggered when the timer capacity for N1N2 transfer exceeds 80% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Transfer Flows:** Many User Equipment (UE) devices are failing to complete N1N2 transfer operations successfully. Each failure leads to retries and the creation of new timers. • **Delivery or Communication Issues:** Persistent network issues preventing successful URSP rule delivery or failures in communication between the UE, AMF (Access and Mobility Management Function), or other relevant network functions can result in repeated N1N2 transfer attempts. • **Resource Constraints or Performance Bottlenecks:** Limited processing resources, high latency, or overload conditions (e.g., CPU/memory/network contention) can slow down or block the completion of transfer requests, causing timers to accumulate. • **High Volume of Requests:** An increased volume of N1N2 transfer requests due to network events or abnormal UE behavior can lead to a rapid consumption of available timer capacity. • **Improper Timer Configuration:** Short back-off intervals or aggressive retry settings can cause repeated rapid reattempts, increasing the number of concurrent timers. • **AMF or Other NF Instability:** Outages or instability in the AMF or related network functions may cause requests to go unprocessed, triggering continual retries from UEs. **Recovery:** • Review recent logs and metrics related to N1N2 transfer failures. • Investigate the health status of the AMF and other supporting NFs. • Check resource utilization and adjust timer back-off/retry configuration if needed. • Look for recent network changes or spikes in request volume. If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.37 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD

Table 8-172 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD
Description	More than 90% of timer capacity has been occupied for n1n2 transfer.
Summary	More than 90% of timer capacity has been occupied for n1n2 transfer.
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageTransfer"})/360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.97
Metric Used	occnp_timer_capacity

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-172 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer subscribe reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer and possibly enable direct/ indirect alternate routing. **Cause:** More than 90% of timer capacity has been occupied for N1N2 transfer. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after a back-off, and creates a new timer. This alert is triggered when the timer capacity for N1N2 transfer exceeds 90% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Transfer Flows:** Many User Equipment (UE) devices are failing to complete N1N2 transfer operations successfully. Each failure leads to retries and the creation of new timers. • **Delivery or Communication Issues:** Persistent network issues preventing successful URSP rule delivery or failures in communication between the UE, AMF (Access and Mobility Management Function), or other relevant network functions can result in repeated N1N2 transfer attempts. • **Resource Constraints or Performance Bottlenecks:** Limited processing resources, high latency, or overload conditions (e.g., CPU/memory/network contention) can slow down or block the completion of transfer requests, causing timers to accumulate. • **High Volume of Requests:** An increased volume of N1N2 transfer requests due to network events or abnormal UE behavior can lead to a rapid consumption of available timer capacity. • **Improper Timer Configuration:** Short back-off intervals or aggressive retry settings can cause repeated rapid reattempts, increasing the number of concurrent timers. • **AMF or Other NF Instability:** Outages or instability in the AMF or related network functions may cause requests to go unprocessed, triggering continual retries from UEs. **Recovery:** • Review recent logs and metrics related to N1N2 transfer failures. • Investigate the health status of the AMF and other supporting NFs. • Check resource utilization and adjust timer back-off/retry configuration if needed. • Look for recent network changes or spikes in request volume. If the issue persists, please check with Support team.

8.1.2.38 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 8-173 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of n1n2 subscribe reattempt failed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-173 (Cont.) UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Summary	More than 25% of n1n2 subscribe reattempt failed.
Severity	Minor
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",operationType="subscribe",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",operationType="subscribe"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.99
Metric Used	http_out_conn_response_total, http_out_conn_request_total
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 subscribe. If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 subscription is failing or if the AMF that request are going to is unhealthy. **Cause:** An elevated percentage of reattempt failures has been detected for UE N1N2 subscriptions. The `http_out_conn_response_total` metric increments whenever the PCF-UE receives a response for outbound messages, specifically tracking reattempts where the operation type is "subscribe" and the response code is not in the 2xx (success) range. This alert triggers when more than 25% of such reattempts fail over a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** The target AMF may be experiencing outages, heavy load, or is otherwise unhealthy, causing it to reject or fail to respond to subscription requests. • **Network Issues or Communication Failures:** Network congestion, routing problems, or transient communication errors may prevent successful delivery of N1N2 subscription requests or receipt of responses. • **Configuration Errors:** Misconfiguration of endpoints (such as incorrect URLs, authentication, or authorization settings) may cause subscription requests to be rejected or fail. • **High Load or Resource Exhaustion:** If the AMF or intermediate network components are overloaded or have run out of necessary resources (e.g., memory, threads, process slots), reattempted requests may be rejected. • **Timeouts or Latency Issues:** Prolonged delays in response times could cause requests to time out, leading to apparent failures. **Recovery:** • Review logs and error codes for patterns or specific failure reasons. • Check the health and recent activity of the AMF(s) and relevant network paths. • Examine configuration settings related to N1N2 subscriptions and ensure they are correct. • Investigate any spikes in load or indications of resource bottlenecks. • Correlate with recent changes or deployments in the environment. If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.39 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 8-174 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of n1n2 subscribe reattempt failed.
Summary	More than 50% of n1n2 subscribe reattempt failed.
Severity	Major
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",operationType="subscribe",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",operationType="subscribe"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.99
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-174 (Cont.) UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 subscribe.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 subscription is failing or if the AMF that request are going to is unhealthy. **Cause:** An elevated percentage of reattempt failures has been detected for UE N1N2 subscriptions. The `http_out_conn_response_total` metric increments whenever the PCF-UE receives a response for outbound messages, specifically tracking reattempts where the operation type is "subscribe" and the response code is not in the 2xx (success) range. This alert triggers when more than 50% of such reattempts fail over a 5-minute period. **Diagnostic Information:** **AMF (Access and Mobility Management Function) Unavailability or Instability:** The target AMF may be experiencing outages, heavy load, or is otherwise unhealthy, causing it to reject or fail to respond to subscription requests. **Network Issues or Communication Failures:** Network congestion, routing problems, or transient communication errors may prevent successful delivery of N1N2 subscription requests or receipt of responses. **Configuration Errors:** Misconfiguration of endpoints (such as incorrect URLs, authentication, or authorization settings) may cause subscription requests to be rejected or fail. **High Load or Resource Exhaustion:** If the AMF or intermediate network components are overloaded or have run out of necessary resources (e.g., memory, threads, process slots), reattempted requests may be rejected. • **Timeouts or Latency Issues:**Prolonged delays in response times could cause requests to time out, leading to apparent failures. **Recovery:** • Review logs and error codes for patterns or specific failure reasons. • Check the health and recent activity of the AMF(s) and relevant network paths. • Examine configuration settings related to N1N2 subscriptions and ensure they are correct. • Investigate any spikes in load or indications of resource bottlenecks. • Correlate with recent changes or deployments in the environment. If the issue persists, please check with Support team.

8.1.2.40 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 8-175 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of n1n2 subscribe reattempt failed.
Summary	More than 75% of n1n2 subscribe reattempt failed.
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-175 (Cont.) UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",operationType="subscribe",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",operationType="subscribe"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.99
Metric Used	http_out_conn_response_total, http_out_conn_request_total
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 subscribe.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 subscription is failing or if the AMF that request are going to is unhealthy. **Cause:** An elevated percentage of reattempt failures has been detected for UE N1N2 subscriptions. The `http_out_conn_response_total` metric increments whenever the PCF-UE receives a response for outbound messages, specifically tracking reattempts where the operation type is "subscribe" and the response code is not in the 2xx (success) range. This alert triggers when more than 75% of such reattempts fail over a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** The target AMF may be experiencing outages, heavy load, or is otherwise unhealthy, causing it to reject or fail to respond to subscription requests. • **Network Issues or Communication Failures:** Network congestion, routing problems, or transient communication errors may prevent successful delivery of N1N2 subscription requests or receipt of responses. • **Configuration Errors:** Misconfiguration of endpoints (such as incorrect URLs, authentication, or authorization settings) may cause subscription requests to be rejected or fail. • **High Load or Resource Exhaustion:** If the AMF or intermediate network components are overloaded or have run out of necessary resources (e.g., memory, threads, process slots), reattempted requests may be rejected. • **Timeouts or Latency Issues:**Prolonged delays in response times could cause requests to time out, leading to apparent failures. **Recovery:** • Review logs and error codes for patterns or specific failure reasons. • Check the health and recent activity of the AMF(s) and relevant network paths. • Examine configuration settings related to N1N2 subscriptions and ensure they are correct. • Investigate any spikes in load or indications of resource bottlenecks. • Correlate with recent changes or deployments in the environment. If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.41 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 8-176 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of n1n2 transfer reattempt failed.
Summary	More than 25% of n1n2 transfer reattempt failed.
Severity	Minor
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.100
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-176 (Cont.) UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 transfer.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 message transfer is failing or if the AMF that request are going to is unhealthy. **Cause:** An increased percentage of reattempt failures has been detected for UE N1N2 message transfers. The `http_out_conn_response_total` metric increments when the PCF-UE receives a response for messages being sent out of the Network Function (NF), specifically monitoring reattempts of the "transfer" operation where the response code is not 2xx (success). This alert is triggered when over 25% of such reattempts result in failure within a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** If the target AMF is down, overloaded, or behaving unpredictably, message transfer requests (especially retries) are more likely to fail. • **Network Path Issues:** Transient or persistent network failures, high latency, or packet loss between the PCF-UE and the target network function can disrupt the successful transfer of N1N2 messages. • **Configuration Errors:** Misconfiguration in endpoints, credentials, or other protocol parameters can cause messages to be consistently rejected or fail to deliver. • **System Resource Constraints:** Resource exhaustion (CPU, memory, file descriptors, etc.) on either the PCF-UE or the AMF could prevent successful handling of transfer requests. • **Timeouts and Slow Processing:** Delayed responses or timeouts can be interpreted as failures, particularly if the operation times out consistently during high load or due to backend issues. **Recovery:** • Review and analyze failure logs and returned error codes. • Check the operational health and resource status of the AMF and other involved NFs. • Validate network connectivity and latency between all relevant components. • Inspect configuration and recent changes for potential misalignments. • Correlate the timing of increased failures with network incidents, maintenance windows, or new deployments. If the issue persists, please check with Support team.

8.1.2.42 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 8-177 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of n1n2 transfer reattempt failed.
Summary	More than 50% of n1n2 transfer reattempt failed.
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-177 (Cont.) UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.100
Metric Used	http_out_conn_response_total, http_out_conn_request_total
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 transfer.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 message transfer is failing or if the AMF that request are going to is unhealthy. **Cause:** An increased percentage of reattempt failures has been detected for UE N1N2 message transfers. The `http_out_conn_response_total` metric increments when the PCF-UE receives a response for messages being sent out of the Network Function (NF), specifically monitoring reattempts of the "transfer" operation where the response code is not 2xx (success). This alert is triggered when over 50% of such reattempts result in failure within a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** If the target AMF is down, overloaded, or behaving unpredictably, message transfer requests (especially retries) are more likely to fail. • **Network Path Issues:** Transient or persistent network failures, high latency, or packet loss between the PCF-UE and the target network function can disrupt the successful transfer of N1N2 messages. • **Configuration Errors:** Misconfiguration in endpoints, credentials, or other protocol parameters can cause messages to be consistently rejected or fail to deliver. • **System Resource Constraints:** Resource exhaustion (CPU, memory, file descriptors, etc.) on either the PCF-UE or the AMF could prevent successful handling of transfer requests. • **Timeouts and Slow Processing:** Delayed responses or timeouts can be interpreted as failures, particularly if the operation times out consistently during high load or due to backend issues. **Recovery:** • Review and analyze failure logs and returned error codes. • Check the operational health and resource status of the AMF and other involved NFs. • Validate network connectivity and latency between all relevant components. • Inspect configuration and recent changes for potential misalignments. • Correlate the timing of increased failures with network incidents, maintenance windows, or new deployments. If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.43 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 8-178 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of n1n2 transfer reattempt failed.
Summary	More than 75% of n1n2 transfer reattempt failed.
Severity	Critical
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.100
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-178 (Cont.) UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 transfer.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 message transfer is failing or if the AMF that request are going to is unhealthy. **Cause:** An increased percentage of reattempt failures has been detected for UE N1N2 message transfers. The `http_out_conn_response_total` metric increments when the PCF-UE receives a response for messages being sent out of the Network Function (NF), specifically monitoring reattempts of the "transfer" operation where the response code is not 2xx (success). This alert is triggered when over 75% of such reattempts result in failure within a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** If the target AMF is down, overloaded, or behaving unpredictably, message transfer requests (especially retries) are more likely to fail. • **Network Path Issues:** Transient or persistent network failures, high latency, or packet loss between the PCF-UE and the target network function can disrupt the successful transfer of N1N2 messages. • **Configuration Errors:** Misconfiguration in endpoints, credentials, or other protocol parameters can cause messages to be consistently rejected or fail to deliver. • **System Resource Constraints:** Resource exhaustion (CPU, memory, file descriptors, etc.) on either the PCF-UE or the AMF could prevent successful handling of transfer requests. • **Timeouts and Slow Processing:** Delayed responses or timeouts can be interpreted as failures, particularly if the operation times out consistently during high load or due to backend issues. **Recovery:** • Review and analyze failure logs and returned error codes. • Check the operational health and resource status of the AMF and other involved NFs. • Validate network connectivity and latency between all relevant components. • Inspect configuration and recent changes for potential misalignments. • Correlate the timing of increased failures with network incidents, maintenance windows, or new deployments. If the issue persists, please check with Support team.

8.1.2.44 SM_STALE_REQUEST_PROCESSING_REJECT_MINOR

Table 8-179 SM_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Name in Alert Yaml File	SM_STALE_REQUEST_PROCESSING_REJECT_MINOR
Description	More than 10% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Summary	More than 10% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-179 (Cont.) SM_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Expression	(sum by (namespace,pod) (rate(occnp_late_processing_rejection_total{microservice=~"occnp_pcf_sm"}[5m])))/ (sum by (namespace,pod) (rate(ocpm_ingress_request_total{microservice=~"occnp_pcf_sm"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.101
Metric Used	occnp_late_processing_rejection_total, ocpm_ingress_request_total
Recommended Actions	The metric **occnp_late_processing_rejection_total** is pegged when Late Processing finds a stale session. **Cause:** The metric **occnp_late_processing_rejection_total** is incremented when the SM Service determines that a request has become stale. For example, if a request includes the following header parameters: • `sbiSenderTimestamp3GPP='2025-11-03T09:48:01.000Z'` (sender timestamp) • `sbiMaxRSPTime3GPP='3000'` (maximum response time in milliseconds) In this scenario, if there is a delay in receiving a response from the external Network Function (NF), a stale check is later performed. If the request is deemed stale during this check, it is counted in the metric. When more than 10% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT, then this alarm will be raised. **Diagnostic Information:** • **Validate Timestamps:** Ensure that system clocks are synchronized (e.g., via NTP). • **Analyze Latency:** Use tracing or metric data to identify bottlenecks in response time—look for patterns in external NF response delays. • **Review Configurations:** Confirm that max response times (`sbiMaxRSPTime3GPP`) are correctly set as per the service contract. • **Scale System Resources**: Check for resource constraints (CPU, memory, bandwidth) and scale up your system or services as needed to handle the incoming request load within the allowed response time. **Recovery:** Once the recommended diagnostic actions are implemented and responses from the external NF are received within the expected timeframe, the percentage of rejected messages will begin to decline, ultimately clearing the alert.

8.1.2.45 SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Table 8-180 SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Name in Alert Yaml File	SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR
Description	More than 20% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Summary	More than 20% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-180 (Cont.) SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Expression	(sum by (namespace,pod) (rate(occnp_late_processing_rejection_total{microservice=~"occnp_pcf_sm"}[5m])))/ (sum by (namespace,pod) (rate(ocpm_ingress_request_total{microservice=~"occnp_pcf_sm"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.101
Metric Used	occnp_late_processing_rejection_total, ocpm_ingress_request_total
Recommended Actions	The metric **occnp_late_processing_rejection_total** is pegged when Late Processing finds a stale session. **Cause:** The metric **occnp_late_processing_rejection_total** is incremented when the SM Service determines that a request has become stale. For example, if a request includes the following header parameters: • `sbiSenderTimestamp3GPP='2025-11-03T09:48:01.000Z'` (sender timestamp) • `sbiMaxRSPTime3GPP='3000'` (maximum response time in milliseconds) In this scenario, if there is a delay in receiving a response from the external Network Function (NF), a stale check is later performed. If the request is deemed stale during this check, it is counted in the metric. When more than 20% and less than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT, then this alarm will be raised. **Diagnostic Information:** • **Validate Timestamps:** Ensure that system clocks are synchronized (e.g., via NTP). • **Analyze Latency:** Use tracing or metric data to identify bottlenecks in response time—look for patterns in external NF response delays. • **Review Configurations:** Confirm that max response times (`sbiMaxRSPTime3GPP`) are correctly set as per the service contract. • **Scale System Resources**: Check for resource constraints (CPU, memory, bandwidth) and scale up your system or services as needed to handle the incoming request load within the allowed response time. **Recovery:** Once the recommended diagnostic actions are implemented and responses from the external NF are received within the expected timeframe, the percentage of rejected messages will begin to decline, ultimately clearing the alert.

8.1.2.46 SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Table 8-181 SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Name in Alert Yaml File	SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL
Description	More than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Summary	More than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-181 (Cont.) SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Expression	(sum by (namespace,pod) (rate(occnp_late_processing_rejection_total{microservice=~"occnp_pcf_sm"}[5m])))/ (sum by (namespace,pod) (rate(ocpm_ingress_request_total{microservice=~"occnp_pcf_sm"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.101
Metric Used	occnp_late_processing_rejection_total, ocpm_ingress_request_total
Recommended Actions	The metric **occnp_late_processing_rejection_total** is pegged when Late Processing finds a stale session. **Cause:** The metric **occnp_late_processing_rejection_total** is incremented when the SM Service determines that a request has become stale. For example, if a request includes the following header parameters: • `sbiSenderTimestamp3GPP='2025-11-03T09:48:01.000Z'` (sender timestamp) • `sbiMaxRSPTime3GPP='3000'` (maximum response time in milliseconds) In this scenario, if there is a delay in receiving a response from the external Network Function (NF), a stale check is later performed. If the request is deemed stale during this check, it is counted in the metric. When more than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT, then this alarm will be raised. **Diagnostic Information:** • **Validate Timestamps:** Ensure that system clocks are synchronized (e.g., via NTP). • **Analyze Latency:** Use tracing or metric data to identify bottlenecks in response time—look for patterns in external NF response delays. • **Review Configurations:** Confirm that max response times (`sbiMaxRSPTime3GPP`) are correctly set as per the service contract. • **Scale System Resources**: Check for resource constraints (CPU, memory, bandwidth) and scale up your system or services as needed to handle the incoming request load within the allowed response time. **Recovery:** Once the recommended diagnostic actions are implemented and responses from the external NF are received within the expected timeframe, the percentage of rejected messages will begin to decline, ultimately clearing the alert.

8.1.2.47 UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Table 8-182 UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Description	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Summary	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-182 (Cont.) UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.104
Metric Used	`occnp_late_processing_rejection_total`
Recommended Actions	Metric `occnp_late_processing_rejection_total` is pegged when requests being processed become stale**.** **Cause:** More than 20% of incoming requests to the ue-service have been rejected because they became stale during processing. The service flags a request as stale when its processing exceeds an acceptable time window. **Diagnostic Information:** • **High System Load or Resource Contention:** The ue-service or its backend components may be overloaded (e.g., CPU, memory, I/O), delaying request processing. • **Inefficient Request Handling or Bottlenecks:** There may be inefficiencies or slow operations within the service logic, such as database queries, API calls, or complex computations causing extended processing times. • **Network Latency or Downstream Delays:** High network latency or slow responses from dependent services or databases could increase the time required to process requests. • **Increased Volume of Requests:** A spike in incoming requests can overwhelm the service, leading to request queues and increased wait times. **Recovery:** • Monitor system and service resource utilization. • Review recent changes to workload, configuration, or deployments. • Tune timeouts and thresholds appropriately based on observed service latency. • Analyze logs to pinpoint where delays are occurring in the request processing workflow. If the issue persists, please check with Support team.

8.1.2.48 UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Table 8-183 UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Description	This alert is triggered when more than 30% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Summary	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.104

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-183 (Cont.) UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Metric Used	`occnp_late_processing_rejection_total`
Recommended Actions	Metric `occnp_late_processing_rejection_total` is pegged when requests being processed become stale**.** **Cause:** More than 30% of incoming requests to the ue-service have been rejected because they became stale during processing. The service flags a request as stale when its processing exceeds an acceptable time window. **Diagnostic Information:** • **High System Load or Resource Contention:** The ue-service or its backend components may be overloaded (e.g., CPU, memory, I/O), delaying request processing. • **Inefficient Request Handling or Bottlenecks:** There may be inefficiencies or slow operations within the service logic, such as database queries, API calls, or complex computations causing extended processing times. • **Network Latency or Downstream Delays:** High network latency or slow responses from dependent services or databases could increase the time required to process requests. • **Increased Volume of Requests:** A spike in incoming requests can overwhelm the service, leading to request queues and increased wait times. **Recovery:** • Monitor system and service resource utilization. • Review recent changes to workload, configuration, or deployments. • Tune timeouts and thresholds appropriately based on observed service latency. • Analyze logs to pinpoint where delays are occurring in the request processing workflow. If the issue persists, please check with Support team.

8.1.2.49 UE_STALE_REQUEST_PROCESSING_REJECT_MINOR

Table 8-184 UE_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Description	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Summary	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.104
Metric Used	`occnp_late_processing_rejection_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-184 (Cont.) UE_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Recommended Actions	Metric `occnp_late_processing_rejection_total` is pegged when requests being processed become stale. **Cause:** More than 10% of incoming requests to the ue-service have been rejected because they became stale during processing. The service flags a request as stale when its processing exceeds an acceptable time window. **Diagnostic Information:** • **High System Load or Resource Contention:** The ue-service or its backend components may be overloaded (e.g., CPU, memory, I/O), delaying request processing. • **Inefficient Request Handling or Bottlenecks:** There may be inefficiencies or slow operations within the service logic, such as database queries, API calls, or complex computations causing extended processing times. • **Network Latency or Downstream Delays:** High network latency or slow responses from dependent services or databases could increase the time required to process requests. • **Increased Volume of Requests:** A spike in incoming requests can overwhelm the service, leading to request queues and increased wait times. **Recovery:** • Monitor system and service resource utilization. • Review recent changes to workload, configuration, or deployments. • Tune timeouts and thresholds appropriately based on observed service latency. • Analyze logs to pinpoint where delays are occurring in the request processing workflow. If the issue persists, please check with Support team.

8.1.2.50 UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Table 8-185 UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Field	Details
Description	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Summary	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_late_arrival_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace)(rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.109
Metric Used	`ocpm_late_arrival_rejection_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-185 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Field	Details
Recommended Actions	Metric `ocpm_late_arrival_rejection_total` is pegged when a received requests is stale. **Cause:** Metric **ocpm_late_arrival_rejection_total** is pegged when a received requests is stale**.** • **Metric:** `ocpm_late_arrival_rejection_total` – Increments when the UE Service determines incoming requests are stale (arrived too late to process). – The staleness check is based on: * `3gpp-Sbi-Sender-Timestamp` (preferred) * `3gpp-Sbi-Origination-Timestamp` (fallback if sender timestamp is unavailable) * `3gpp-Sbi-Max-Rsp-Time` (maximum allowed response time, in ms) • **Request Example:** – `3gpp-Sbi-Sender-Timestamp='2025-11-03T09:48:01.000Z'` – `3gpp-Sbi-Max-Rsp-Time='3000'` (i.e., 3 seconds) • If request arrives after (Sender-Timestamp + Max-Rsp-Time), it is considered **stale** and counted in the metric. • **Alarm Condition:** – If **more than 10%** of ingress requests result in `504 GATEWAY_TIMEOUT` errors due to staleness, an alarm is raised. **Diagnostic Information:** 1. **Verify Time Synchronization** • Ensure all Network Functions (NFs) have synchronized system clocks (using NTP). • Time drift between sender and UE Service may falsely trigger staleness. 2. **Check Network Latency** • Investigate possible network delays or congestion between external NF and the UE Service. • High or unstable latency can lead to late arrival of requests. 3. **Analyze Sender Behavior** • Validate that the sending NF populates `3gpp-Sbi-Sender-Timestamp` (or Origination-Timestamp) correctly. • Misconfigured or delayed timestamping can corrupt staleness calculation. 4. **Assess Max Response Time Values** • Review if the `3gpp-Sbi-Max-Rsp-Time` value is appropriate for your network and application conditions. • Very short response times may not be feasible under current latency conditions. 5. **Review Application Load** • Monitor system/resource utilization (CPU, memory, queue lengths) on the UE Service. • Resource exhaustion may delay request processing, even if requests arrive on time. 6. **Correlation with Other Metrics** • Examine related metrics such as total request counts, processing times, error types, etc., to identify trends. • Check if certain sources or request types are consistently late. 7. **Check for Backlogs**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-185 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Field	Details
	• Review UE Service logs for any signs of backlogs, bottlenecks, or spikes in the request handling pipeline. **Recovery:** 1. **Verify Time Synchronization** • Ensure all relevant Network Functions (NFs) have correct system time. Resynchronize clocks if any drift is detected. 2. **Check Network Latency and Connectivity** • Investigate any current network issues or bottlenecks between the external NF and the UE Service. Resolve any high latency or packet loss immediately if detected. 3. **Review UE Service Application & Resources** • Check the UE Service for high CPU/memory usage or any request processing backlogs. • Restart or scale up resources temporarily if the system is overloaded. 4. **Contact Upstream NF Owners** Notify owners of external NFs if they are sending delayed or incorrectly timestamped requests so they can take corrective action.

8.1.2.51 UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Table 8-186 UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Field	Details
Description	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Summary	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_late_arrival_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace)(rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.109
Metric Used	`ocpm_late_arrival_rejection_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-186 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Field	Details
Recommended Actions	Metric `ocpm_late_arrival_rejection_total` is pegged when a received requests is stale. **Cause:** Metric **ocpm_late_arrival_rejection_total** is pegged when a received requests is stale**.** • **Metric:** `ocpm_late_arrival_rejection_total` – Increments when the UE Service determines incoming requests are stale (arrived too late to process). – The staleness check is based on: * `3gpp-Sbi-Sender-Timestamp` (preferred) * `3gpp-Sbi-Origination-Timestamp` (fallback if sender timestamp is unavailable) * `3gpp-Sbi-Max-Rsp-Time` (maximum allowed response time, in ms) • **Request Example:** – `3gpp-Sbi-Sender-Timestamp='2025-11-03T09:48:01.000Z'` – `3gpp-Sbi-Max-Rsp-Time='3000'` (i.e., 3 seconds) • If request arrives after (Sender-Timestamp + Max-Rsp-Time), it is considered **stale** and counted in the metric. • **Alarm Condition:** – If **more than 20%** of ingress requests result in `504 GATEWAY_TIMEOUT` errors due to staleness, an alarm is raised. **Diagnostic Information:** 1. **Verify Time Synchronization** • Ensure all Network Functions (NFs) have synchronized system clocks (using NTP). • Time drift between sender and UE Service may falsely trigger staleness. 2. **Check Network Latency** • Investigate possible network delays or congestion between external NF and the UE Service. • High or unstable latency can lead to late arrival of requests. 3. **Analyze Sender Behavior** • Validate that the sending NF populates `3gpp-Sbi-Sender-Timestamp` (or Origination-Timestamp) correctly. • Misconfigured or delayed timestamping can corrupt staleness calculation. 4. **Assess Max Response Time Values** • Review if the `3gpp-Sbi-Max-Rsp-Time` value is appropriate for your network and application conditions. • Very short response times may not be feasible under current latency conditions. 5. **Review Application Load** • Monitor system/resource utilization (CPU, memory, queue lengths) on the UE Service. • Resource exhaustion may delay request processing, even if requests arrive on time. 6. **Correlation with Other Metrics** • Examine related metrics such as total request counts, processing times, error types, etc., to identify trends. • Check if certain sources or request types are consistently late. 7. **Check for Backlogs**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-186 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Field	Details
	• Review UE Service logs for any signs of backlogs, bottlenecks, or spikes in the request handling pipeline. **Recovery:** 1. **Verify Time Synchronization** • Ensure all relevant Network Functions (NFs) have correct system time. Resynchronize clocks if any drift is detected. 2. **Check Network Latency and Connectivity** • Investigate any current network issues or bottlenecks between the external NF and the UE Service. Resolve any high latency or packet loss immediately if detected. 3. **Review UE Service Application & Resources** • Check the UE Service for high CPU/memory usage or any request processing backlogs. • Restart or scale up resources temporarily if the system is overloaded. 4. **Contact Upstream NF Owners** Notify owners of external NFs if they are sending delayed or incorrectly timestamped requests so they can take corrective action.

8.1.2.52 UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Table 8-187 UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Field	Details
Description	This alert is triggered when more than 30% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Summary	This alert is triggered when more than 30% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_late_arrival_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace)(rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.109
Metric Used	`ocpm_late_arrival_rejection_total`

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-187 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Field	Details
Recommended Actions	Metric `ocpm_late_arrival_rejection_total` is pegged when a received requests is stale. **Cause:** Metric **ocpm_late_arrival_rejection_total** is pegged when a received requests is stale**.** • **Metric:** `ocpm_late_arrival_rejection_total` – Increments when the UE Service determines incoming requests are stale (arrived too late to process). – The staleness check is based on: * `3gpp-Sbi-Sender-Timestamp` (preferred) * `3gpp-Sbi-Origination-Timestamp` (fallback if sender timestamp is unavailable) * `3gpp-Sbi-Max-Rsp-Time` (maximum allowed response time, in ms) • **Request Example:** – `3gpp-Sbi-Sender-Timestamp='2025-11-03T09:48:01.000Z'` – `3gpp-Sbi-Max-Rsp-Time='3000'` (i.e., 3 seconds) • If request arrives after (Sender-Timestamp + Max-Rsp-Time), it is considered **stale** and counted in the metric. • **Alarm Condition:** – If **more than 30%** of ingress requests result in `504 GATEWAY_TIMEOUT` errors due to staleness, an alarm is raised. **Diagnostic Information:** 1. **Verify Time Synchronization** • Ensure all Network Functions (NFs) have synchronized system clocks (using NTP). • Time drift between sender and UE Service may falsely trigger staleness. 2. **Check Network Latency** • Investigate possible network delays or congestion between external NF and the UE Service. • High or unstable latency can lead to late arrival of requests. 3. **Analyze Sender Behavior** • Validate that the sending NF populates `3gpp-Sbi-Sender-Timestamp` (or Origination-Timestamp) correctly. • Misconfigured or delayed timestamping can corrupt staleness calculation. 4. **Assess Max Response Time Values** • Review if the `3gpp-Sbi-Max-Rsp-Time` value is appropriate for your network and application conditions. • Very short response times may not be feasible under current latency conditions. 5. **Review Application Load** • Monitor system/resource utilization (CPU, memory, queue lengths) on the UE Service. • Resource exhaustion may delay request processing, even if requests arrive on time. 6. **Correlation with Other Metrics** • Examine related metrics such as total request counts, processing times, error types, etc., to identify trends. • Check if certain sources or request types are consistently late. 7. **Check for Backlogs**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-187 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Field	Details
	• Review UE Service logs for any signs of backlogs, bottlenecks, or spikes in the request handling pipeline. **Recovery:** 1. **Verify Time Synchronization** • Ensure all relevant Network Functions (NFs) have correct system time. Resynchronize clocks if any drift is detected. 2. **Check Network Latency and Connectivity** • Investigate any current network issues or bottlenecks between the external NF and the UE Service. Resolve any high latency or packet loss immediately if detected. 3. **Review UE Service Application & Resources** • Check the UE Service for high CPU/memory usage or any request processing backlogs. • Restart or scale up resources temporarily if the system is overloaded. 4. **Contact Upstream NF Owners** Notify owners of external NFs if they are sending delayed or incorrectly timestamped requests so they can take corrective action.

8.1.2.53 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 8-188 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of N1N2 transfer failure notification reattempts failed.
Summary	More than 75% of N1N2 transfer failure notification reattempts failed.
Severity	Critical
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.106
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-188 (Cont.) UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case the alert notifies when there is a certain amount of reattempt failure for UE N1N2 transfer failure notification. If there is an increase of failure, operator can investigate on: • Why the flow triggering N1N2 transfer failure notification is failing, or • Check the health of the AMF to which the request are going to **Cause:** http_out_conn_response_total metric with indicated dimensions is pegged when PCF-UE receives a response for an outgoing reattempt transfer request triggered for N1N2TransferFailure notification. Dimensions: IsReattempt : true reattemptType : UE_N1N2TransferFailure OperationType : transfer ResponseCode : !2xx In this case more than 75% of outgoing transfer reattempts (due to **N1N2TransferFailure** as notified by AMF) receive a non-2xx (failure) response in the last 5 minutes (or selected sample frame) **Diagnostic Information :** 1. ***Check Recent Logs***: • Analyze logs for both PCF-UE and Egress Gateway in the relevant namespace for error details (timestamps matching the period of alert). • Focus on error responses: look for 4xx/5xx HTTP responses and their reasons. 2. ***Correlate with Traffic Patterns***: • Determine if failures are for specific to certain AMFs or random. • Check if there's a sudden surge in failures (indicating a broader issue). 3. ***Inspect Network Health and Configuration***: • Ensure connectivity and correct routing between PCF-UE and its downstream targets. • Validate configurations, especially recently changed ones. 4. ***Cross-check Incident/Event Timeline***: • Review recent maintenance, deployments, or network events that could correlate with the increase in failures. 5. ***Evaluate for Service Overload***: • Examine resource metrics (CPU, memory, rate of requests) of the affected service(PCF-UE, PCF-EGW) to determine if it's under duress. 6. ***Check with Peers***: • See if corresponding namespaces (other tenants/products) are seeing similar issues, could indicate a platform or shared service problem. **Recovery :** 1. **Resolve Underlying Service Issues**: • If the upstream service (e.g., AMF or other network function) is unhealthy, work with the respective team to restore normal operation. • Address any misconfiguration or errors causing repeated non-2xx responses.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-188 (Cont.) UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
	2. **Revert Recent Changes**: • If the issue correlates with recent deployments or configuration changes, consider rolling back to the previous stable state after assessing impact. 3. **Mitigate Service Overload**: • If resource constraints are detected (CPU, memory, connections), scale up resources or reduce load by throttling non-critical requests where possible. 4. **Network Remediation**: • Resolve any detected connectivity or routing issues between PCF-UE and the egress gateway or upstream endpoints. 5. **Monitor and Confirm Recovery**: • Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold. Ensure related services in affected namespaces also recover.

8.1.2.54 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 8-189 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of N1N2 transfer failure notification reattempts failed.
Summary	More than 50% of N1N2 transfer failure notification reattempts failed.
Severity	Major
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.106
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-189 (Cont.)
UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case the alert notifies when there is a certain amount of reattempt failure for UE N1N2 transfer failure notification. If there is an increase of failure, operator can investigate on: • Why the flow triggering N1N2 transfer failure notification is failing, or • Check the health of the AMF to which the request are going to **Cause:** http_out_conn_response_total metric with indicated dimensions is pegged when PCF-UE receives a response for an outgoing reattempt transfer request triggered for N1N2TransferFailure notification. Dimensions: IsReattempt : true reattemptType : UE_N1N2TransferFailure OperationType : transfer ResponseCode : !2xx In this case more than 50% of outgoing transfer reattempts (due to **N1N2TransferFailure** as notified by AMF) receive a non-2xx (failure) response in the last 5 minutes (or selected sample frame) **Diagnostic Information :** 1. ***Check Recent Logs***: • Analyze logs for both PCF-UE and Egress Gateway in the relevant namespace for error details (timestamps matching the period of alert). • Focus on error responses: look for 4xx/5xx HTTP responses and their reasons. 2. ***Correlate with Traffic Patterns***: • Determine if failures are for specific to certain AMFs or random. • Check if there's a sudden surge in failures (indicating a broader issue). 3. ***Inspect Network Health and Configuration***: • Ensure connectivity and correct routing between PCF-UE and its downstream targets. • Validate configurations, especially recently changed ones. 4. ***Cross-check Incident/Event Timeline***: • Review recent maintenance, deployments, or network events that could correlate with the increase in failures. 5. ***Evaluate for Service Overload***: • Examine resource metrics (CPU, memory, rate of requests) of the affected service(PCF-UE, PCF-EGW) to determine if it’s under duress. 6. ***Check with Peers***: • See if corresponding namespaces (other tenants/products) are seeing similar issues, could indicate a platform or shared service problem. **Recovery :** 1. **Resolve Underlying Service Issues**: • If the upstream service (e.g., AMF or other network function) is unhealthy, work with the respective team to restore normal operation. • Address any misconfiguration or errors causing repeated non-2xx responses. 2. **Revert Recent Changes**:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-189 (Cont.) UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
	• If the issue correlates with recent deployments or configuration changes, consider rolling back to the previous stable state after assessing impact. 3. **Mitigate Service Overload**: • If resource constraints are detected (CPU, memory, connections), scale up resources or reduce load by throttling non-critical requests where possible. 4. **Network Remediation**: • Resolve any detected connectivity or routing issues between PCF-UE and the egress gateway or upstream endpoints. 5. **Monitor and Confirm Recovery**: • Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold. Ensure related services in affected namespaces also recover.

8.1.2.55 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 8-190 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of N1N2 transfer failure notification reattempts failed.
Summary	More than 25% of N1N2 transfer failure notification reattempts failed.
Severity	Minor
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.106
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-190 (Cont.)
UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case the alert notifies when there is a certain amount of reattempt failure for UE N1N2 transfer failure notification. If there is an increase of failure, operator can investigate on: • Why the flow triggering N1N2 transfer failure notification is failing, or • Check the health of the AMF to which the request are going to **Cause:** http_out_conn_response_total metric with indicated dimensions is pegged when PCF-UE receives a response for an outgoing reattempt transfer request triggered for N1N2TransferFailure notification. Dimensions: IsReattempt : true reattemptType : UE_N1N2TransferFailure OperationType : transfer ResponseCode : !2xx In this case more than 25% of outgoing transfer reattempts (due to **N1N2TransferFailure** as notified by AMF) receive a non-2xx (failure) response in the last 5 minutes (or selected sample frame) **Diagnostic Information :** 1. ***Check Recent Logs***: • Analyze logs for both PCF-UE and Egress Gateway in the relevant namespace for error details (timestamps matching the period of alert). • Focus on error responses: look for 4xx/5xx HTTP responses and their reasons. 2. ***Correlate with Traffic Patterns***: • Determine if failures are for specific to certain AMFs or random. • Check if there's a sudden surge in failures (indicating a broader issue). 3. ***Inspect Network Health and Configuration***: • Ensure connectivity and correct routing between PCF-UE and its downstream targets. • Validate configurations, especially recently changed ones. 4. ***Cross-check Incident/Event Timeline***: • Review recent maintenance, deployments, or network events that could correlate with the increase in failures. 5. ***Evaluate for Service Overload***: • Examine resource metrics (CPU, memory, rate of requests) of the affected service(PCF-UE, PCF-EGW) to determine if it’s under duress. 6. ***Check with Peers***: • See if corresponding namespaces (other tenants/products) are seeing similar issues, could indicate a platform or shared service problem. **Recovery :** 1. **Resolve Underlying Service Issues**: • If the upstream service (e.g., AMF or other network function) is unhealthy, work with the respective team to restore normal operation. • Address any misconfiguration or errors causing repeated non-2xx responses. 2. **Revert Recent Changes**:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-190 (Cont.)
UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
	• If the issue correlates with recent deployments or configuration changes, consider rolling back to the previous stable state after assessing impact. 3. **Mitigate Service Overload**: • If resource constraints are detected (CPU, memory, connections), scale up resources or reduce load by throttling non-critical requests where possible. 4. **Network Remediation**: • Resolve any detected connectivity or routing issues between PCF-UE and the egress gateway or upstream endpoints. 5. **Monitor and Confirm Recovery**: • Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold. Ensure related services in affected namespaces also recover.

8.1.2.56 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 8-191 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of amf discovery reattempts failed.
Summary	More than 75% of amf discovery reattempts failed.
Severity	Critical
Expression	(sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_response_total{operationType="timer_expiry_notification",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_request_total{operationType="timer_expiry_notification"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.105
Metric Used	occnp_ue_nf_discovery_reattempt_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-191 (Cont.) UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_ue_nf_discovery_reattempt_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case, the alert notifies when there is a certain number of reattempt failure while discovering AMF. If there is an increase of failure, operator can investigate on: • Why the AMF discovery flow is failing, or • Check the health of the AMF to which the request are going to. **Cause:** The main cause of the `occnp_ue_nf_discovery_reattempt_response_total` metric being pegged—indicating a notable number of reattempt failures during AMF discovery—is that the PCF-UE (Policy Control Function - User Equipment) is receiving non-success responses (failures) when retrying AMF (Access and Mobility Management Function) discovery requests. **Diagnostic Information:** • **AMF Unavailability or Health Issues:** The target AMF may be down, unresponsive, overloaded, or otherwise unhealthy, resulting in failed or rejected discovery attempts. • **Network Issues or Latency:** Communication issues such as network congestion, high latency, or dropped packets between the PCF-UE and the AMF (or intermediary NFs) can cause discovery attempts to fail. • **Incorrect Configuration:** Misconfigurations in the PCF-UE or AMF—such as wrong endpoint addresses, security settings, or authentication parameters—may prevent the successful completion of discovery requests. • **NRF (Network Repository Function) Problems:** If AMF discovery relies on the NRF and the NRF is unhealthy or misconfigured, the PCF-UE may be unable to retrieve up-to-date or correct AMF information. • **Resource Exhaustion:** If the system is under heavy load or resources (CPU, memory, threads) are depleted, discovery requests may not be handled on time. • **Timeouts and Slow Processing:** Slow responses from the AMF or network timeouts can contribute to repeated reattempts and failures. **Recovery:** • Review logs and error responses associated with AMF discovery attempts. • Check the health status and recent operational history of the target AMF and NRF. • Verify network health and connectivity between all relevant components. • Validate all associated configurations (PCF-UE, AMF, NRF). If the issue persists, please check with Support team.

8.1.2.57 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 8-192 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of amf discovery reattempts failed.
Summary	More than 50% of amf discovery reattempts failed.
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-192 (Cont.) UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_response_total{operationType="timer_expiry_notification",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_request_total{operationType="timer_expiry_notification"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.105
Metric Used	occnp_ue_nf_discovery_reattempt_response_total
Recommended Actions	The `occnp_ue_nf_discovery_reattempt_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case, the alert notifies when there is a certain number of reattempt failure while discovering AMF. If there is an increase of failure, operator can investigate on: • Why the AMF discovery flow is failing, or • Check the health of the AMF to which the request are going to. **Cause:** The main cause of the `occnp_ue_nf_discovery_reattempt_response_total` metric being pegged—indicating a notable number of reattempt failures during AMF discovery—is that the PCF-UE (Policy Control Function - User Equipment) is receiving non-success responses (failures) when retrying AMF (Access and Mobility Management Function) discovery requests. **Diagnostic Information:** • **AMF Unavailability or Health Issues:** The target AMF may be down, unresponsive, overloaded, or otherwise unhealthy, resulting in failed or rejected discovery attempts. • **Network Issues or Latency:** Communication issues such as network congestion, high latency, or dropped packets between the PCF-UE and the AMF (or intermediary NFs) can cause discovery attempts to fail. • **Incorrect Configuration:** Misconfigurations in the PCF-UE or AMF—such as wrong endpoint addresses, security settings, or authentication parameters—may prevent the successful completion of discovery requests. • **NRF (Network Repository Function) Problems:** If AMF discovery relies on the NRF and the NRF is unhealthy or misconfigured, the PCF-UE may be unable to retrieve up-to-date or correct AMF information. • **Resource Exhaustion:** If the system is under heavy load or resources (CPU, memory, threads) are depleted, discovery requests may not be handled on time. • **Timeouts and Slow Processing:** Slow responses from the AMF or network timeouts can contribute to repeated reattempts and failures. **Recovery:** • Review logs and error responses associated with AMF discovery attempts. • Check the health status and recent operational history of the target AMF and NRF. • Verify network health and connectivity between all relevant components. • Validate all associated configurations (PCF-UE, AMF, NRF). If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.58 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 8-193 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of amf discovery reattempts failed.
Summary	More than 25% of amf discovery reattempts failed.
Severity	Minor
Expression	(sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_response_total{operationType="timer_expiry_notification",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_request_total{operationType="timer_expiry_notification"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.105
Metric Used	occnp_ue_nf_discovery_reattempt_response_total
Recommended Actions	The `occnp_ue_nf_discovery_reattempt_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then, in this case the alert notifies when there is a certain number of reattempt failure while discovering AMF. If there is an increase of failure, operator can investigate on: • Why the AMF discovery flow is failing, or • Check the health of the AMF to which the request are going to. **Cause:** The main cause of the `occnp_ue_nf_discovery_reattempt_response_total` metric being pegged—indicating a notable number of reattempt failures during AMF discovery—is that the PCF-UE (Policy Control Function - User Equipment) is receiving non-success responses (failures) when retrying AMF (Access and Mobility Management Function) discovery requests. **Diagnostic Information:** • **AMF Unavailability or Health Issues:** The target AMF may be down, unresponsive, overloaded, or otherwise unhealthy, resulting in failed or rejected discovery attempts. • **Network Issues or Latency:** Communication issues such as network congestion, high latency, or dropped packets between the PCF-UE and the AMF (or intermediary NFs) can cause discovery attempts to fail. • **Incorrect Configuration:** Misconfigurations in the PCF-UE or AMF—such as wrong endpoint addresses, security settings, or authentication parameters—may prevent the successful completion of discovery requests. • **NRF (Network Repository Function) Problems:** If AMF discovery relies on the NRF and the NRF is unhealthy or misconfigured, the PCF-UE may be unable to retrieve up-to-date or correct AMF information. • **Resource Exhaustion:** If the system is under heavy load or resources (CPU, memory, threads) are depleted, discovery requests may not be handled on time. • **Timeouts and Slow Processing:** Slow responses from the AMF or network timeouts can contribute to repeated reattempts and failures. **Recovery:** • Review logs and error responses associated with AMF discovery attempts. • Check the health status and recent operational history of the target AMF and NRF. • Verify network health and connectivity between all relevant components. • Validate all associated configurations (PCF-UE, AMF, NRF). If the issue persists, please check with Support team.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.59 INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD

Table 8-194 INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD

Field	Details
Name	INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD
Description	Ingress Error Rate above 10 Percent in {{$labels.pod}} in {{$labels.namespace}}
Summary	Transaction Error Rate in {{$labels.pod}} (current value is: {{ $value }})
Severity	Critical
Expression	(sum by(pod)(rate(ocpm_ingress_response_total{response_code!~"2.*"}[24h]) or (up * 0))/sum by(pod)(rate(ocpm_ingress_response_total[24h]))) * 100>= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.2
Metric Used	ocpm_ingress_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-194 (Cont.) INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD

Field	Details
Recommended Actions	**Cause** This alert fires when 10% or more of ingress (incoming) HTTP requests handled by any individual pod result in non-2xx (unsuccessful) responses, measured over a 1-day window. A high ingress error rate per pod suggests issues that could impact application availability, reliability, or user experience. Common causes include: • Application-level errors (returning 4xx or 5xx status codes) due to bugs, configuration issues, invalid client requests, or backend failures • Resource exhaustion (CPU, memory, open connections) or saturation within the affected pod • Dependency failures (database, cache, or external service outages), causing the pod to respond with errors • Recent deployments, rollouts, or configuration changes introducing regressions or incompatibilities • Network problems or timeouts impacting request processing • Unhandled exceptions or circuit breaker activations **Diagnostic Information** • Identify affected pods from alert labels • Review pod logs to categorize errors by type (4xx client errors, 5xx server errors, timeouts, etc.) • Correlate errors with spikes in traffic, resource usage, or specific endpoints • Examine resource utilization and health metrics (CPU, memory, connection pools, thread pools) • Check readiness/liveness probe status and pod restart history • Review changes in deployments, configurations, or dependencies preceding the alert • Investigate for signs of dependency issues, cascading failures, or external API problems **Recovery** • **Isolate and address root cause:** Use logs, error breakdowns, and metrics to determine if issues are within the pod, code, dependencies, or external factors • **Rollback if needed:** If problems started following a recent deployment or config change, consider reverting • **Increase resources or scale out:** Add capacity if the pod is resource-constrained • **Fix code or configuration:** Resolve bugs, correct misconfigurations, or address unhandled cases • **Remediate downstream/third-party issues:** Work with owners of failing dependencies if external • **Alert resolution:** The alert will auto-resolve when the pod's ingress error rate falls below 10% for the measuring window

8.1.2.60 SM_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 8-195 SM_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Name	SM_TRAFFIC_RATE_ABOVE_THRESHOLD

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-195 (Cont.) SM_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Description	SM service Ingress traffic Rate is above threshold of Max MPS (current value is: {{ $value }})
Summary	Traffic Rate is above 90 Percent of Max requests per second
Severity	Major
Expression	sum(rate(ocpm_ingress_request_total{servicename_3gpp="npcf-smpolicycontrol"}[2m])) >= 900
OID	1.3.6.1.4.1.323.5.3.52.1.2.3
Metric Used	ocpm_ingress_request_total
Recommended Actions	**Cause:** The metric `ocpm_ingress_request_total` is incremented for every inbound HTTP request reaching the SM component of the SM service with the dimension `serviceName3gpp="npcf-smpolicycontrol"`. If the 2-minute average exceeds 900 mps, this indicates that the system may be experiencing an overload or an abnormal spike in traffic. **Diagnostic Information:** **Examine Current Rate:** Query `ocpm_ingress_request_total` for `serviceName3gpp="npcf-smpolicycontrol"` to assess the current ingress traffic rate. **Review Upstream Sources:** Identify if request rates from any upstream SMF, AF, or TDF instances have increased. **Inspect Application Logs:** Check for `WARN` or `ERROR` messages in logs related to overload or congestion control rejections, which can help determine if the system is rejecting requests or experiencing resource pressure. **Recovery:** • **Throttle or Rate-Limit:** Apply or adjust overload/congestion control configurations to throttle or rate-limit requests from SMF as appropriate, to restore rate to expected levels. • **Scale Resources:** Add more replicas to the `sm-service` deployment if needed to reduce the average rate per instance. • **Threshold Adjustment:** Adjust the alert threshold if normal traffic patterns or business requirements change. • **Alert Resolution:** When the sustained request rate stays below 900 mps, Prometheus will automatically clear the `SM_TRAFFIC_RATE_ABOVE_THRESHOLD` alert.

8.1.2.61 SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 8-196 SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Name	SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT
Description	Transaction Error Rate detected above 10 Percent of Total on SM service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 10 Percent of Total Transactions
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-196 (Cont.) SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Expression	(sum(rate(ocpm_ingress_response_total{servicename_3gpp="npcf-smpolicycontrol",response_code!~"2.*"}[24h]) or (up * 0)) / sum(rate(ocpm_ingress_response_total{servicename_3gpp="npcf-smpolicycontrol"}[24h]))) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.4
Metric Used	ocpm_ingress_response_total
Recommended Actions	**Cause** This alert fires when more than 10% of all HTTP responses returned by the SM Service (`npcf-smpolicycontrol`)over the past day are non-2xx (i.e., not successful). This may be due to: • Upstream or downstream system failures • Application-level errors (5xx codes) • Client-side or bad requests (4xx codes) • Misconfiguration, rate limiting, or resource exhaustion **Diagnostic Information** • Break down error rates by response code to differentiate client, server, and other errors. • Search for error messages, stack traces, and signs of repeated failure or congestion. • Validate that dependencies(upstream services, DB) are functioning correctly. • Analyze recent deployments or config changes • Check for network latency **Recovery:** • **Identify and Address Root Cause:** Use error breakdown and logs to pinpoint and fix the underlying issue. • **Rollback Recent Changes:** If a recent deployment is responsible, consider rolling back temporarily. • **Scale or Resource Adjustment:** Add resources if you detect resource exhaustion. • **Rate Limiting or Throttling:** Apply throttling to minimize error propagation from upstream. • **Alert Resolution:** Once the error rate remains below 10% for a sustained period (1 day), the alert will auto-resolve.

8.1.2.62 SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Table 8-197 SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Name in Alert Yaml File	SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT
Description	Egress Transaction Error Rate detected above 1 Percent of Total Transactions (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 1 Percent of Total Transactions
Severity	Minor
Expression	(sum(rate(ocpm_egress_response_total{servicename_3gpp="npcf-smpolicycontrol",response_code!~"2.*"}[24h]) or (up * 0)) / sum(rate(ocpm_egress_response_total{servicename_3gpp="npcf-smpolicycontrol"}[24h]))) * 100 >= 1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-197 (Cont.) SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.5
Metric Used	ocpm_egress_response_total
Recommended Actions	**Cause** This alert fires when more than 1% of all HTTP responses returned by the SM Service (`npcf-smpolicycontrol`)over the past day are non-2xx (i.e., not successful). This may be due to: • Upstream or downstream system failures • Application-level errors (5xx codes) • Client-side or bad requests (4xx codes) • Misconfiguration, rate limiting, or resource exhaustion **Diagnostic Information** • Break down error rates by response code to differentiate client, server, and other errors. • Search for error messages, stack traces, and signs of repeated failure or congestion. • Validate that dependencies(upstream services, DB) are functioning correctly. • Analyze recent deployments or config changes • Check for network latency **Recovery:** • **Identify and Address Root Cause:** Use error breakdown and logs to pinpoint and fix the underlying issue. • **Rollback Recent Changes:** If a recent deployment is responsible, consider rolling back temporarily. • **Scale or Resource Adjustment:** Add resources if you detect resource exhaustion. • **Rate Limiting or Throttling:** Apply throttling to minimize error propagation from upstream. **Alert Resolution:** Once the error rate remains below 10% for a sustained period (1 day), the alert will auto-resolve. For any additional guidance, contact My Oracle Support.

8.1.2.63 PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 8-198 PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Name	PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD
Description	User service Ingress traffic Rate from CHF is above threshold of Max MPS (current value is: {{ $value }})
Summary	Traffic Rate is above 90 Percent of Max requests per second
Severity	Major
Expression	sum(rate(occnp_userservice_inbound_count_total{service_resource="chf-service"}[2m])) >= 900
OID	1.3.6.1.4.1.323.5.3.52.1.2.11
Metric Used	ocpm_userservice_inbound_count_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-198 (Cont.) PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
Recommended Actions	**Cause:** The metric ocpm_userservice_inbound_count_total with dimension service_resource="chf-service" is incremented for every inbound HTTP request reaching the CHF connector service. If the 2-minute average exceeds 900 mps, this indicates that the system may be experiencing an overload or an abnormal spike in traffic. **Diagnostic Information:** **Examine Current Rate:** Query ocpm_userservice_inbound_count_total for service_resource="chf-service" to assess the current ingress traffic rate. **Review Upstream Sources:** Identify if request rates from any upstream CHF, SMF, AMF instances have increased. **Inspect Application Logs:** Check for `WARN` or `ERROR` messages in logs related to overload or congestion control rejections, which can help determine if the system is rejecting requests or experiencing resource pressure. **Recovery:** • **Throttle or Rate-Limit:** Apply or adjust congestion control configurations to throttle requests from downstream services as appropriate, to restore rate to expected levels. • **Scale Resources:** Add more replicas to the `Chf connector` deployment if needed to reduce the average rate per instance. • **Threshold Adjustment:** Adjust the alert threshold if normal traffic patterns or business requirements change. **Alert Resolution:** When the sustained request rate stays below 900 mps, Prometheus will automatically clear the PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD alert. For any additional guidance, contact My Oracle Support.

8.1.2.64 PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 8-199 PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Name	PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT
Description	Egress Transaction Error Rate detected above 10 Percent of Total on User service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 10 Percent of Total Transactions
Severity	Critical
Expression	(sum(rate(ocpm_chf_tracking_response_total {servicename_3gpp="nchf-spendinglimitcontrol",response_code!~"2.*"} [24h]) or (up * 0)) / sum(rate(ocpm_chf_tracking_response_total {servicename_3gpp="nchf-spendinglimitcontrol"} [24h]))) 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.12
Metric Used	ocpm_chf_tracking_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-199 (Cont.) PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Recommended Actions	**Cause:** This alert fires when more than 10% of all HTTP responses for the PCF (CHF connector the PCF component that calls the external CHF via nchf-spendinglimitcontrol) over the past day are non-2xx (i.e., not successful). This may be due to: • External CHF partial outage or dependency failures. • Application-level errors (5xx) or timeouts on the CHF path. • Client/bad requests (4xx) from the CHF connector due to schema/version or auth issues. • Misconfiguration, rate limiting/throttling, TLS/mTLS or DNS problems, or resource exhaustion. **Diagnostic Information:** • Break down error rates by response class (4xx vs 5xx vs timeouts/TLS/connect resets). • Search CHF connector service logs and traces for recurring errors, stack traces, circuit-breaker events, or congestion. • Validate external CHF health and dependencies (service/DB), and check for throttling indicators. • Analyze recent deployments or configuration changes in PCF or CHF (endpoints, timeouts, retries, API versions). • Check for traffic spikes, connection pool saturation, CPU/memory pressure, or elevated latency. **Recovery:** • **Identify and address root cause:** Use error breakdown, logs, and traces to pinpoint whether the issue is in the PCF CHF client, network/TLS/auth, or the external CHF. • **Roll back recent changes:** Temporarily revert relevant PCF/CHF deployments or configs if correlated with the onset. • **Scale or resource adjustment:** Increase capacity or tune connection/thread pools; enable autoscaling if appropriate. • **Rate limiting or throttling:** Use bounded retries with backoff and apply throttling to reduce cascading failures. **Alert resolution:** Once the non-2xx rate remains below 10% for a sustained period (1 day), the alert will auto-resolve. For any additional guidance, contact My Oracle Support.

8.1.2.65 PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Table 8-200 PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Field	Details
Name	PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD
Description	Ingress Timeout Error Rate detected above 10 Percent of Total towards CHF service (current value is: {{ $value }})
Summary	Timeout Error Rate detected above 10 Percent of Total Transactions
Severity	Major
Expression	(sum(rate(ocpm_chf_tracking_request_timeout_total{servicename_3gpp="nchf-spendinglimitcontrol"}[24h]) or (up * 0)) / sum(rate(ocpm_chf_tracking_request_total{servicename_3gpp="nchf-spendinglimitcontrol"}[24h]))) * 100 >=10

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-200 (Cont.) PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.17
Metric Used	ocpm_chf_tracking_request_timeout_total
Recommended Actions	**Cause:** This alert is triggered when more than 10% of all inbound requests from PCF (Policy Control Function) to the CHF (`nchf-spendinglimitcontrol`) time out over a 1-day window. This may impact charging, quota enforcement, or service delivery. Common causes include: • Network latency, intermittent packet loss, or connectivity issues between PCF and CHF • Overload, resource congestion, or unresponsiveness in the CHF or its dependencies • Resource exhaustion or scaling limits in the PCF, CHF, or intermediary components • Misconfiguration of timeout thresholds, retries, or circuit breaker settings • Downstream service or database issues affecting CHF's ability to respond in time • Recent changes or deployments that introduced performance bottlenecks or regressions **Diagnostic Information:** • Identify which part of the infrastructure is experiencing timeouts: is it consistent across all traffic or localized? • Review logs from PCF, CHF, and network/security appliances for repeated timeout, retry, or connection reset events • Check health dashboards for CHF (CPU, memory, response latency, DB availability, etc.) • Analyze request/response timings, queue lengths, and backlog at ingress points • Correlate with recent deployment, scaling, or network changes • Examine resource usage and pod health for PCF and CHF components **Recovery:** • **Isolate the root cause:** Use logs and health metrics to determine if the problem is with CHF availability, network path, or PCF. • **Scale or optimize:** Increase resources, scale instances, or optimize configuration for PCF and CHF services as needed. • **Rollback if needed:** If the alert correlates with new deployments or config changes, consider reverting. • **Network remediation:** Address any identified network latency, packet loss, or DNS resolution issues. • **Tune configuration:** Adjust timeout settings, connection pools, and retry logic based on observed conditions. • **Coordinate:** Engage CHF, PCF, and platform support teams as needed for collaborative troubleshooting. **Alert Resolution:** This alert will auto-resolve once the ingress timeout error rate drops below 10% of total requests to CHF over the evaluation window.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.66 PCF_PENDING_BINDING_SITE_TAKEOVER

Table 8-201 PCF_PENDING_BINDING_SITE_TAKEOVER

Field	Details
Description	The site takeover configuration has been activated
Summary	The site takeover configuration has been activated
Severity	CRITICAL
Expression	sum by (application, container, namespace) (changes(occnp_pending_binding_site_takeover[2m])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.45
Metric Used	occnp_pending_binding_site_takeover
Recommended Actions	**Cause:** This alert fires when the site takeover functionality is engaged to handle geo-redundancy scenarios. Site takeover is typically activated when a site in a distributed PCF deployment is down or unreachable, empowering another site to process that site's pending binding operations for service continuity. **Diagnostic Information:** • Check configuration to confirm the alternate site profile is correctly set and the takeover flag is enabled. • Examine PendingOperation records to ensure the alternate site is processing entries from the down site's site ID. • Review service logs for site takeover-related events, handoff messages, and any associated errors during takeover or operation processing. **Recovery & Actions:** • **Verify** that site takeover activation was intentional and aligns with fail-over or DR (Disaster Recovery) procedures. • **Monitor** processing of pending operations for successful handoff and completion under the alternate site. • **Communicate** with relevant operations/support teams about the takeover to prevent conflicting operations. • **Disable site takeover** once the original site is restored to normal operation, so pending operations revert to their standard ownership and workflow. • **Audit** for any missed or failed operations during the site handover, and remediate as needed. **Alert Resolution:** The alert will auto-resolve once there are no new site takeover events, and the takeover configuration is deactivated or no longer required. For any additional guidance, contact My Oracle Support.

8.1.2.67 PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Table 8-202 PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Field	Details
Description	The Pending Operation table threshold has been reached.
Summary	The Pending Operation table threshold has been reached.
Severity	CRITICAL
Expression	sum by (application, container, namespace) (changes(occnp_threshold_limit_reached_total[2m])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.46

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-202 (Cont.) PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Field	Details
Metric Used	occnp_threshold_limit_reached_total
Recommended Actions	**Cause** This alert fires when the number of records in the Pending Operation table (to reattempt binding registration in BSF at a later time) reaches a predefined threshold. This means the system's retry or pending queue for binding operations is saturated and may be at risk of delaying, or failing new operations. Exceeding this threshold typically signals that retry or binding registrations are not clearing at an expected rate. Common causes include: • Persistent errors or failures from BSF in response to binding attempts, triggering retries • Widespread or systemic service degradation in BSF, Binding Service, or network paths • Application bugs resulting in stuck or orphaned PendingOperation records • Misconfigured thresholds, retry intervals, or logic in SM or Binding Service • Resource starvation (CPU, memory, DB connections) preventing timely processing of pending operations • Recent deployments, configuration updates, or load spikes overwhelming the binding flow **Diagnostic Information** • Check the volume, age, and growth trend of records in the Pending Operation table • Correlate with other alerts or incident tickets related to BSF, Binding Service, network, or DB health • Analyze logs from SM Service, Binding Service, and (if applicable) Audit Service for repeated errors, retry loops, or slow processing • Review recent deployments or configuration changes to PCF Service components • Inspect resource utilization for relevant pods, containers, and backend storage • Confirm correct configuration of the threshold limit, retry intervals, and error code handling **Recovery** • **Prioritize clearing pending records:** Investigate and remediate the root cause(s) of unprocessed binding operations (BSF issues, infra bottlenecks, logic bugs) • **Scale resources or prioritize processing:** Add capacity or redistribute load if resource constraints are found • **Tune configuration:** Adjust thresholds, error code mappings, and retry intervals as necessary • **Audit retry and cleanup logic:** Ensure orphaned or stale records are purged and retry logic is functioning as intended • **Rollback if needed:** If issue began with a recent deployment or config change, consider reverting • **Coordinate across teams:** Engage with BSF, Infrastructure, and DB owners as required **Alert resolution:** The alert will auto-resolve once the number of records in the Pending Operation table returns below the configured threshold and normal processing resumes. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.68 PCF_PENDING_BINDING_RECORDS_COUNT

Table 8-203 PCF_PENDING_BINDING_RECORDS_COUNT

Field	Details
Name	PCF_PENDING_BINDING_RECORDS_COUNT
Description	Pending Operation Table contains records.
Summary	Pending Operation Table contains records.
Severity	MINOR
Expression	sum by (application, container, namespace) (changes(occnp_pending_operation_records_count[10s])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.47
Metric Used	occnp_pending_operation_records_count
Recommended Actions	**Cause** This alert fires when a new pending binding operation is inserted into the system by the SM Service(to reattempt binding registration in BSF at a later time). This typically happens when the BSF reattempt settings are configured and the response from BSF to a binding registration indicates an error condition that requires a retry (as per pre-configured error codes). Common causes for entries in the PendingOperation table include:Common causes include: • BSF returns a transient or retry-eligible error code in response to binding requests. • Temporary unavailability or instability of BSF or related network paths. • Application bugs leading to improper handling of BSF responses or retry logic. • Recent configuration changes impacting retry or error handling logic. **Diagnostic Information** • Review SM Service and binding service logs to trace binding requests, BSF response codes, and the creation/updating of PendingOperations. • Verify resource utilization and health across relevant pods or containers. • Analyze timing and Volume of pending operation records—spikes may indicate regression or external service instability. **Recovery** • **Monitor pending operation clearance:** Confirm that retries triggered by Audit Service notifications are processed and successfully clear pending records. • **Investigate recurring or persistent errors:** If retries are frequently required or repeatedly fail, drill down to BSF responses, retry outcomes, and any correlated infrastructure issues. • **Coordinate with BSF/service owners:** If an underlying BSF or network problem persists, work with those teams to restore normal registration flow. • **Tune configuration:** Adjust error code mapping, retry intervals, or thresholds based on observed workload and service behavior. • **Rollback if needed:** Revert recent deployments or config updates if they correlate with spikes in pending operations. **Alert resolution:** The alert will auto-resolve when new pending binding operation records are no longer being routinely created, retries are succeeding, and the overall pending queue stabilizes or clears. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.69 AUTONOMOUS_SUBSCRIPTION_FAILURE

Table 8-204 AUTONOMOUS_SUBSCRIPTION_FAILURE

Field	Details
Description	Autonomous subscription failed for a configured Slice Load Level
Summary	Autonomous subscription failed for a configured Slice Load Level
Severity	Critical
Expression	The number of failed Autonomous Subscription for a configured Slice Load Level in nwdaf-agent is greater than zero.
OID	1.3.6.1.4.1.323.5.3.52.1.2.49
Metric Used	subscription_failure{requestType="autonomous"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-204 (Cont.) AUTONOMOUS_SUBSCRIPTION_FAILURE

Field	Details
Recommended Actions	The alert gets cleared when the failed Autonomous Subscription is corrected. To clear the alert, perform the following steps: 1. Delete the Slice Load Level configuration. 2. Re-provision the Slice Load Level configuration. **Cause:** This alert activates when there is at least one autonomous subscription (such as the NWDAF event subscription process) failure detected for a given S-NSSAI, indicating that the system was unable to successfully initiate or maintain a subscription for a specific network slice. Common causes may include: • Remote service (e.g., NWDAF) is unavailable, responds with a failure, or returns an error code. • Authentication/authorization failures (invalid tokens, credentials, certificates). • Incorrect, missing, or unsupported subscription parameters (S-NSSAI, event types, notification targets). • API version or schema mismatches between subscribing and serving systems. • Rate limiting, resource exhaustion, or capacity constraints in remote service. • Network or DNS/connectivity problems between components. • Recent deployment or configuration change introducing new issues. **Diagnostic Information:** • Check which S-NSSAI (network slice) is affected using the alert labels. • Review NWDAF gent service logs, and collect relevant error codes and messages from the failed subscription attempts. • Examine recent changes or deployments to the NWDAF Agent, remote NWDAF, or related interfaces/services. • Assess service health and connectivity between the agent and NWDAF (latency, errors, authentication status). • Validate the subscription request payload, endpoint URLs, and configuration for the target S-NSSAI. • Look for evidence of transient or repeated network/service issues. **Recovery:** • **Identify the failed subscription(s):** Use the alert labels and logs to pinpoint the slice(s) affected. • **Resolve remote or local service issues:** Work with relevant teams to restore NWDAF or agent functionality, address authentication or network problems, or resolve configuration mismatches. • **Retry or re-initiate subscriptions** as needed after addressing the root cause. • **Rollback changes** if the alert coincides with recent deployments, configuration modifications, or rollouts. **Alert Resolution:** This alert will automatically resolve once the system detects that there are no new autonomous subscription failures (i.e., no new increments in the failure counter) for the affected S-NSSAI(s) within the evaluation window. Successful re-establishment or correction will clear the alert. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.70 AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Table 8-205 AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Name	AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT
Description	AMF Notification Error Rate detected above 1 Percent of Total on AM Service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 1 Percent of Total Transactions on AM Notification
Severity	MINOR
Expression	(sum(rate(http_out_conn_response_total{pod=~".*amservice.*",responseCode!~"2.*",servicename3gpp="npcf-am-policy-control"}[1d])) / sum(rate(http_out_conn_response_total{pod=~".*amservice.*",servicename3gpp="npcf-am-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.54
Metric Used	http_out_conn_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-205 (Cont.) AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert triggers when 1% or more of notification requests sent from the AM service (part of PCF) to the AMF (`npcf-am-policy-control` endpoint) result in non-2xx (unsuccessful) responses over a 1-day window. These notifications inform AMF about access or mobility events. A significant portion of errors could be 404 responses, which occur when AMF does not have the corresponding session in its context. This may indicate attempts to notify AMF about sessions that have already ended or were never established. Other possible causes include: • Partial outage, degradation, or overload in the AMF • Application errors in the AM service or AMF (e.g., other 4xx or 5xx codes) • Schema or API mismatches due to recent deployments or configuration changes • Authentication, authorization, or TLS certificate issues • Network/connectivity problems • Resource exhaustion in the AMF **Diagnostic Information** • Break down non-2xx responses by HTTP status code, especially 404 versus other 4xx/5xx • Examine AM service and AMF logs for detailed error messages and patterns • Review session establishment, update, and termination flows in both AM service and AMF • Investigate recent deployments, configuration changes, or spikes in error rates • Assess resource usage and health of both AM service and AMF • Validate API contracts, payload formats, and endpoint configurations • Check for authentication/authorization or certificate issues **Recovery** • **Identify and resolve the root cause:** Use logs, traces, and error breakdowns to determine if high 404 rates are expected (due to session lifecycle), or if there is a systematic issue such as stale notifications • **Tune notification logic:** Adjust workflows to minimize duplicate or late notifications when sessions may already have ended • **Rollback or adjust recent changes:** If errors correlate with deployments or config updates, consider reverting them • **Scale or adjust resources:** Add capacity or tune connection/timeouts if resource exhaustion is present • **Remediate network or security problems:** Ensure stable communication and correct authentication/certificates between PCF and AMF **Alert resolution:** The alert will auto-resolve when the error rate drops below 1% over the measuring window For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.71 AM_AR_ERROR_RATE_ABOVE_1_PERCENT

Table 8-206 AM_AR_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Name	AM_AR_ERROR_RATE_ABOVE_1_PERCENT
Description	Alternate Routing Error Rate detected above 1 Percent of Total on AM Service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 1 Percent of Total Transactions on AM Alternate Routing
Severity	MINOR
Expression	(sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*amservice.*",responseCode!~"2.*",servicename3gpp="npcf-am-policy-control"}[1d])) / sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*amservice.*",servicename3gpp="npcf-am-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.55
Metric Used	ocpm_ar_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-206 (Cont.) AM_AR_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert fires when 1% or more of alternate routing (AR) requests initiated by the AM service (as part of PCF) to AMF (`npcf-am-policy-control`) result in non-2xx (unsuccessful) responses over a 1-day window, grouped by FQDN. Alternate routing is the process of retrying the original request to a different AMF instance when the initial attempt fails. A rising AR error rate suggests persistent issues with connectivity, service health, or configuration for primary or alternate AMF endpoints. Typical causes include: • Persistent unavailability, overload, or partial outages affecting some or all AMF instances • Application-level errors from AMF (many 4xx/5xx responses, including 404s for missing sessions) • Schema or API incompatibility after deployments or configuration changes • Authentication, authorization, or certificate-related failures during retries • Network or DNS problems affecting communication with one or more AMF instances • Resource exhaustion, scaling issues, or retry storm in the AM service • Misconfiguration of alternate endpoint lists or retry logic **Diagnostic Information** • Break down failed AR responses by HTTP status code (4xx, 5xx, timeouts) to pinpoint the failure type • Review AM service logs to identify why alternate routing was triggered and the response from each retry • Inspect AMF logs for errors and session context associated with AR requests • Assess health, status, and readiness of all AMF endpoints relevant to the alerting FQDN • Check authentication credentials, certificate validity, and endpoint configuration • Correlate AR error spikes with recent deployments, updates, scaling actions, or network incidents • Analyze retry logic to ensure backoff and failover policies are working as expected **Recovery** • **Isolate the root cause:** Use logs and metrics to determine if AR failures are due to persistent AMF unavailability, configuration problems, or retry logic bugs • **Remediate endpoint or network issues:** Restore AMF health, increase capacity, or fix network connectivity to all AMF endpoints • **Fix authentication or certificate problems:** Update or refresh security credentials as necessary • **Adjust or rollback changes as needed:** If increased errors align with a recent deployment or config update • **Tune retry/backoff policies:** Update AR configuration to minimize repeated failures or retry storms **Alert resolution:** The alert auto-resolves once the AR error rate drops below 1% over the measurement window For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.72 UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Table 8-207 UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Name	UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT
Description	AMF Notification Error Rate detected above 1 Percent of Total from UE Service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 1 Percent of Total AMF Notification from UE Service
Severity	MINOR
Expression	(sum(rate(http_out_conn_response_total{pod=~".*ueservice.*",responseCode!~"2.*",servicename3gpp="npcf-ue-policy-control"}[1d])) / sum(rate(http_out_conn_response_total{pod=~".*ueservice.*",servicename3gpp="npcf-ue-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.56
Metric Used	http_out_conn_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-207 (Cont.) UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert triggers when 1% or more of notification requests sent from the UE service (part of PCF) to the AMF (npcf-ue-policy-control endpoint) result in non-2xx (unsuccessful) responses over a 1-day window. These notifications inform AMF about UE policy events. A significant portion of errors could be 404 responses, which occur when AMF does not have the corresponding session in its context. This may indicate attempts to notify AMF about sessions that have already ended or were never established. Other possible causes include: • Partial outage, degradation, or overload in the AMF • Application errors in the AM service or AMF (e.g., other 4xx or 5xx codes) • Schema or API mismatches due to recent deployments or configuration changes • Authentication, authorization, or TLS certificate issues • Network/connectivity problems • Resource exhaustion in the AMF **Diagnostic Information** • Break down non-2xx responses by HTTP status code, especially 404 versus other 4xx/5xx • Examine AM service and AMF logs for detailed error messages and patterns • Review session establishment, update, and termination flows in both AM service and AMF • Investigate recent deployments, configuration changes, or spikes in error rates • Assess resource usage and health of both AM service and AMF • Validate API contracts, payload formats, and endpoint configurations • Check for authentication/authorization or certificate issues **Recovery** • **Identify and resolve the root cause:** Use logs, traces, and error breakdowns to determine if high 404 rates are expected (due to session lifecycle), or if there is a systematic issue such as stale notifications • **Tune notification logic:** Adjust workflows to minimize duplicate or late notifications when sessions may already have ended • **Rollback or adjust recent changes:** If errors correlate with deployments or config updates, consider reverting them • **Scale or adjust resources:** Add capacity or tune connection/timeouts if resource exhaustion is present • **Remediate network or security problems:** Ensure stable communication and correct authentication/certificates between PCF and AMF **Alert resolution:** The alert will auto-resolve when the error rate drops below 1% over the measuring window For any additional guidance, contact My Oracle Support.

8.1.2.73 UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Table 8-208 UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Field	Details
Description	Alternate Routing Error Rate detected above 1 Percent of Total on UE Service (current value is: {{ $value }})

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-208 (Cont.) UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Field	Details
Summary	Transaction Error Rate detected above 1 Percent of Total Transactions on UE Alternate Routing
Severity	MINOR
Expression	(sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*ueservice.*",responseCode!~"2.*",servicename3gpp="npcf-ue-policy-control"}[1d])) / sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*ueservice.*",servicename3gpp="npcf-ue-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.57
Metric Used	ocpm_ar_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-208 (Cont.) UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert fires when 1% or more of alternate routing (AR) requests initiated by the AM service (as part of PCF) to AMF (npcf-ue-policy-control) result in non-2xx (unsuccessful) responses over a 1-day window, grouped by FQDN. Alternate routing is the process of retrying the original request to a different AMF instance when the initial attempt fails. A rising AR error rate suggests persistent issues with connectivity, service health, or configuration for primary or alternate AMF endpoints. Typical causes include: • Persistent unavailability, overload, or partial outages affecting some or all AMF instances • Application-level errors from AMF (many 4xx/5xx responses, including 404s for missing sessions) • Schema or API incompatibility after deployments or configuration changes • Authentication, authorization, or certificate-related failures during retries • Network or DNS problems affecting communication with one or more AMF instances • Resource exhaustion, scaling issues, or retry storm in the AM service • Misconfiguration of alternate endpoint lists or retry logic **Diagnostic Information** • Break down failed AR responses by HTTP status code (4xx, 5xx, timeouts) to pinpoint the failure type • Review AM service logs to identify why alternate routing was triggered and the response from each retry • Inspect AMF logs for errors and session context associated with AR requests • Assess health, status, and readiness of all AMF endpoints relevant to the alerting FQDN • Check authentication credentials, certificate validity, and endpoint configuration • Correlate AR error spikes with recent deployments, updates, scaling actions, or network incidents • Analyze retry logic to ensure backoff and failover policies are working as expected **Recovery** • **Isolate the root cause:** Use logs and metrics to determine if AR failures are due to persistent AMF unavailability, configuration problems, or retry logic bugs • **Remediate endpoint or network issues:** Restore AMF health, increase capacity, or fix network connectivity to all AMF endpoints • **Fix authentication or certificate problems:** Update or refresh security credentials as necessary • **Adjust or rollback changes as needed:** If increased errors align with a recent deployment or config update • **Tune retry/backoff policies:** Update AR configuration to minimize repeated failures or retry storms **Alert resolution:** The alert auto-resolves once the AR error rate drops below 1% over the measurement window For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.74 SMSC_CONNECTION_DOWN

Table 8-209 SMSC_CONNECTION_DOWN

Field	Details
Description	Connection to SMSC peer {{$labels.smscName}} is down in notifier service pod {{$labels.pod}}
Summary	Connection to SMSC peer {{$labels.smscName}} is down in notifier service pod {{$labels.pod}}
Severity	MAJOR
Expression	sum by(namespace, pod, smscName)(occnp_active_smsc_conn_count) == 0
OID	`1.3.6.1.4.1.323.5.3.52.1.2.63`
Metric Used	occnp_active_smsc_conn_count

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-209 (Cont.) SMSC_CONNECTION_DOWN

Field	Details
Recommended Actions	**Cause** This alert fires when the connection count to a specific SMSC (Short Message Service Center) peer (`smscName`) drops to zero in a notifier service pod. This means that the notifier service in the indicated pod has lost connectivity with the SMSC peer, which may halt or delay SMS delivery for affected sessions. Common causes include: • Network connectivity issues between the notifier pod and the SMSC peer (latency, packet loss, firewall changes) • SMSC peer instance is offline, unresponsive, or undergoing maintenance • Unexpected restart or crash of the notifier service pod • TCP session timeout, reset, or socket exhaustion • TLS/certificate negotiation failures (if applicable) • Misconfiguration of SMSC endpoint, port, or authentication details • Recent pod or infrastructure changes affecting networking or endpoints **Diagnostic Information** • Identify which `namespace`, `pod`, and `smscName` are affected from alert labels • Check notifier pod logs for errors, timeouts, or repeated reconnection attempts to the SMSC • Confirm SMSC peer health and status via monitoring tools or coordination with peer's operations • Validate network connectivity (test with ping/telnet/traceroute), DNS resolution, and firewall or security rules • Review recent changes in deployment, SMSC endpoint configuration, or certificate rotation • Check for underlying resource issues (CPU, memory, open file/socket limits) on the notifier pod **Recovery** • **Restore connectivity:** Address any network or firewall problems between the notifier pod and SMSC peer • **Restart services:** If the notifier pod is in a bad state, restart it to reestablish the connection • **Engage SMSC operations:** If the peer is down, coordinate with the SMSC provider/team to restore service • **Correct configuration:** Verify endpoint settings, authentication, and port assignments in both notifier and SMSC • **Rollback recent changes:** If disconnection began after deployment or configuration change, consider reverting **Alert resolution:** The alert will auto-resolve once the connection count returns above zero for the affected pod and SMSC For any additional guidance, contact My Oracle Support.

8.1.2.75 LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Table 8-210 LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Field	Details
Name	LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD
Description	Lock acquisition failures exceed the minor threshold limit. The (current value is: {{ $value }})

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-210 (Cont.) LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Field	Details
Summary	Keys used in Bulwark lock request which are already in locked state detected above 20 Percent of Total Transactions.
Severity	Minor
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >=20 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, between 20% and 50% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 20%. If the rate exceeds 50%, a higher severity alert will trigger.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.76 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Table 8-211 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Name	LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD
Description	Lock acquisition failures exceed the major threshold limit. The (current value is: {{ $value }})
Summary	Keys used in Bulwark lock request which are already in locked state detected above 50 Percent of Total Transactions.
Severity	Major
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-211 (Cont.) LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, between 50% and 75% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 50%. If the rate exceeds 75%, a higher severity alert will trigger.

8.1.2.77 LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Table 8-212 LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Name	LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD
Description	Lock acquisition failures exceed the critical threshold limit. The (current value is: {{ $value }})
Summary	Keys used in Bulwark lock request which are already in locked state detected above 75 Percent of Total Transactions.
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-212 (Cont.) LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >=75
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, above 75% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 75%.

8.1.2.78 SM_UPDATE_NOTIFY_FAILED_ABOVE_50_PERCENT

Table 8-213 SM_UPDATE_NOTIFY_FAILED_ABOVE_50_PERCENT

Field	Details
Description	Update Notify Terminate sent to SMF failed >= 50 < 60

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-213 (Cont.) SM_UPDATE_NOTIFY_FAILED_ABOVE_50_PERCENT

Field	Details
Summary	Update Notify Terminate sent to SMF failed >= 50 < 60
Severity	MINOR
Expression	(sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol",responseCode!~"2.*"})*100)/ sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol"}) >= 50 < 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.80
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause** This alert fires when, over the evaluation period, between 50% and 60% of `terminate_notify` HTTP outbound requests sent from PCF (SM Service pods) to SMF result in non-2xx (failed) HTTP responses. In this workflow, PCF notifies SMF to terminate a session. Notably, SMF will return a 404 error if the session does not exist in its current context. Elevated rates of 404 errors could indicate attempts to terminate already-removed sessions or stale references. Other common causes include: • SMF service partial outage or overload • Application-level errors (4xx other than 404, 5xx) • Network issues • Configuration mistakes • Recent deployments or system changes **Diagnostic Information** • Break down non-2xx responses by HTTP code (especially distinguishing 404s from 5xx or other 4xx) • Check PCF and SM Service logs for error details related to `terminate_notify` requests • Review SMF logs for the context and reasoning behind 404 responses • Analyze the timing and volume of session termination requests compared to active session counts • Correlate with recent maintenance, scaling events, or deployment changes • Evaluate resource utilization and connectivity between PCF and SMF **Recovery** • **Determine Root Cause:** Use error codes, logs, and traces to identify whether high 404s are expected (e.g., requests for sessions already removed) or whether there are issues with session tracking, race conditions, or stale data • **Rollback if Needed:** If recent changes coincide with failures, consider rolling back deployments or configurations. • **Scale/Resources:** Address resource exhaustion or performance bottlenecks as needed **Alert Resolution:** The alert will auto-resolve once failed response rates fall below 50% for the evaluation window. A higher-severity alert may trigger if failures exceed 60%. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.79 SM_UPDATE_NOTIFY_FAILED_ABOVE_60_PERCENT

Table 8-214 SM_UPDATE_NOTIFY_FAILED_ABOVE_60_PERCENT

Field	Details
Description	Update Notify Terminate sent to SMF failed >= 60 < 70
Summary	Update Notify Terminate sent to SMF failed >= 60 < 70
Severity	MAJOR
Expression	(sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol",responseCode!~"2.*"})*100)/ sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol"}) >= 60 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.80
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause** This alert fires when, over the evaluation period, between 60% and 70% of `terminate_notify` HTTP outbound requests sent from PCF (SM Service pods) to SMF result in non-2xx (failed) HTTP responses. In this workflow, PCF notifies SMF to terminate a session. Notably, SMF will return a 404 error if the session does not exist in its current context. Elevated rates of 404 errors could indicate attempts to terminate already-removed sessions or stale references. Other common causes include: • SMF service partial outage or overload • Application-level errors (4xx other than 404, 5xx) • Network issues • Configuration mistakes • Recent deployments or system changes **Diagnostic Information** • Break down non-2xx responses by HTTP code (especially distinguishing 404s from 5xx or other 4xx) • Check PCF and SM Service logs for error details related to `terminate_notify` requests • Review SMF logs for the context and reasoning behind 404 responses • Analyze the timing and volume of session termination requests compared to active session counts • Correlate with recent maintenance, scaling events, or deployment changes • Evaluate resource utilization and connectivity between PCF and SMF **Recovery** • **Determine Root Cause:** Use error codes, logs, and traces to identify whether high 404s are expected (e.g., requests for sessions already removed) or whether there are issues with session tracking, race conditions, or stale data • **Rollback if Needed:** If recent changes coincide with failures, consider rolling back deployments or configurations. • **Scale/Resources:** Address resource exhaustion or performance bottlenecks as needed **Alert Resolution:** The alert will auto-resolve once failed response rates fall below 60% for the evaluation window. A higher-severity alert may trigger if failures exceed 70%. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.80 SM_UPDATE_NOTIFY_FAILED_ABOVE_70_PERCENT

Table 8-215 SM_UPDATE_NOTIFY_FAILED_ABOVE_70_PERCENT

Field	Details
Description	Update Notify Terminate sent to SMF failed >= 70
Summary	Update Notify Terminate sent to SMF failed >= 70
Severity	CRITICAL
Expression	(sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol",responseCode!~"2.*"})*100)/ sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol"}) >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.80
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause** This alert fires when, over the evaluation period, above 70% of `terminate_notify` HTTP outbound requests sent from PCF (SM Service pods) to SMF result in non-2xx (failed) HTTP responses. In this workflow, PCF notifies SMF to terminate a session. Notably, SMF will return a 404 error if the session does not exist in its current context. Elevated rates of 404 errors could indicate attempts to terminate already-removed sessions or stale references. Other common causes include: • SMF service partial outage or overload • Application-level errors (4xx other than 404, 5xx) • Network issues • Configuration mistakes • Recent deployments or system changes **Diagnostic Information** • Break down non-2xx responses by HTTP code (especially distinguishing 404s from 5xx or other 4xx) • Check PCF and SM Service logs for error details related to `terminate_notify` requests • Review SMF logs for the context and reasoning behind 404 responses • Analyze the timing and volume of session termination requests compared to active session counts • Correlate with recent maintenance, scaling events, or deployment changes • Evaluate resource utilization and connectivity between PCF and SMF **Recovery** • **Determine Root Cause:** Use error codes, logs, and traces to identify whether high 404s are expected (e.g., requests for sessions already removed) or whether there are issues with session tracking, race conditions, or stale data • **Rollback if Needed:** If recent changes coincide with failures, consider rolling back deployments or configurations. • **Scale/Resources:** Address resource exhaustion or performance bottlenecks as needed **Alert Resolution:** The alert will auto-resolve once failed response rates fall below 70%. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.81 UPDATE_NOTIFY_FAILURE_ABOVE_30_PERCENT

Table 8-216 UPDATE_NOTIFY_FAILURE_ABOVE_30_PERCENT

Field	Details
Name	UPDATE_NOTIFY_FAILURE_ABOVE_30_PERCENT
Description	{{ $value }} % of update notify sent to SMF that failed.
Summary	More than 30% of update notify sent to SMF failed
Severity	minor
Expression	sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.94
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause**: At least 30 % of the sent Update Notify Requests have failed. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and SMF. Maybe Update Notify requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and SM logs to further investigate on why Update Notify requests are taking too long. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. **Recovery**: Once Update Notify requests are properly processed, the percentage of failed requests will decrease, and the Alert will turn off by itself.

8.1.2.82 UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT

Table 8-217 UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT

Field	Details
Name	UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT
Description	{{ $value }} % of update notify sent to SMF that failed
Summary	More than 50% of update notify sent to SMF failed
Severity	MAJOR
Expression	(sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.94
Metric Used	occnp_http_out_conn_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-217 (Cont.) UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT

Field	Details
Recommended Actions	**Cause**: At least 50 % of the sent Update Notify Requests have failed. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and SMF. Maybe Update Notify requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and SM logs to further investigate on why Update Notify requests are taking too long. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. **Recovery**: Once Update Notify requests are properly processed, the percentage of failed requests will decrease, and the Alert will turn off by itself.

8.1.2.83 UPDATE_NOTIFY_FAILURE_ABOVE_70_PERCENT

Table 8-218 UPDATE_NOTIFY_FAILURE_ABOVE_70_PERCENT

Field	Details
Name	UPDATE_NOTIFY_FAILURE_ABOVE_70_PERCENT
Description	{{ $value }} % of update notify sent to SMF that failed
Summary	More than 70% of update notify sent to SMF failed
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.94
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause**: At least 70 % of the sent Update Notify Requests have failed. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and SMF. Maybe Update Notify requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and SM logs to further investigate on why Update Notify requests are taking too long. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. **Recovery**: Once Update Notify requests are properly processed, the percentage of failed requests will decrease, and the Alert will turn off by itself.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.84 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST

Table 8-219 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST

Field	Details
Description	Ingress Gateway traffic gets rejected more than 1% because of ratelimiting.
Summary	Ingress Gateway traffic gets rejected more than 1% because of ratelimiting.
Severity	Major
Expression	(sum by (namespace,pod) (rate(oc_ingressgateway_http_request_ratelimit_values_total {Allowed="false",app_kubernetes_io_name="occnp-ingress-gateway"}[2m])))/ (sum by (namespace,pod) (rate(oc_ingressgateway_http_request_ratelimit_values_total {app_kubernetes_io_name="occnp-ingress-gateway"}[2m]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.103
Metric Used	oc_ingressgateway_http_request_ratelimit_values_total
Recommended Actions	**Cause:** Alert is triggered when percentage of denied requests is above 1% of total tps.. **Diagnostic Information:** • Metric involved: oc_ingressgateway_http_request_ratelimit_values_total • Error observed: 429 Too Many Requests, NF_CONGESTION_RISK • Cause value: Allowed="false" • Condition: podProtectionByRateLimiting.enabled = true and podProtectionByRateLimiting.fillRate settings • Verification steps: – podProtectionByRateLimiting.fillRate to a lower value and podProtectionByRateLimiting.deniedRequestActions.action=REJECT for lower congestion level – Run 4500 TPS or above for SM traffic; – Confirm some request dropped with Error 429. – Verify that the alert get triggered. • Monitoring recommendations: – Monitor 4xx error; and counter increase for oc_ingressgateway_http_request_ratelimit_values_total{Allowed="false"} – Watch for spikes following client deployments. **Recovery:** • Check Network traffic burst and storm • Investigate traffic load balancer issues and network issues. • Review SM Service Resources • Restart or scale up resources temporarily if the system is congested • Reconfig setting for podProtectionByRateLimiting.fillRate to a higher value and assign podProtectionByRateLimiting.deniedRequestActions.action=REJECT to higher congestion level • Disable feature if this flow is the only one affected we can disable this feature as a last resource For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.85 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD

Table 8-220 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Name	UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD
Description	UE N1N2 Notification Rate containing requests of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 20 Percent of Total n1n2 notify Requests (current value: {{ $value }} %)
Summary	Above 20 percent of total N1N2 Notify Requests from AMF are containing MANAGE_UE_POLICY_COMMAND_REJECT
Severity	Minor
Expression	sum by (namespace) (rate(ue_n1_transfer_ue_notification_total{commandType="MANAGE_UE_POLICY_COMMAND_REJECT"}[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 20 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.91
Metric Used	• ue_n1_transfer_ue_notification_total • ue_n1_transfer_response_total
Recommended Actions	**Cause**: At least 20 % of the sent UE Notifications sent are due to MANAGE_UE_POLICY_COMMAND_REJECT. Which means that a fragment delivered by PCF was rejected by UE. **Diagnostic Information**: • Configurations: Check UE configurations and PRE Policies to understand why these requests could've been rejected. • **Logs**: Check PCF UE and PRE logs to better understand why it could've been rejected. **Recovery**: Once UE Notifications are properly processed, the percentage of rejected requests will decrease, and the alert will turn off by itself.

8.1.2.86 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD

Table 8-221 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name	UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD
Description	UE N1N2 Notification Rate containing requests of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 50 Percent of Total n1n2 notify Requests (current value: {{ $value }} %)
Summary	Above 50 percent of total N1N2 Notify Requests from AMF are containing MANAGE_UE_POLICY_COMMAND_REJECT
Severity	Major
Expression	sum by (namespace) (rate(ue_n1_transfer_ue_notification_total{commandType="MANAGE_UE_POLICY_COMMAND_REJECT"}[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.91
Metric Used	• ue_n1_transfer_ue_notification_total • ue_n1_transfer_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-221 (Cont.) UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: At least 50 % of the sent UE Notifications sent are due to MANAGE_UE_POLICY_COMMAND_REJECT. Which means that a fragment delivered by PCF was rejected by UE. **Diagnostic Information**: • Configurations: Check UE configurations and PRE Policies to understand why these requests could've been rejected. • **Logs**: Check PCF UE and PRE logs to better understand why it could've been rejected. **Recovery**: Once UE Notifications are properly processed, the percentage of rejected requests will decrease, and the alert will turn off by itself.

8.1.2.87 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD

Table 8-222 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name	UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD
Description	UE N1N2 Notification Rate containing requests of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 75 Percent of Total n1n2 notify Requests (current value: {{ $value }} %)
Summary	Above 75 percent of total N1N2 Notify Requests from AMF are containing MANAGE_UE_POLICY_COMMAND_REJECT
Severity	critical
Expression	sum by (namespace) (rate(ue_n1_transfer_ue_notification_total{commandType="MANAGE_UE_POLICY_COMMAND_REJECT"}[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.91
Metric Used	• ue_n1_transfer_ue_notification_total • ue_n1_transfer_response_total
Recommended Actions	**Cause**: At least 75 % of the sent UE Notifications sent are due to MANAGE_UE_POLICY_COMMAND_REJECT. Which means that a fragment delivered by PCF was rejected by UE. **Diagnostic Information**: • Configurations: Check UE configurations and PRE Policies to understand why these requests could've been rejected. • **Logs**: Check PCF UE and PRE logs to better understand why it could've been rejected. **Recovery**: Once UE Notifications are properly processed, the percentage of rejected requests will decrease, and the alert will turn off by itself.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.88 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD

Table 8-223 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Name	UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD
Description	Above 20 percent of total N1N2 Transfer Requests are of N1N2 Transfer failure notification Requests from AMF (current value: {{ $value }} %)
Summary	UE n1n2 transfer failure Notification Rate is above 20 percent of total n1n2 Transfers requests
Severity	minor
Expression	sum by (namespace) (rate(ue_n1_transfer_failure_notification_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 20 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.92
Metric Used	• ue_n1_transfer_failure_notification_total • ue_n1_transfer_response_total
Recommended Actions	**Cause**: At least 20 % of the sent N1N2 Transfer Requests have failed. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and AMF. Maybe N1N2 requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and UE logs to further investigate on why N1N2 Transfer requests are failing. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check AMF has proper retransmission and re-attempt configurations in place. **Recovery**: Once N1N2 Transfer requests are properly processed, the percentage of non-2xx responses will decrease, and the Alert will turn off by itself.

8.1.2.89 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Table 8-224 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name	UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD
Description	Above 50 percent of total N1N2 Transfer Requests are of N1N2 Transfer failure notification Requests from AMF (current value: {{ $value }} %)
Summary	UE n1n2 transfer failure Notification Rate is above 50 percent of total n1n2 Transfers requests
Severity	major
Expression	sum by (namespace) (rate(ue_n1_transfer_failure_notification_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.92
Metric Used	• ue_n1_transfer_failure_notification_total • ue_n1_transfer_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-224 (Cont.) UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause**: At least 50 % of the sent N1N2 Transfer Requests have failed. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and AMF. Maybe N1N2 requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and UE logs to further investigate on why N1N2 Transfer requests are failing. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check AMF has proper retransmission and re-attempt configurations in place. **Recovery**: Once N1N2 Transfer requests are properly processed, the percentage of non-2xx responses will decrease, and the Alert will turn off by itself.

8.1.2.90 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD

Table 8-225 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name	UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD
Description	Above 75 percent of total N1N2 Transfer Requests are of N1N2 Transfer failure notification Requests from AMF (current value: {{ $value }} %)
Summary	UE n1n2 transfer failure Notification Rate is above 75 percent of total n1n2 Transfers requests
Severity	critical
Expression	sum by (namespace) (rate(ue_n1_transfer_failure_notification_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.92
Metric Used	• ue_n1_transfer_failure_notification_total • ue_n1_transfer_response_total
Recommended Actions	**Cause**: At least 75 % of the sent N1N2 Transfer Requests have failed. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and AMF. Maybe N1N2 requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and UE logs to further investigate on why N1N2 Transfer requests are failing. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check AMF has proper retransmission and re-attempt configurations in place. **Recovery**: Once N1N2 Transfer requests are properly processed, the percentage of non-2xx responses will decrease, and the Alert will turn off by itself.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.91 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD

Table 8-226 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Name	UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD
Description	Out of the total UE n1n2 Transfers more than 20 percent of transfer requests have T3501 Timer expiry before n1n2 notify is reached from AMF for that transfer (current value: {{ $value }} %)
Summary	UE n1n2 Transfer T3501 timer expiry rate is above 20 percent of total n1n2 Transfers
Severity	minor
Expression	sum by (namespace) (rate(ue_n1_transfer_t3501_expiry_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 20 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.93
Metric Used	• ue_n1_transfer_t3501_expiry_total • ue_n1_transfer_response_total
Recommended Actions	**Cause**: At least 20 % of the sent N1N2 Transfer Requests have had its T3501 timer expired. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and AMF. Maybe N1N2 requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and UE logs to further investigate on why N1N2 Transfer requests are failing. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check AMF has proper retransmission and re-attempt configurations in place. If latency is too high, increase the T3501 Timer Duration field to a greater value. **Recovery**: Once N1N2 Transfer requests are properly processed, the percentage of expired T3501 timers will decrease, and the Alert will turn off by itself.

8.1.2.92 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD

Table 8-227 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name	UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD
Description	Out of the total UE n1n2 Transfers more than 50 percent of transfer requests have T3501 Timer expiry before n1n2 notify is reached from AMF for that transfer (current value: {{ $value }} %)
Summary	UE n1n2 Transfer T3501 timer expiry rate is above 50 percent of total n1n2 Transfers

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-227 (Cont.)
UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Severity	major
Expression	sum by (namespace) (rate(ue_n1_transfer_t3501_expiry_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.93
Metric Used	• ue_n1_transfer_t3501_expiry_total • ue_n1_transfer_response_total
Recommended Actions	**Cause**: At least 50 % of the sent N1N2 Transfer Requests have had its T3501 timer expired. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and AMF. Maybe N1N2 requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and UE logs to further investigate on why N1N2 Transfer requests are failing. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check AMF has proper retransmission and re-attempt configurations in place. If latency is too high, increase the T3501 Timer Duration field to a greater value. **Recovery**: Once N1N2 Transfer requests are properly processed, the percentage of expired T3501 timers will decrease, and the Alert will turn off by itself.

8.1.2.93 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD

Table 8-228 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name	UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD
Description	Out of the total UE n1n2 Transfers more than 75 percent of transfer requests have T3501 Timer expiry before n1n2 notify is reached from AMF for that transfer (current value: {{ $value }} %)
Summary	UE n1n2 Transfer T3501 Timer expiry rate is above 75 percent of total n1n2 Transfers
Severity	critical
Expression	sum by (namespace) (rate(ue_n1_transfer_t3501_expiry_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 >= 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.93
Metric Used	• ue_n1_transfer_t3501_expiry_total • ue_n1_transfer_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-228 (Cont.)
UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause**: At least 75 % of the sent N1N2 Transfer Requests have had its T3501 timer expired. **Diagnostic Information**: • **Analyze Latency**: Check how much latency there is between PCF and AMF. Maybe N1N2 requests are not being sent, or taking too long to reach. • **Review Logs**: Check PCF's EGW and UE logs to further investigate on why N1N2 Transfer requests are failing. • **Scale System Resources**: High CPU or memory usage may lead to some requests to not be processed. Scale pods as required by the traffic. • **Configuration**: Check AMF has proper retransmission and re-attempt configurations in place. If latency is too high, increase the T3501 Timer Duration field to a greater value. **Recovery**: Once N1N2 Transfer requests are properly processed, the percentage of expired T3501 timers will decrease, and the Alert will turn off by itself.

8.1.2.94 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL_THRESHOLD

Table 8-229 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_error_response_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.111
Metric Used	ocpm_handle_update_notify_error_response_as_pending_confirmation_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-229 (Cont.) RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	Cause: Metric ocpm_handle_update_notify_error_response_as_pending_confirmation_total is pegged when the operation Update Notify towards SMF ends up with an Error • Metrics: ocpm_handle_update_notify_error_response_as_pending_confirmation_total – This will be incremented when configuration flag SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED is enabled and specific error error is added in SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPOMNSE_CODE and timeout happens during update notify triggered by AAR-I and AAR-U. • Alarm Condition: – If more than or equal to 70% of update_notify total requests fails with configured errorCode, an alarm is raised Diagnostic Information: • Check Network Latency – Investigate possible delays in network which is resulting in timeouts • Verify sender information – Verify if the notifUri where we are sending the information is correct • Verify receiver NF – Verify that the SMF that is receiving the traffic is in a healthy state • Review application – Verify if Sm is not congested – If signs like constant error logs are showing – Monitor System/resource utilization (CPU, Memory, queues) Recover: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF and the SM Service. Resolve any high latency or packet loss immediately if detected. • Review SM Service Application and Resources – Restart or scale up resources temporarily if the system is overloaded • Disable feature – if this flow is the only one affected we can disable this feature as a last resource For any additional guidance, contact My Oracle Support.

8.1.2.95 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_THRESHOLD

Table 8-230 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 50% in a given time period.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-230 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_THRESHOLD

Field	Details
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 50% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_error_response_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.111
Metric Used	ocpm_handle_update_notify_error_response_as_pending_confirmation_total
Recommended Actions	Cause: Metric ocpm_handle_update_notify_error_response_as_pending_confirmation_total is pegged when the operation Update Notify towards SMF ends up with an Error • Metrics: ocpm_handle_update_notify_error_response_as_pending_confirmation_total – This will be incremented when configuration flag SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED is enabled and specific error error is added in SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPOMNSE_CODE and timeout happens during update notify triggered by AAR-I and AAR-U. • Alarm Condition: – If more than or equal to 50% but less than 70% of update_notify total requests fails with configured errorCode, an alarm is raised Diagnostic Information: • Check Network Latency – Investigate possible delays in network which is resulting in timeouts • Verify sender information – Verify if the notifUri where we are sending the information is correct • Verify receiver NF – Verify that the SMF that is receiving the traffic is in a healthy state • Review application – Verify if Sm is not congested – If signs like constant error logs are showing – Monitor System/resource utilization (CPU, Memory, queues) Recover: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF and the SM Service. Resolve any high latency or packet loss immediately if detected. • Review SM Service Application and Resources – Restart or scale up resources temporarily if the system is overloaded • Disable feature – if this flow is the only one affected we can disable this feature as a last resource For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.96 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_THRESHOLD

Table 8-231 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_error_response_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm", responseCode=~"5xx/4xx"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.111
Metric Used	ocpm_handle_update_notify_error_response_as_pending_confirmation_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-231 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	Cause: Metric **ocpm_handle_update_notify_error_response_as_pending_confirmation_total** is pegged when the operation **Update Notify** towards SMF ends up with an error. **Metrics:** • **ocpm_handle_update_notify_error_response_as_pending_confirmation_total** – This will be incremented when: * Configuration flag `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED` is enabled, and * A specific error is added in `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPONSE_CODE`, and * A timeout happens during Update Notify triggered by AAR-I and AAR-U. **Alarm Condition:** • If **≥50% and < 70%** of update_notify total requests fail with the configured error code, an alarm is raised. **Diagnostic Information:** • **Check Network Latency** – Investigate possible delays in the network that are resulting in timeouts. • **Verify Sender Information** – Verify if the `notifUri` where we are sending the information is correct. • **Verify Receiver NF** – Verify that the SMF receiving the traffic is in a healthy state. • **Review Application** – Verify that SM is not congested. – Check for constant error logs. – Monitor system/resource utilization (CPU, memory, queues). **Recover:** • **Check Network Latency and Connectivity** – Investigate any current network issues or bottlenecks between the external NF and the SM service. – Resolve any high latency or packet loss immediately if detected. • **Review SM Service Application and Resources** – Restart or scale up resources temporarily if the system is overloaded. • **Disable Feature** – If this flow is the only one affected, disable this feature as a last resort.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.97 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHOLD

Table 8-232 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_timeout_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.112
Metric Used	ocpm_handle_update_notify_timeout_as_pending_confirmation_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-232 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHOLD

Field	Details

Recommended Actions	**Cause:**
	Metric **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** is pegged when the **Update Notify** operation towards SMF ends up with a timeout.
	Metrics:
	• **ocpm_handle_update_notify_timeout_as_pending_confirmation_total**
	– This will be incremented when:
	* Configuration flag
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED`
	is enabled, and
	* A specific error is added in
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS`
	, and
	* A timeout happens during Update Notify triggered by AAR-I and AAR-U.
	Alarm Condition:
	• If ⩾**70%** of update_notify total requests fail with a timeout, an alarm is raised.
	Diagnostic Information:
	• **Check Network Latency**
	– Investigate possible delays in the network that are resulting in timeouts.
	• **Verify Sender Information**
	– Verify if the
	`notifUri`
	where we are sending the information is correct.
	• **Verify Receiver NF**
	– Verify that the SMF receiving the traffic is in a healthy state.
	• **Review Application**
	– Verify that SM is not congested.
	– Check for constant error logs.
	– Monitor system/resource utilization (CPU, memory, queues).
	Recover:
	• **Check Network Latency and Connectivity**
	– Investigate any current network issues or bottlenecks between the external NF and the SM service.
	– Resolve any high latency or packet loss immediately if detected.
	• **Review SM Service Application and Resources**
	– Restart or scale up resources temporarily if the system is overloaded.
	• **Disable Feature**
	– If this flow is the only one affected, disable this feature as a last resort.
	For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.98 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD

Table 8-233 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify that failed because a timeout is equal or above 50% but less than 70% in a given time period.
Summary	This alert is triggered when the number of update notify that failed because a timeout is equal or above 50% but less than 70% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_timeout_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.112
Metric Used	ocpm_handle_update_notify_timeout_as_pending_confirmation_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-233 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	Cause: Metric **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** is pegged when the operation Update Notify towards SMF ends up with a timeout. • Metrics: **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** – This will be incremented when the configuration flag SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED is enabled and a specific error is added in SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS, and a timeout happens during update notify triggered by AAR-I and AAR-U. • Alarm Condition: – If more than or equal to 50% but less than 70% of update_notify total requests fail with a timeout, an alarm is raised. Diagnostic Information: • Check Network Latency – Investigate possible delays in the network which are resulting in timeouts. • Verify sender information – Verify if the notifUri where we are sending the information is correct. • Verify receiver NF – Verify that the SMF that is receiving the traffic is in a healthy state. • Review application – Verify if SM is not congested. – Look for signs such as constant error logs. – Monitor system/resource utilization (CPU, memory, queues). Recover: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF and the SM Service. Resolve any high latency or packet loss immediately if detected. • Review SM Service Application and Resources – Restart or scale up resources temporarily if the system is overloaded. • Disable feature – If this flow is the only one affected, you can disable this feature as a last resort. For any additional guidance, contact My Oracle Support.

8.1.2.99 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Table 8-234 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify that failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-234 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Field	Details
Summary	This alert is triggered when the number of update notify that failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_timeout_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.112
Metric Used	ocpm_handle_update_notify_timeout_as_pending_confirmation_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-234 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Field	Details

Recommended Actions	**Cause:**
	Metric **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** is pegged when the **Update Notify** operation towards SMF ends up with a timeout.
	Metrics:
	• **ocpm_handle_update_notify_timeout_as_pending_confirmation_total**
	– This will be incremented when:
	* Configuration flag
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED`
	is enabled, and
	* A specific error is added in
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS`
	, and
	* A timeout happens during Update Notify triggered by AAR-I and AAR-U.
	Alarm Condition:
	• If ≥**30% and < 50%** of update_notify total requests fail with a timeout, an alarm is raised.
	Diagnostic Information:
	• **Check Network Latency**
	– Investigate possible delays in the network that are resulting in timeouts.
	• **Verify Sender Information**
	– Verify if the
	`notifUri`
	where we are sending the information is correct.
	• **Verify Receiver NF**
	– Verify that the SMF receiving the traffic is in a healthy state.
	• **Review Application**
	– Verify that SM is not congested.
	– Check for constant error logs.
	– Monitor system/resource utilization (CPU, memory, queues).
	Recover:
	• **Check Network Latency and Connectivity**
	– Investigate any current network issues or bottlenecks between the external NF and the SM service.
	– Resolve any high latency or packet loss immediately if detected.
	• **Review SM Service Application and Resources**
	– Restart or scale up resources temporarily if the system is overloaded.
	• **Disable Feature**
	– If this flow is the only one affected, disable this feature as a last resort.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-234 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Field	Details
	For any additional guidance, contact My Oracle Support.

8.1.2.100 PCF_STATE_NON_FUNCTIONAL_CRITICAL

Table 8-235 PCF_STATE_NON_FUNCTIONAL_CRITICAL

Field	Details
Description	Policy is in non functional state due to DB cluster state down.
Summary	Policy is in non functional state due to DB cluster state down.
Severity	Critical
Expression	appinfo_nfDbFunctionalState_current{nfDbFunctionalState="Not_Running"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.102
Metric Used	appinfo_nfDbFunctionalState_current
Recommended Actions	For any additional guidance, contact My Oracle Support.

8.1.2.101 UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Table 8-236 UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code!~"2.*",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.108
Metric Used	ocpm_udr_tracking_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-236 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR is received in UDR connector. This alert is notifying when the number of responses received from UDR for operation resubscribe that failed is above the threshold mentioned. **Cause:** The **ocpm_udr_tracking_response_total** metric is pegged whenever a response is received from the UDR in the UDR Connector. In this case, alerts are triggered when the number of failed responses received from UDR for the **resubscribe** operation exceeds the configured threshold. This alert is triggered when **more than 50% but less than 70%** of GET calls for UDR revalidation (`operation_type=resubscribe`, `service_resource=subscription-revalidation`) sent by the **PCF-UserService** fail (i.e., receive non-2xx HTTP response codes). **Diagnostic Information:** 1. **Check Recent Logs** • Review logs from the **PCF UDR Connector** and **Egress Gateway** for the relevant time intervals. • Review errors at **SCP routing**. • Identify the failure responses—look for non-2xx HTTP status codes and any error payloads. 2. **Analyze Failure Patterns** • Determine if failures are tied to specific UDRs, subscriber groups, or are distributed across all revalidations. • Assess whether there is a spike in failed revalidations or if failures are intermittent. 3. **Inspect UDR Health and Reachability** • Verify the health and responsiveness of the UDR service. • Check network connectivity from the PCF to UDR; look for timeouts, DNS errors, or other connectivity issues in intermediary services (EGW, SCP). 4. **Review PCF–UDR Connector Configuration** • Ensure proper configuration of endpoints, service credentials, and connection settings between PCF and UDR. • Review any recent configuration or deployment changes that might correspond to the start of failures. 5. **Check for Resource or Rate Limiting** • Evaluate whether there are signs of resource exhaustion (CPU, memory, network) on either service. • Investigate if the UDR is rate-limiting incoming requests or experiencing overload. 6. **Correlate with Related Alerts or Incidents** • Cross-check whether other alerts in the same namespace indicate broader issues (e.g., infrastructure, dependency outages, authentication errors). **Recovery:** 1. **Restore UDR Service Health** • Address any service outages, restarts, or degraded performance on the UDR side.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-236 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
	• If resource constraints are detected, consider scaling UDR or optimizing load. 2. **Fix Connectivity or Configuration Issues** • Resolve network issues (latency, DNS, firewall). • Correct any erroneous endpoint URLs or authentication parameters in PCF User or UDR Connector configurations. For any additional guidance, contact My Oracle Support.

8.1.2.102 UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Table 8-237 UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code!~"2.*",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.108
Metric Used	ocpm_udr_tracking_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-237 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR is received in UDR connector. This alert is notifying when the number of responses received from UDR for operation resubscribe that failed is above the threshold mentioned. **Cause:** The **ocpm_udr_tracking_response_total** metric is pegged whenever a response is received from the UDR in the UDR Connector. In this case, alerts are triggered when the number of failed responses received from UDR for the **resubscribe** operation exceeds the configured threshold. This alert is triggered when **more than 70%** of GET calls for UDR revalidation (`operation_type=resubscribe`, `service_resource=subscription-revalidation`) sent by the **PCF-UserService** fail (i.e., receive non-2xx HTTP response codes). **Diagnostic Information:** 1. **Check Recent Logs** • Review logs from **PCF UDR Connector** and **Egress Gateway** for the relevant time intervals. • Review errors at **SCP routing**. • Identify the failure responses — look for non-2xx HTTP status codes and any error payloads. 2. **Analyze Failure Patterns** • Determine if failures are tied to specific UDRs, subscriber groups, or are distributed across all revalidations. • Assess whether there is a spike in failed revalidations or if failures are intermittent. 3. **Inspect UDR Health and Reachability** • Verify the health and responsiveness of the UDR service. • Check network connectivity from the PCF to UDR; look for timeouts, DNS errors, or other connectivity issues in intermediary services (EGW, SCP). 4. **Review PCF–UDR Connector Configuration** • Ensure proper configuration of endpoints, service credentials, and connection settings between PCF and UDR. • Review any recent configuration or deployment changes that might correspond to the start of failures. 5. **Check for Resource or Rate Limiting** • Evaluate whether there are signs of resource exhaustion (CPU, memory, network) on either service. • Investigate if the UDR is rate-limiting incoming requests or experiencing overload. 6. **Correlate with Related Alerts or Incidents** • Cross-check whether other alerts in the same namespace indicate broader issues (e.g., infrastructure, dependency outages, authentication errors). **Recovery:** 1. **Restore UDR Service Health** • Address any service outages, restarts, or degraded performance on the UDR side. • If resource constraints are detected, consider scaling UDR or optimizing load.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-237 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
	2. **Fix Connectivity or Configuration Issues** • Resolve network issues (latency, DNS, firewall). • Correct any erroneous endpoint URLs or authentication parameters in PCF User or UDR Connector configurations. For any additional guidance, contact My Oracle Support.

8.1.2.103 UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Table 8-238 UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code!~"2.*",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.108
Metric Used	ocpm_udr_tracking_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-238 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Field	Details

Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR is received in UDR connector. This alert is notifying when the number of responses received from UDR for operation resubscribe that failed is above the threshold mentioned.
	Cause:
	The **ocpm_udr_tracking_response_total** metric is pegged whenever we receive a response from the UDR in the UDR Connector.
	In this case, alerts are triggered when the number of failed responses received from UDR for the **resubscribe** operation is above the configured threshold.
	This alert is triggered when **more than 30% but less than 50%** of GET calls for UDR revalidation
	(
	`operation_type=resubscribe`
	,
	`service_resource=subscription-revalidation`
	) sent by the **PCF-UserService** fail (i.e., receive non-2xx HTTP response codes).
	Diagnostic Information:
	1. **Check Recent Logs**
	• Review logs from the **PCF UDR Connector** and **Egress Gateway** for the relevant time intervals.
	• Review errors at **SCP routing**.
	• Identify the failure responses — look for non-2xx HTTP status codes and any error payloads.
	2. **Analyze Failure Patterns**
	• Determine if failures are tied to specific UDRs, subscriber groups, or are distributed across all revalidations.
	• Assess if there is a spike in failed revalidations or if failures are intermittent.
	3. **Inspect UDR Health and Reachability**
	• Verify the health and responsiveness of the UDR service.
	• Check network connectivity from the PCF to UDR; look for timeouts, DNS errors, or other connectivity issues in intermediary services (EGW, SCP).
	4. **Review PCF–UDR Connector Configuration**
	• Ensure proper configuration of endpoints, service credentials, and connection settings between PCF and UDR.
	• Review any recent configuration or deployment changes that might correspond to the start of failures.
	5. **Check for Resource or Rate Limiting**
	• Evaluate if there are signs of resource exhaustion (CPU, memory, network) on either service.
	• Investigate if the UDR is rate-limiting incoming requests or experiencing overload.
	6. **Correlate with Related Alerts or Incidents**

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-238 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
	• Cross-check if other alerts in the same namespace indicate broader issues (e.g., infrastructure, dependency outages, authentication errors). **Recovery:** 1. **Restore UDR Service Health** • Address any service outages, restarts, or degraded performance on the UDR side. • If resource constraints are detected, consider scaling UDR or optimizing load. 2. **Fix Connectivity or Configuration Issues** • Resolve network issues (latency, DNS, firewall). • Correct any erroneous endpoint URLs or authentication parameters in PCF User or UDR Connector configurations. For any additional guidance, contact My Oracle Support.

8.1.2.104 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT

Table 8-239 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed with status code 404 NOT FOUND.
Summary	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed with status code 404 NOT FOUND.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code="404",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.110
Metric Used	ocpm_udr_tracking_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-239 (Cont.) UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR in UDR connector is received. This alert notifies when the number of responses received from UDR for operation resubscribe that failed with a 404 Not Found is above the threshold mentioned. Cause: This alert is triggered when more than 70% of UDR revalidation GET operations managed by PCF fail with an HTTP 404 (Not Found) response code within the specified window. A 404 response indicates that the requested subscription for revalidation was not found in UDR. Diagnostic Information: 1. Check UDR logs: Look for 404 errors and the accompanying trigger request details (trigger of UDR revalidation request) for the affected time period. 2. Verify subscription states: Ensure that the subscriptions expected to be present actually exist and are not being deleted, expired, or unavailable. 3. Investigate Missing Subscriptions: • Determine why the revalidation call is being made for a non-existent subscription ID. If the subscription has gone stale, verify why an audit was not triggered for it. • Check if there is a data synchronization issue between the originator and UDR. 4. Look for patterns: Determine whether the 404s are concentrated in a particular user group. Recovery: 1. Audit Subscription Lifecycle: Ensure proper creation, update, and deletion workflows so stale subscription IDs are not reused or referenced. 2. Review Recent Deployments or Changes: Check whether recent code or configuration changes in **pcf_user** or UDR might have led to increased 404s. For any additional guidance, contact My Oracle Support.

8.1.2.105 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT

Table 8-240 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code="404",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 50 < 70

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-240 (Cont.) UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.110
Metric Used	ocpm_udr_tracking_response_total
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR in UDR connector is received. This alert notifies when the number of responses received from UDR for operation resubscribe that failed with a 404 Not Found is above the threshold mentioned. Cause: This alert is triggered when more than 50% (but less than 70%) of UDR revalidation GET operations managed by PCF fail with an HTTP 404 (Not Found) response code within the specified window. A 404 response indicates that the requested subscription for revalidation was not found in UDR. Diagnostic Information: 1. Check UDR logs: Look for 404 errors and the accompanying trigger request details (trigger of UDR revalidation request) for the affected time period. 2. Verify subscription states: Ensure that the subscriptions expected to be present actually exist and are not being deleted, expired, or unavailable. 3. Investigate missing subscriptions: • Determine why the revalidation call is being made for a non-existent subscription ID. If the subscription has gone stale, verify why an audit was not triggered for the same. • Check if there is a data synchronization issue between the originator and UDR. 4. Look for patterns: Determine whether the 404s are concentrated in a particular user group. Recovery: 1. Audit subscription lifecycle: Ensure proper creation, update, and deletion workflows so stale subscription IDs are not reused or referenced. 2. Review recent deployments or changes: Check whether recent code or configuration changes in pcf_user or UDR might have led to increased 404s. For any additional guidance, contact My Oracle Support.

8.1.2.106 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT

Table 8-241 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-241 (Cont.) UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code="404",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.110
Metric Used	ocpm_udr_tracking_response_total
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR in UDR connector is received. This alert notifies when the number of responses received from UDR for operation resubscribe that failed with a 404 Not Found is above the threshold mentioned. Cause: This alert is triggered when more than 30% (but less than 50%) of UDR revalidation GET operations managed by PCF fail with an HTTP 404 (Not Found) response code within the specified window. A 404 response indicates that the requested subscription for revalidation was not found in UDR. Diagnostic Information: 1. Check UDR logs: Look for 404 errors and the accompanying trigger request details (trigger of UDR revalidation request) for the affected time period. 2. Verify subscription states: Ensure that the subscriptions expected to be present actually exist and are not being deleted, expired, or unavailable. 3. Investigate missing subscriptions: • Determine why the revalidation call is being made for a non-existent subscription ID. If the subscription has gone stale, verify why an audit was not triggered for the same. • Check if there is a data synchronization issue between the originator and UDR. 4. Look for patterns: Determine whether the 404s are concentrated in a particular user group. Recovery: 1. Audit subscription lifecycle: Ensure proper creation, update, and deletion workflows so stale subscription IDs are not reused or referenced. 2. Review recent deployments or changes: Check whether recent code or configuration changes in **pcf_user** or UDR might have led to increased 404s. For any additional guidance, contact My Oracle Support.

8.1.2.107 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Table 8-242 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-242 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",imm_reports_present="false"}[5m])) / sum(rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.116
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-242 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing AM user data check is based on: * `service_subresource = "am-data"` (indicates the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `imm_reports_present = "false"` (indicates no AM user data was returned from UDR as part of the Immediate Reporting capability) – If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response without AM user data as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (e.g., `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.108 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Table 8-243 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.116
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-243 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing AM user data check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no AM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response **without** user data for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and still no AM user data is retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.109 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Table 8-244 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting.
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.116
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-244 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing AM user data check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no AM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response **without** user data for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in the request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.110 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Table 8-245 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.117
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-245 (Cont.) UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.111 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Table 8-246 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.117
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-246 (Cont.) UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The failed feature negotiation check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in the request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.112 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Table 8-247 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.117
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-247 (Cont.) UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "am-data"` (indicates the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `immediate_report_pcc = "false"` (indicates that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.113 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR

Table 8-248 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.118
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-248 (Cont.) UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The missing UE user data check is based on: * `service_subresource = "ue-policy-set"` (indicates the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `imm_reports_present = "false"` (indicates no UE user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response **without UE user data** as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and UE user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.114 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Table 8-249 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.118
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-249 (Cont.) UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The missing UE user data check is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no UE user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response **without UE user data** as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and UE user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.115 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Table 8-250 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Severity	CRITICAL
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.118
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-250 (Cont.) UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The missing UE user data check is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no UE user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response without UE user data as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.116 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Table 8-251 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.119
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-251 (Cont.) UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **10%** but less than **20%** of the traffic: UDR returned a POST Subscribe response with failed feature negotiation for UE as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.117 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Table 8-252 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.119
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-252 (Cont.) UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **20%** but less than **30%** of the traffic: UDR returned a POST Subscribe response with failed feature negotiation for UE as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.118 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Table 8-253 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.119
Metric Used	occnp_immrep_response_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-253 (Cont.) UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response with failed feature negotiation for UE as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the request payload for the UDR POST. 3. **Verify UDR Profile** • Ensure that User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.119 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERCENT

Table 8-254 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 60% in a given time period.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="403"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.120
Metric Used	occnp_pa_sponsored_sessions_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-254 (Cont.)
SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). **Cause:** Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **403 Requested Service Not Authorized** response. This occurs when the client sends a Sponsored request with `umcDataIncluded="false"` but the requested service is not authorized. As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. **Diagnostic Information:** • **Metric involved:**`occnp_pa_sponsored_sessions_total` • **Error observed:** 403 Requested Service Not Authorized • **Condition:** Unauthorized Sponsored Connectivity requests **Verification steps:** 1. Send a Sponsored Connectivity request with valid authorization and supported features. 2. Confirm the request succeeds. 3. Verify that the 403 / Requested Service Not Authorized ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Track the 4xx error ratio by caller/tenant and by sponsor/ASP. • Pay special attention to spikes after client deployments or policy/configuration changes. **Recovery:** 1. Identify the failing caller. 2. Review the request payload, entitlement, and policy configuration. 3. Confirm that the sponsor/ASP is authorized for the requested service. 4. Correct any misconfigurations in policy rules or subscription data. 5. Ensure that Sponsored Connectivity is supported in both the PCF SM Service and the PA Service. 6. Escalate if the issue persists after authorization or policy fixes, or if it impacts multiple tenants or partners.

8.1.2.120 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCENT

Table 8-255 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-255 (Cont.)
SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 40% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="403"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 40 < 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.120
Metric Used	occnp_pa_sponsored_sessions_total
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). **Cause:** Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **403 Requested Service Not Authorized** response. This occurs when the client sends a Sponsored request with `umcDataIncluded="false"` but the requested service is not authorized. As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. **Diagnostic Information:** • **Metric involved:**`occnp_pa_sponsored_sessions_total` • **Error observed:** 403 Requested Service Not Authorized • **Condition:** Unauthorized Sponsored Connectivity requests **Verification steps:** 1. Send a Sponsored Connectivity request with valid authorization and supported features. 2. Confirm the request succeeds. 3. Verify that the 403 / Requested Service Not Authorized ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Track the 4xx error ratio by caller/tenant and by sponsor/ASP. • Pay special attention to spikes after client deployments or policy/configuration changes. **Recovery:** 1. Identify the failing caller. 2. Review the request payload, entitlement, and policy configuration. 3. Confirm that the sponsor/ASP is authorized for the requested service. 4. Correct any misconfigurations in policy rules or subscription data. 5. Ensure that Sponsored Connectivity is supported in both the PCF SM Service and the PA Service. 6. Escalate if the issue persists after authorization or policy fixes, or if it impacts multiple tenants or partners.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.121 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCENT

Table 8-256 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 20% in a given time period.
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="403"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 20 < 40
OID	1.3.6.1.4.1.323.5.3.52.1.2.120
Metric Used	occnp_pa_sponsored_sessions_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-256 (Cont.)
SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **403 Requested Service Not Authorized** response. This occurs when the client sends a Sponsored request with `umcDataIncluded="false"`, but the requested service is not authorized. As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 403 Requested Service Not Authorized • **Condition:** Unauthorized Sponsored Connectivity requests **Verification steps:** 1. Send a Sponsored Connectivity request with valid authorization and supported features. 2. Confirm the request succeeds. 3. Verify that the 403 / Requested Service Not Authorized ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Track the 4xx error ratio by caller/tenant and by sponsor/ASP. • Pay special attention to spikes after client deployments or policy/configuration changes. Recovery: 1. Identify the failing caller. 2. Review the request payload, entitlement, and policy configuration. 3. Confirm that the sponsor/ASP is authorized for the requested service. 4. Correct any misconfigurations in policy rules or subscription data. 5. Ensure that Sponsored Connectivity is supported in both the PCF SM Service and the PA Service. 6. Escalate if the issue persists after authorization or policy fixes, or if it impacts multiple tenants or partners.

8.1.2.122 AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT

Table 8-257 AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 60% in a given time period.
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-257 (Cont.) AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="400",cause="MANDATORY_IE_MISSING"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.122
Metric Used	occnp_pa_sponsored_sessions_total
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **400 Bad Request** due to `cause="MANDATORY_IE_MISSING"`. This happens when the client sends a Sponsored Connectivity request missing one or more mandatory Information Elements (IEs). As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 400 Bad Request • **Cause value:** MANDATORY_IE_MISSING • **Condition:** Sponsored Connectivity requests missing mandatory IE fields • **Common missing IEs:** sponId, aspId, afAppId **Verification steps:** 1. Send a valid Sponsored Connectivity request including all mandatory IEs. 2. Ensure sponId and aspId are present and that Sponsored Connectivity is negotiated. 3. Confirm the request succeeds. 4. Verify that the 400 / MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Monitor the 4xx error ratio by caller/tenant and by sponsor/ASP. • Watch for spikes following client deployments or gateway transformation changes. Recovery: 1. Identify the failing caller. 2. Compare the request payload against the API contract. 3. Restore all mandatory IE fields (sponId, aspId, afAppId, etc.). 4. Review and fix any gateway or payload transformation issues. 5. Redeploy the corrected configuration or client. 6. Escalate if the issue persists after fixes or impacts multiple tenants.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.123 AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT

Table 8-258 AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 40% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="400",cause="MANDATORY_IE_MISSING"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 40 < 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.122
Metric Used	occnp_pa_sponsored_sessions_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-258 (Cont.) AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **400 Bad Request** due to `cause="MANDATORY_IE_MISSING"`. This happens when the client sends a Sponsored Connectivity request missing one or more mandatory Information Elements (IEs). As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 400 Bad Request • **Cause value:** MANDATORY_IE_MISSING • **Condition:** Sponsored Connectivity requests missing mandatory IE fields • **Common missing IEs:** sponId, aspId, afAppId **Verification steps:** 1. Send a valid Sponsored Connectivity request including all mandatory IEs. 2. Ensure sponId and aspId are present and that Sponsored Connectivity is negotiated. 3. Confirm the request succeeds. 4. Verify that the 400 / MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Monitor the 4xx error ratio by caller/tenant and by sponsor/ASP. • Watch for spikes following client deployments or gateway transformation changes. Recovery: 1. Identify the failing caller. 2. Compare the request payload against the API contract. 3. Restore all mandatory IE fields (sponId, aspId, afAppId, etc.). 4. Review and fix any gateway or payload transformation issues. 5. Redeploy the corrected configuration or client. 6. Escalate if the issue persists after fixes or impacts multiple tenants.

8.1.2.124 AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT

Table 8-259 AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 20% in a given time period.
Severity	Minor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-259 (Cont.) AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="400",cause="MANDATORY_IE_MISSING"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 20 < 40
OID	1.3.6.1.4.1.323.5.3.52.1.2.122
Metric Used	occnp_pa_sponsored_sessions_total
Recommended Actions	If this alert is triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **400 Bad Request** due to `cause="MANDATORY_IE_MISSING"`. This happens when the client sends a Sponsored Connectivity request missing one or more mandatory Information Elements (IEs). As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 400 Bad Request • **Cause value:** MANDATORY_IE_MISSING • **Condition:** Sponsored Connectivity requests missing mandatory IE fields • **Common missing IEs:** sponId, aspId, afAppId **Verification steps:** 1. Send a valid Sponsored Connectivity request including all mandatory IEs. 2. Ensure sponId and aspId are present and that Sponsored Connectivity is negotiated. 3. Confirm the request succeeds. 4. Verify that the 400 / MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Monitor the 4xx error ratio by caller/tenant and by sponsor/ASP. • Watch for spikes following client deployments or gateway transformation changes. Recovery: 1. Identify the failing caller. 2. Compare the request payload against the API contract. 3. Restore all mandatory IE fields (sponId, aspId, afAppId, etc.). 4. Review and fix any gateway or payload transformation issues. 5. Redeploy the corrected configuration or client. 6. Escalate if the issue persists after fixes or impacts multiple tenants.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.125 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD

Table 8-260 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	At least 30% (but less than 50%) of N1N2Transfer requests have failed with a "retryAfter IE" timer within the last 5 mins
Summary	At least 30% (but less than 50%) of N1N2Transfer requests have failed with a "retryAfter IE" timer within the last 5 mins
Severity	Minor
Expression	(sum by (namespace) (increase(occnp_n1n2transfer_error_with_retryafter_seconds_count{microservice=~".*pcf_ueservice"}[5m]))) / (sum by (namespace) (increase(http_out_conn_response_total{operationType="transfer",microservice=~".*pcf_ueservice",responseCode!="2xx"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.135
Metric Used	occnp_n1n2transfer_error_with_retryafter_seconds_count
Recommended Actions	Cause: This alert gets triggered when the percentage of N1N2Transfer failures containing a retryAfter exceed defined thresholds within a 5-minute window. When `occnp_n1n2transfer_error_with_retryafter_seconds_count` increases, it indicates: • UE is not reachable. • AMF is instructing PCF to retry after a specified interval. • Transfer is delayed, not permanently failed. • High percentage indicates increasing UE unreachability or signaling instability between AMF and UE. Diagnostics Information: • Check retryAfter failure percentage trend. • Filter by response_code, amf_id, mcc, mnc. • Review retryAfter histogram buckets (0–600s, 600–3600s, >3600s). • Correlate with UE health and signaling load. Recovery: • Validate if spike is transient. • Investigate UE reach ability issues. • Escalate if sustained at Major or Critical level.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Note

- `UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_*` alerts mean AMF is returning retryAfter IE values for a high percentage of N1N2Transfer requests. This usually means AMF cannot currently reach the UE and requests PCF to wait before retrying.
- `UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_*` alerts mean AMF returned a retryAfter IE value that is <=0 or greater than 600 seconds.
- For a value <=0, PCF uses normal session retry behavior.
- For a value >600, PCF caps the value at 600 seconds.
- The following must be verified manually:
  - **Enable Retry After IE** is enabled in the Retry Profile.
  - `RETRY.AFTER.IE.MAX.SECONDS` is between 1 and 600; default 600.
  - `RETRY.AFTER.IE.TIMER.CAPACITY` is appropriate; default 50,000.
  - `RETRY.AFTER.IE.TIMER.RATE` is appropriate; default 50 per second.
  - UE Policy service is registered with Timer Service.
  - The affected AMF and UE are reachable.
  - Alert dimensions such as AMF ID, MCC, MNC, and response code identify the affected AMF.
- The feature supports retryAfter IE in the N1N2 response payload only. It does not support the HTTP Retry-After header.

8.1.2.126 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Table 8-261 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	At least 50% (but less than 70%) of N1N2Transfer requests have failed with a "retryAfter IE" timer within the last 5 mins
Summary	At least 50% (but less than 70%) of N1N2Transfer requests have failed with a "retryAfter IE" timer within the last 5 mins
Severity	Major
Expression	(sum by (namespace) (increase(occnp_n1n2transfer_error_with_retryafter_seconds_count{microservice=~".*pcf_ueservice"}[5m]))) / (sum by (namespace) (increase(http_out_conn_response_total{operationType="transfer",microservice=~".*pcf_ueservice",responseCode!="2xx"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.135

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-261 (Cont.) UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Metric Used	occnp_n1n2transfer_error_with_retryafter_seconds_count
Recommended Actions	Cause: This alert gets triggered when the percentage of N1N2Transfer failures containing a retryAfter exceed defined thresholds within a 5-minute window. When `occnp_n1n2transfer_error_with_retryafter_seconds_count` increases, it indicates: • UE is not reachable. • AMF is instructing PCF to retry after a specified interval. • Transfer is delayed, not permanently failed. • High percentage indicates increasing UE unreachability or signaling instability between AMF and UE. Diagnostics Information: • Check retryAfter failure percentage trend. • Filter by response_code, amf_id, mcc, mnc. • Review retryAfter histogram buckets (0–600s, 600–3600s, >3600s). • Correlate with UE health and signaling load. Recovery: • Validate if spike is transient. • Investigate UE reach ability issues. • Escalate if sustained at Major or Critical level.

8.1.2.127 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD

Table 8-262 UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	At least 70% of N1N2Transfer requests have failed with a "retryAfter IE" timer within the last 5 mins
Summary	At least 70% of N1N2Transfer requests have failed with a "retryAfter IE" timer within the last 5 mins
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-262 (Cont.)
UE_N1N2_TRANSFER_RETRYAFTER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(occnp_n1n2transfer_error_with_retryafter_seconds_count{microservice=~".*pcf_ueservice"}[5m]))) / (sum by (namespace) (increase(http_out_conn_response_total{operationType="transfer",microservice=~".*pcf_ueservice",responseCode!="2xx"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.135
Metric Used	occnp_n1n2transfer_error_with_retryafter_seconds_count
Recommended Actions	Cause: This alert gets triggered when the percentage of N1N2Transfer failures containing a retryAfter exceed defined thresholds within a 5-minute window. When `occnp_n1n2transfer_error_with_retryafter_seconds_count` increases, it indicates: • UE is not reachable. • AMF is instructing PCF to retry after a specified interval. • Transfer is delayed, not permanently failed. • High percentage indicates increasing UE unreachability or signaling instability between AMF and UE. Diagnostics Information: • Check retryAfter failure percentage trend. • Filter by response_code, amf_id, mcc, mnc. • Review retryAfter histogram buckets (0–600s, 600–3600s, >3600s). • Correlate with UE health and signaling load. Recovery: • Validate if spike is transient. • Investigate UE reach ability issues. • Escalate if sustained at Major or Critical level.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.128 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MINOR_THRESHOLD

Table 8-263 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	At least 30% (but less than 50%) of N1N2Transfer error responses in the last 5m have an invalid retryAfter IE value (greater than the allowed maximum).
Summary	At least 30% (but less than 50%) of N1N2Transfer error responses in the last 5m have an invalid retryAfter IE value (greater than the allowed maximum).
Severity	Minor
Expression	(sum by (namespace) (increase(occnp_n1n2transfer_error_retryafter_invalid_total{retry_after_gt_config_max="true",microservice=~".*pcf_ueservice"}[5m]))) / (sum by (namespace) (increase(occnp_n1n2transfer_error_with_retryafter_seconds_count{microservice=~".*pcf_ueservice"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.136
Metric Used	occnp_n1n2transfer_error_retryafter_invalid_total occnp_n1n2transfer_error_with_retryafter_seconds_count

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-263 (Cont.)
UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	Cause: • Triggered when the percentage of N1N2Transfer error responses containing an invalid retryAfter value exceeds defined thresholds within a 5-minute window. • Invalid means value greater than configured maximum (Advanced Settings). When `occnp_n1n2transfer_error_retryafter_invalid_total` increases, it indicates: • AMF is sending invalid retryAfter values. • If retryAfter 0, PCF falls back to normal session retry logic. • If retryAfter > configured max, PCF caps it to the configured maximum value – RETRY.AFTER.IE.MAX.SECONDS (This is the advance setting key used to set retryAfterIE max) • Service remains protected by fallback logic, but high percentage indicates signaling or configuration inconsistency. Diagnostics Information: • Check retryAfter failure percentage trend. • Filter by response_code, amf_id, mcc, mnc. • Review retry_after_le_zero and retry_after_gt_config_max dimensions. • Verify configured maximum retryAfter value. • Identify if issue is isolated to a specific AMF. Recovery: • Validate Advanced Settings configuration. • Check AMF configuration and behavior as why invalid values are sent. • Investigate configuration mismatch between PCF and AMF. • Escalate if sustained at Major or Critical level.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.2.129 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MAJOR_THRESHOLD

Table 8-264 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	At least 50% (but less than 70%) of N1N2Transfer error responses in the last 5m have an invalid retryAfter IE value (greater than the allowed maximum).
Summary	At least 50% (but less than 70%) of N1N2Transfer error responses in the last 5m have an invalid retryAfter IE value (greater than the allowed maximum).
Severity	Major
Expression	(sum by (namespace) (increase(occnp_n1n2transfer_error_retryafter_invalid_total{retry_after_gt_config_max="true",microservice=~".*pcf_ueservice"}[5m]))) / (sum by (namespace) (increase(occnp_n1n2transfer_error_with_retryafter_seconds_count{microservice=~".*pcf_ueservice"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.136
Metric Used	occnp_n1n2transfer_error_retryafter_invalid_total occnp_n1n2transfer_error_with_retryafter_seconds_count

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-264 (Cont.) UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	Cause: • Triggered when the percentage of N1N2Transfer error responses containing an invalid retryAfter value exceeds defined thresholds within a 5-minute window. • Invalid means value greater than configured maximum (Advanced Settings). When `occnp_n1n2transfer_error_retryafter_invalid_total` increases, it indicates: • AMF is sending invalid retryAfter values. • If retryAfter 0, PCF falls back to normal session retry logic. • If retryAfter > configured max, PCF caps it to the configured maximum value – RETRY.AFTER.IE.MAX.SECONDS (This is the advance setting key used to set retryAfterIE max) • Service remains protected by fallback logic, but high percentage indicates signaling or configuration inconsistency. Diagnostics Information: • Check retryAfter failure percentage trend. • Filter by response_code, amf_id, mcc, mnc. • Review retry_after_le_zero and retry_after_gt_config_max dimensions. • Verify configured maximum retryAfter value. • Identify if issue is isolated to a specific AMF. Recovery: • Validate Advanced Settings configuration. • Check AMF configuration and behavior as why invalid values are sent. • Investigate configuration mismatch between PCF and AMF. • Escalate if sustained at Major or Critical level.

8.1.2.130 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_CRITICAL_THRESHOLD

Table 8-265 UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	At least 70% of N1N2Transfer error responses in the last 5m have an invalid retryAfter IE value (greater than the allowed maximum).

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-265 (Cont.) UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Summary	At least 70% of N1N2Transfer error responses in the last 5m have an invalid retryAfter IE value (greater than the allowed maximum).
Severity	Critical
Expression	(sum by (namespace) (increase(occnp_n1n2transfer_error_retryafter_invalid_total{retry_after_gt_config_max="true",microservice=~".*pcf_ueservice"}[5m]))) / (sum by (namespace) (increase(occnp_n1n2transfer_error_with_retryafter_seconds_count{microservice=~".*pcf_ueservice"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.136
Metric Used	occnp_n1n2transfer_error_retryafter_invalid_total occnp_n1n2transfer_error_with_retryafter_seconds_count

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-265 (Cont.) UE_N1N2_TRANSFER_INVALID_RETRYAFTER_VALUE_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	Cause: • Triggered when the percentage of N1N2Transfer error responses containing an invalid retryAfter value exceeds defined thresholds within a 5-minute window. • Invalid means value greater than configured maximum (Advanced Settings). When `occnp_n1n2transfer_error_retryafter_invalid_total` increases, it indicates: • AMF is sending invalid retryAfter values. • If retryAfter 0, PCF falls back to normal session retry logic. • If retryAfter > configured max, PCF caps it to the configured maximum value – RETRY.AFTER.IE.MAX.SECONDS (This is the advance setting key used to set retryAfterIE max) • Service remains protected by fallback logic, but high percentage indicates signaling or configuration inconsistency. Diagnostics Information: • Check retryAfter failure percentage trend. • Filter by response_code, amf_id, mcc, mnc. • Review retry_after_le_zero and retry_after_gt_config_max dimensions. • Verify configured maximum retryAfter value. • Identify if issue is isolated to a specific AMF. Recovery: • Validate Advanced Settings configuration. • Check AMF configuration and behavior as why invalid values are sent. • Investigate configuration mismatch between PCF and AMF. • Escalate if sustained at Major or Critical level.

8.1.2.131 IGW_POD_PROTECTION_CONGESTED_STATE

Table 8-266 IGW_POD_PROTECTION_CONGESTED_STATE

Field	Details
Name	IGW_POD_PROTECTION_CONGESTED_STATE
Description	The Ingress Gateway is in Congested Level for the pod {{$labels.pod}} in namespace {{$labels.namespace}} (current congestion level: {{ $value }} %)
Summary	Ingress Gateway pod congestion state in Congested level.
Severity	critical
Expression	oc_ingressgateway_congestion_system_state{microservice=~".*ingress-gateway"} == 4

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-266 (Cont.) IGW_POD_PROTECTION_CONGESTED_STATE

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.123
Metric Used	oc_ingressgateway_congestion_system_state
Recommended Actions	**Cause**: Alert get triggered when the pod cpu consumption raises above the configured onset value for the CONGESTED level. **Diagnostic Information**: • Metric involved: oc_ingressgateway_congestion_system_state • Error observed: 429 Too Many Requests, NF_CONGESTION_RISK • Cause value: congestionConfig.levels.resources.onset value for CONGESTED level • Condition: podProtectionByRLConfigMode.enabled = true and congestionConfig.levels.value=4 and congestionConfig.levels.name=CONGESTED • Verification steps: – Set congestionConfig.levels.resources.onset to a lower value for CONGESTED level configuration; – Run 4500 TPS or above for SM traffic; – Confirm some request dropped with Error 429. – Verify that the alert get triggered. • Monitoring recommendations: – Monitor 4xx error; and CPU consumption for the pod in dashboard – Watch for spikes following client deployments. **Recovery**: • Check Network traffic burst and storm – Investigate traffic load balancer issues and network issues. • Review SM Service Resources – Restart or scale up resources temporarily if the system is congested • Disable feature – if this flow is the only one affected we can disable this feature as a last resource.

8.1.2.132 IGW_POD_PROTECTION_DOC_STATE

Table 8-267 IGW_POD_PROTECTION_DOC_STATE

Field	Details
Name	IGW_POD_PROTECTION_DOC_STATE
Description	The Ingress Gateway is in Danger_of_Congestion Level for the pod {{$labels.pod}} in namespace {{$labels.namespace}} (current congestion level: {{ $value }} %)
Summary	Ingress Gateway pod congestion state in Danger_of_Congestion Level.
Severity	Minor
Expression	oc_ingressgateway_congestion_system_state{microservice=~".*ingress-gateway"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.123
Metric Used	oc_ingressgateway_congestion_system_state

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-267 (Cont.) IGW_POD_PROTECTION_DOC_STATE

Field	Details
Recommended Actions	**Cause**: Alert get triggered when the pod cpu consumption raises above the configured onset value for the DANGER_OF_CONGESTION level. **Diagnostic Information**: • Metric involved: oc_ingressgateway_congestion_system_state • Error observed: 429 Too Many Requests, NF_CONGESTION_RISK • Cause value: congestionConfig.levels.resources.onset value for DANGER_OF_CONGESTION level • Condition: podProtectionByRLConfigMode.enabled = true and congestionConfig.levels.value=1 and congestionConfig.levels.name=DANGER_OF_CONGESTION • Verification steps: – Set congestionConfig.levels.resources.onset to a lower value for DANGER_OF_CONGESTION level configuration; – Run 4500 TPS or above for SM traffic; – Confirm some request dropped with Error 429. – Verify that the alert get triggered. • Monitoring recommendations: – Monitor 4xx error; and CPU consumption for the pod in dashboard – Watch for spikes following client deployments. **Recovery**: • Check Network traffic burst and storm – Investigate traffic load balancer issues and network issues. • Review SM Service Resources – Restart or scale up resources temporarily if the system is congested • Disable feature – if this flow is the only one affected we can disable this feature as a last resource.

8.1.2.133 EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Table 8-268 EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Field	Details
Name	EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
Description	Policy Egress Gateway Data Director unreachable for {{$labels.namespace}}.
Summary	kubernetes_namespace: {{$labels.kubernetes_namespace}}, timestamp: {{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}{{ end }} BSF Egress Gateway Data Director unreachable
Severity	Major
Expression	sum(oc_egressgateway_dd_unreachable) by(namespace,container) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.84
Metric Used	oc_egressgateway_dd_unreachable

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-268 (Cont.) EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Field	Details
Recommended Actions	**Cause**: Data Director for Egress Gateway is unreachable **Diagnostic Information**: • **Namespace health**: Verify that all pods are healthy and have enough CPU / Memory for the expected traffic. • **Logs**: Check EGW's Logs for more information on why it is unreachable. • **IP's**: Check that EGW's configured IP's are the correct, and Data Director is exposed for connections **Recovery**: As soon as EGW connects to is Data Director the Alert will turn off by itself.

8.1.2.134 INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Table 8-269 INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Field	Details
Name	INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
Description	Policy Ingress Gateway Data Director unreachable for {{$labels.namespace}}.
Summary	'kubernetes_namespace: {{$labels.kubernetes_namespace}}, timestamp: {{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}{{ end }} BSF Ingress Gateway Data Director unreachable'
Severity	major
Expression	sum(oc_ingressgateway_dd_unreachable) by(namespace,container) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.83
Metric Used	oc_ingressgateway_dd_unreachable
Recommended Actions	**Cause**: Data Director for Ingress Gateway is unreachable **Diagnostic Information**: • **Namespace health**: Verify that all pods are healthy and have enough CPU / Memory for the expected traffic. • **Logs**: Check IGW's Logs for more information on why it is unreachable. • **IP's**: Check that IGW's configured IP's are the correct, and Data Director is exposed for connections **Recovery**: As soon as IGW connects to is Data Director the Alert will turn off by itself.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3 PCRF Alerts

This section provides information about PCRF alerts.

8.1.3.1 PRE_UNREACHABLE_EXCEEDS_CRITICAL_THRESHOLD

Table 8-270 PRE_UNREACHABLE_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	PRE fail count exceeds the critical threshold limit.
Summary	Alert PRE unreachable NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	Critical
Expression	PRE fail count exceeds the critical threshold limit.
OID	1.3.6.1.4.1.323.5.3.44.1.2.9
Metric Used	http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}
Recommended Actions	**Cause:** `PRE_UNREACHABLE_EXCEEDS_CRITICAL_THRESHOLD` is raised when the PRE service becomes unreachable beyond the configured critical threshold. This usually indicates severe service unavailability caused by pod failures, service crashes, network interruptions, node issues, or deployment failures. It may also occur when the service is failing health checks, has backend connectivity problems, or is under extreme resource pressure. **Diagnostic Information:** Check the PRE pod status, restarts, and readiness/liveness probe failures. Verify the service is running using `kubectl get service -n <namespace>`. Review PRE service logs from Kibana to identify crashes, startup failures, or connectivity issues.Check whether there is a sudden surge in traffic or retry behavior from upstream services causing overload. Correlate the alert with recent deployments, configuration changes, or node-level incidents. Verify whether related dependent services are healthy and reachable. **Recovery:** Restart the affected PRE pods or perform a rolling restart if the failure is pod-specific. Rollback recent changes if the issue started after a deployment or configuration update. Fix the underlying cause such as resource exhaustion, probe failure, network issue, or dependency outage. If the service does not recover quickly, escalate to Oracle Support for further investigation.

8.1.3.2 PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD

Table 8-271 PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	PRE fail count exceeds the major threshold limit.
Summary	Alert PRE unreachable NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-271 (Cont.) PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	PRE fail count exceeds the major threshold limit.
OID	1.3.6.1.4.1.323.5.3.44.1.2.9
Metric Used	http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}
Recommended Actions	**Cause:** `PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD` is raised when the PRE service becomes unreachable beyond the configured threshold (between 80% to 90%). This usually indicates severe service unavailability caused by pod failures, service crashes, network interruptions, node issues, or deployment failures. It may also occur when the service is failing health checks, has backend connectivity problems, or is under extreme resource pressure. **Diagnostic Information:** Check the PRE pod status, restarts, and readiness/liveness probe failures. Verify the service is running using `kubectl get service -n <namespace>`. Review PRE service logs from Kibana to identify crashes, startup failures, or connectivity issues.Check whether there is a sudden surge in traffic or retry behavior from upstream services causing overload. Correlate the alert with recent deployments, configuration changes, or node-level incidents. Verify whether related dependent services are healthy and reachable. **Recovery:** Restart the affected PRE pods or perform a rolling restart if the failure is pod-specific. Rollback recent changes if the issue started after a deployment or configuration update. Fix the underlying cause such as resource exhaustion, probe failure, network issue, or dependency outage. If the service does not recover quickly, escalate to Oracle Support for further investigation.

8.1.3.3 PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD

Table 8-272 PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	PRE fail count exceeds the minor threshold limit.
Summary	Alert PRE unreachable NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	minor
Expression	sum(rate(http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}[5m])) / sum(rate(http_out_conn_response_total{container="pcrf-core",serviceResource="PRE"}[5m])) * 100 > 60 and sum(rate(http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}[5m])) / sum(rate(http_out_conn_response_total{container="pcrf-core",serviceResource="PRE"}[5m])) * 100 <=80
OID	1.3.6.1.4.1.323.5.3.44.1.2.9
Metric Used	http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-272 (Cont.) PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** `PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD` is raised when the PRE service becomes unreachable beyond the configured threshold (between 60% to 80%). This usually indicates severe service unavailability caused by pod failures, service crashes, network interruptions, node issues, or deployment failures. It may also occur when the service is failing health checks, has backend connectivity problems, or is under extreme resource pressure. **Diagnostic Information:** Check the PRE pod status, restarts, and readiness/liveness probe failures. Verify the service is running using `kubectl get service -n <namespace>`. Review PRE service logs from Kibana to identify crashes, startup failures, or connectivity issues.Check whether there is a sudden surge in traffic or retry behavior from upstream services causing overload. Correlate the alert with recent deployments, configuration changes, or node-level incidents. Verify whether related dependent services are healthy and reachable. **Recovery:** Restart the affected PRE pods or perform a rolling restart if the failure is pod-specific. Rollback recent changes if the issue started after a deployment or configuration update. Fix the underlying cause such as resource exhaustion, probe failure, network issue, or dependency outage. If the service does not recover quickly, escalate to Oracle Support for further investigation.

8.1.3.4 PCRF_DOWN

Table 8-273 PCRF_DOWN

Field	Details
Description	PCRF Service is down
Summary	Alert PCRF_DOWN NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	Critical
Expression	appinfo_service_running{service=~".*pcrf-core"} == 0
OID	1.3.6.1.4.1.323.5.3.44.1.2.33
Metric Used	appinfo_service_running{service=~".*pcrf-core"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-273 (Cont.) PCRF_DOWN

Field	Details
Recommended Actions	**Cause:** PCRF_DOWN is raised when the PCRF service becomes unavailable or stops responding. This can be caused by pod failures, service restarts, node issues, network interruptions, deployment problems, or upstream dependency failures. It may also occur when the service is unhealthy due to resource pressure, configuration issues, or backend connectivity problems. **Diagnostic Information:** Check PCRF pod status, restarts, and readiness/liveness probe failures. Verify the running status of the service using `kubectl get service -n <namespace>`. Review PCRF service logs from Kibana to identify crashes, startup failures, or connection issues. Check Grafana for CPU, memory, and network trends to see whether the service was under stress before going down. Correlate the alert with recent deployments, config changes, or node-level incidents. Verify whether related dependent services are healthy and reachable. **Recovery:** Restart the affected PCRF pods or perform a rolling restart if the failure is pod-specific. Rollback recent changes if the issue started after a deployment or configuration update. Fix the underlying cause such as resource exhaustion, probe failure, or dependency outage. If the service does not recover cleanly, escalate to Oracle Support for further investigation.

8.1.3.5 CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-274 CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	CCA fail count exceeds the critical threshold limit
Summary	Alert CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.13
Metric Used	occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-274 (Cont.) CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause:** CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD is raised when the number of failed Credit Control Answer (CCA) transactions exceeds the major threshold. This indicates a significant failure rate in credit control responses, typically caused by downstream charging system issues, connectivity problems, or invalid request handling. It may also result from timeout scenarios, misconfigurations, or increased load impacting CCR/CCA processing. **Diagnostic Information:** Check CCA failure count trends to determine whether the increase is sustained or a sudden spike. Analyze Diameter traffic metrics to identify failure response codes and patterns. Check the policy that is getting evaluated upon receiving CCR-I to identify any misconfigurations or evaluation failures. Correlate with upstream/downstream systems such as CHF/OCS to verify their health and responsiveness. Review logs in Kibana for CCR/CCA transactions to identify timeout errors, rejection causes, or connectivity issues. Check recent deployments or configuration changes impacting Diameter flows. **Recovery:** Fix underlying issues with downstream systems (e.g., CHF/OCS, UDR, LDAP availability, latency, or misconfiguration). Fix the policy in case the issue is caused by incorrect policy evaluation. Validate request formats and ensure proper handling of CCR/CCA messages. If failures are due to timeouts or load, consider scaling or tuning timeout/retry configurations. Rollback recent changes if the issue started after a deployment. The alert will clear once the CCA failure count drops below the major threshold.

8.1.3.6 CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-275 CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	CCA fail count exceeds the major threshold limit
Summary	Alert CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*"}[5m])) * 100 <=90
OID	1.3.6.1.4.1.323.5.3.44.1.2.13
Metric Used	occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-275 (Cont.) CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD is raised when the number of failed Credit Control Answer (CCA) transactions exceeds the major threshold. This indicates a significant failure rate in credit control responses, typically caused by downstream charging system issues, connectivity problems, or invalid request handling. It may also result from timeout scenarios, misconfigurations, or increased load impacting CCR/CCA processing. **Diagnostic Information:** Check CCA failure count trends to determine whether the increase is sustained or a sudden spike. Analyze Diameter traffic metrics to identify failure response codes and patterns. Check the policy that is getting evaluated upon receiving CCR-I to identify any misconfigurations or evaluation failures. Correlate with upstream/downstream systems such as CHF/OCS to verify their health and responsiveness. Review logs in Kibana for CCR/CCA transactions to identify timeout errors, rejection causes, or connectivity issues. Check recent deployments or configuration changes impacting Diameter flows. **Recovery:** Fix underlying issues with downstream systems (e.g., CHF/OCS, UDR, LDAP availability, latency, or misconfiguration). Fix the policy in case the issue is caused by incorrect policy evaluation. Validate request formats and ensure proper handling of CCR/CCA messages. If failures are due to timeouts or load, consider scaling or tuning timeout/retry configurations. Rollback recent changes if the issue started after a deployment. The alert will clear once the CCA failure count drops below the major threshold.

8.1.3.7 CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-276 CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	CCA fail count exceeds the minor threshold limit
Summary	Alert CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"CCA.*"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.44.1.2.13
Metric Used	occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-276 (Cont.) CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD is raised when the number of failed Credit Control Answer (CCA) transactions exceeds the major threshold. This indicates a significant failure rate in credit control responses, typically caused by downstream charging system issues, connectivity problems, or invalid request handling. It may also result from timeout scenarios, misconfigurations, or increased load impacting CCR/CCA processing. **Diagnostic Information:** Check CCA failure count trends to determine whether the increase is sustained or a sudden spike. Analyze Diameter traffic metrics to identify failure response codes and patterns. Check the policy that is getting evaluated upon receiving CCR-I to identify any misconfigurations or evaluation failures. Correlate with upstream/downstream systems such as CHF/OCS to verify their health and responsiveness. Review logs in Kibana for CCR/CCA transactions to identify timeout errors, rejection causes, or connectivity issues. Check recent deployments or configuration changes impacting Diameter flows. **Recovery:** Fix underlying issues with downstream systems (e.g., CHF/OCS, UDR, LDAP availability, latency, or misconfiguration). Fix the policy in case the issue is caused by incorrect policy evaluation. Validate request formats and ensure proper handling of CCR/CCA messages. If failures are due to timeouts or load, consider scaling or tuning timeout/retry configurations. Rollback recent changes if the issue started after a deployment. The alert will clear once the CCA failure count drops below the major threshold.

8.1.3.8 AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-277 AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	AAA fail count exceeds the critical threshold limit
Summary	Alert AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*", responseCode! ~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.34
Metric Used	occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-277 (Cont.) AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause:**The percentage of failed AAA (Authentication, Authorization, and Accounting) Diameter responses has exceeded the critical threshold (greater than 90%). This indicates that the majority of AAA requests are being rejected or encountering errors (non-2xx response codes), which may be due to backend system failures, misconfiguration, connectivity issues, or overload conditions. --- **Diagnostic Information:** • Metric evaluates: `Failed AAA Responses / Total AAA Responses * 100` over a 5-minute window • Failure is identified by Diameter response codes not starting with "2" (i.e., non-success responses). • Trigger condition: Failure rate > 90% • Key checks: – Inspect response codes (e.g., 4xxx, 5xxx) for error patterns – Verify connectivity to downstream systems (e.g., HSS/UDM, AAA servers) – Check recent configuration changes or deployments – Review system logs for spikes in errors or timeouts – Monitor load, latency, and resource utilization (CPU, memory, thread pools) – Validate if specific msgTypes (subset of AAA) are disproportionately failing --- **Recovery:** • Restore connectivity to dependent systems (AAA backend, subscriber databases) • Roll back recent configuration or deployment changes if correlated • Restart or scale affected services to handle load • Fix misconfigurations related to routing, policies, or credentials • Address specific error codes (e.g., authentication failure vs system error) • Implement traffic throttling or circuit breaking if overload is detected • Continue monitoring until failure rate drops below threshold • If the issue still persist please contact the support.

8.1.3.9 AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-278 AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	AAA fail count exceeds the major threshold limit
Summary	Alert AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*"}[5m])) * 100 <=90
OID	1.3.6.1.4.1.323.5.3.52.1.2.34
Metric Used	occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-278 (Cont.) AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** The percentage of failed AAA (Authentication, Authorization, and Accounting) Diameter responses has exceeded the major threshold (greater than 80%). This indicates a high rate of unsuccessful AAA transactions, though not yet at critical levels. It may signal emerging issues such as partial service degradation, backend instability, configuration inconsistencies, or increasing load impacting successful processing. **Diagnostic Information:** • Metric evaluates: `Failed AAA Responses / Total AAA Responses * 100` over a 5-minute window • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% • Key checks: – Analyze distribution of response codes (e.g., 3xxx, 4xxx, 5xxx) – Identify whether failures are intermittent or steadily increasing – Check health and responsiveness of dependent systems (HSS/UDM, AAA servers) – Review recent configuration changes, deployments, or scaling events – Examine logs for timeout errors, connection failures, or policy rejections – Monitor system performance metrics (CPU, memory, queue depth, latency) – Determine if specific AAA message types are more affected **Recovery:** • Investigate and stabilize backend dependencies (e.g., subscriber database, AAA services) • Roll back or correct recent configuration or deployment changes if applicable • Scale system resources or optimize performance to handle load • Resolve specific failure causes based on response codes • Apply traffic management strategies (rate limiting, retries, failover) • Perform targeted restarts of impacted components if necessary • Closely monitor trends to prevent escalation to critical threshold • If the issue still persist, Please contact the Support.

8.1.3.10 AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-279 AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	AAA fail count exceeds the minor threshold limit
Summary	Alert AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType=~"AAA.*"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.34

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-279 (Cont.) AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Metric Used	occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}
Recommended Actions	**Cause:** The percentage of failed AAA (Authentication, Authorization, and Accounting) Diameter responses has exceeded the minor threshold (greater than 60%). This indicates an early sign of degradation where a noticeable portion of AAA requests are failing. While the system may still be operational, this could point to developing issues such as intermittent backend failures, rising load, or minor misconfigurations. **Diagnostic Information:** • Metric evaluates: `Failed AAA Responses / Total AAA Responses * 100` over a 5-minute window • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% • Key checks: – Observe trends to see if failure rate is increasing toward major/critical thresholds – Review response code distribution to identify early error patterns – Check connectivity and latency to backend systems (HSS/UDM, AAA servers) – Inspect logs for intermittent errors, retries, or timeouts – Review recent configuration or deployment changes – Monitor system resource utilization (CPU, memory, threads, queues) – Identify if failures are isolated to specific AAA message types **Recovery:** • Investigate and address early signs of backend or connectivity issues • Validate configurations and recent changes for potential impact • Optimize system performance or scale resources if load is increasing • Resolve identified error patterns based on response codes • Apply preventive measures (e.g., retries tuning, connection pooling adjustments) • Continue close monitoring to prevent escalation to higher severity levels • If the issue still persist, Please contact the Support.

8.1.3.11 RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-280 RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Gx fail count exceeds the critical threshold limit
Summary	Alert RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.18

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-280 (Cont.) RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}
Recommended Actions	**Cause:** The percentage of failed RAA (Re-Auth Answer) messages on the Gx interface has exceeded the critical threshold (greater than 90%). This indicates that most re-authorization responses are failing, which can severely impact policy enforcement, session updates, and charging control. The issue is likely due to failures in communication with PCRF/PCF, policy inconsistencies, or system/resource issues. **Diagnostic Information:** • Metric evaluates: `Failed RAA (Gx) Responses / Total RAA (Gx) Responses * 100` over a 5-minute window • Scope: – `msgType = "RAA"` (Re-Auth Answer) – `appType = "Gx"` (Policy and Charging Control interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 90% • Key checks: – Analyze Diameter response codes (e.g., authorization failures, unable to comply, system errors) – Verify connectivity and health of PCRF/PCF systems – Check for policy rule mismatches or invalid re-authorization requests – Review logs for session state issues or failed updates – Monitor latency, timeouts, and retransmissions on the Gx interface – Inspect system resource utilization (CPU, memory, thread pools) – Correlate with spikes in re-auth requests or network events (e.g., QoS changes, session updates) **Recovery:** • Restore or stabilize connectivity with PCRF/PCF • Fix policy configuration issues or rule inconsistencies • Address specific Diameter error codes causing failures • Restart or scale affected components handling Gx traffic • Tune timeout and retry mechanisms if needed • Roll back recent changes impacting policy control or signaling • Continue monitoring until failure rate drops below the critical threshold • If the issue persists, please contact the Support.

8.1.3.12 RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-281 RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Gx fail count exceeds the major threshold limit
Summary	Alert RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-281 (Cont.) RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.18
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}
Recommended Actions	**Cause:** The percentage of failed RAA (Re-Auth Answer) messages on the Gx interface has exceeded the critical threshold (greater than 80%). This indicates that most re-authorization responses are failing, which can severely impact policy enforcement, session updates, and charging control. The issue is likely due to failures in communication with PCRF/PCF, policy inconsistencies, or system/resource issues. **Diagnostic Information:** • Metric evaluates: `Failed RAA (Gx) Responses / Total RAA (Gx) Responses * 100` over a 5-minute window • Scope: – `msgType = "RAA"` (Re-Auth Answer) – `appType = "Gx"` (Policy and Charging Control interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 80% • Key checks: – Analyze Diameter response codes (e.g., authorization failures, unable to comply, system errors) – Verify connectivity and health of PCRF/PCF systems – Check for policy rule mismatches or invalid re-authorization requests – Review logs for session state issues or failed updates – Monitor latency, timeouts, and retransmissions on the Gx interface – Inspect system resource utilization (CPU, memory, thread pools) – Correlate with spikes in re-auth requests or network events (e.g., QoS changes, session updates) **Recovery:** • Restore or stabilize connectivity with PCRF/PCF • Fix policy configuration issues or rule inconsistencies • Address specific Diameter error codes causing failures • Restart or scale affected components handling Gx traffic • Tune timeout and retry mechanisms if needed • Roll back recent changes impacting policy control or signaling • Continue monitoring until failure rate drops below the critical threshold • If the issue persists, please contact the Support.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.13 RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-282 RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Gx fail count exceeds the minor threshold limit
Summary	Alert RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.44.1.2.18
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-282 (Cont.) RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** The percentage of failed RAA (Re-Auth Answer) messages on the Gx interface has exceeded the critical threshold (greater than 60%). This indicates that most re-authorization responses are failing, which can severely impact policy enforcement, session updates, and charging control. The issue is likely due to failures in communication with PCRF/PCF, policy inconsistencies, or system/resource issues. **Diagnostic Information:** • Metric evaluates: `Failed RAA (Gx) Responses / Total RAA (Gx) Responses * 100` over a 5-minute window • Scope: – `msgType = "RAA"` (Re-Auth Answer) – `appType = "Gx"` (Policy and Charging Control interface) • Failure is defined as Diameter response codes not starting with "2" (non-success responses). • Trigger condition: Failure rate > 60% • Key checks: – Analyze Diameter response codes (e.g., authorization failures, unable to comply, system errors) – Verify connectivity and health of PCRF/PCF systems – Check for policy rule mismatches or invalid re-authorization requests – Review logs for session state issues or failed updates – Monitor latency, timeouts, and retransmissions on the Gx interface – Inspect system resource utilization (CPU, memory, thread pools) – Correlate with spikes in re-auth requests or network events (e.g., QoS changes, session updates) **Recovery:** • Restore or stabilize connectivity with PCRF/PCF • Fix policy configuration issues or rule inconsistencies • Address specific Diameter error codes causing failures • Restart or scale affected components handling Gx traffic • Tune timeout and retry mechanisms if needed • Roll back recent changes impacting policy control or signaling • Continue monitoring until failure rate drops below the critical threshold • If the issue persists, please contact the Support.

8.1.3.14 ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-283 ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA fail count exceeds the critical threshold limit
Summary	Alert ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-283 (Cont.) ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.17
Metric Used	occnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-283 (Cont.) ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details

Recommended Actions	**Cause:**
	A high failure rate of ASA responses returned by the remote peer indicates that ASR requests are not being successfully handled. Common causes include:
	• **Session does not exist (common):** `responseCode = 5002` means the **session doesn't exist** (already terminated/ aged out, state not found, or session identifier mismatch).
	• **Remote peer issues:** overload, internal errors, session/policy/state problems preventing ASR handling.
	• **Connectivity/routing problems:** intermittent network issues, routing/realm misconfiguration, peer unreachable leading to failed responses.
	• **Configuration mismatch:** incorrect peer configuration, realm/route, application/ capability negotiation issues.
	• **Traffic spike:** increased ASR volume causing the peer to reject requests or return error responses.
	• **Overload condition:** peer-side throttling/rejection or cascading failures due to sudden ASR storms.
	• **Widespread configuration issue:** incorrect routing tables, realm/peer identity mismatch introduced by a change.
	Diagnostic Information:
	1. Confirm current ASA failure rate Use the alert expression as-is to validate the observed error percentage.
	2. Identify dominant failure response codes.
	3. Check if overall ASA volume changed
	4. Determine whether the issue is peer-specific
	5. Review application and Diameter logs. Look for:
	  • peer disconnects / flapping connections
	  • timeouts, retransmits, watchdog failures
	  • "unable to route" / realm routing errors
	  • overload/congestion indications
	  • any recent config/deploy changes correlated with onset
	Recovery:
	• **Validate peer health and connectivity:** confirm the remote peer is up, reachable, and accepting traffic; check network/routing and Diameter peer status.
	• **Reduce load if needed:** if ASR volume is abnormal, identify the trigger and throttle upstream behavior where applicable.
	• **Fix routing/realm/config mismatches:** correct peer configuration, routing tables, realm mappings, or capability negotiation issues.
	• **Scale/restore capacity (peer or local):** if failures correlate with overload, scale the constrained component(s) or adjust resource limits.
	• **Rollback recent changes (if applicable):**
	  – revert recent configuration, routing, or deployment changes that align with the start of failures
	• **Mitigate overload:**
	  – reduce upstream triggers generating ASRs (where feasible)
	  – coordinate with peer team to increase capacity or adjust overload controls
	• **Verify recovery:** the alert clears automatically once the ASA non-2xxx rate stays below **90%** for the evaluation period.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.15 ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-284 ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA fail count exceeds the major threshold limit
Summary	Alert ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.44.1.2.17
Metric Used	occnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-284 (Cont.) ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details

Recommended Actions	**Cause:**
	A high failure rate of ASA responses returned by the remote peer indicates that ASR requests are not being successfully handled. Common causes include:
	• **Session does not exist (common):** `responseCode = 5002` means the **session doesn't exist** (already terminated/ aged out, state not found, or session identifier mismatch).
	• **Remote peer issues:** overload, internal errors, session/policy/state problems preventing ASR handling.
	• **Connectivity/routing problems:** intermittent network issues, routing/realm misconfiguration, peer unreachable leading to failed responses.
	• **Configuration mismatch:** incorrect peer configuration, realm/route, application/ capability negotiation issues.
	• **Traffic spike:** increased ASR volume causing the peer to reject requests or return error responses.
	• **Overload condition:** peer-side throttling/rejection or cascading failures due to sudden ASR storms.
	• **Widespread configuration issue:** incorrect routing tables, realm/peer identity mismatch introduced by a change.
	Diagnostic Information:
	1. Confirm current ASA failure rate Use the alert expression as-is to validate the observed error percentage.
	2. Identify dominant failure response codes.
	3. Check if overall ASA volume changed
	4. Determine whether the issue is peer-specific
	5. Review application and Diameter logs. Look for:
	  • peer disconnects / flapping connections
	  • timeouts, retransmits, watchdog failures
	  • "unable to route" / realm routing errors
	  • overload/congestion indications
	  • any recent config/deploy changes correlated with onset
	Recovery:
	• **Validate peer health and connectivity:** confirm the remote peer is up, reachable, and accepting traffic; check network/routing and Diameter peer status.
	• **Reduce load if needed:** if ASR volume is abnormal, identify the trigger and throttle upstream behavior where applicable.
	• **Fix routing/realm/config mismatches:** correct peer configuration, routing tables, realm mappings, or capability negotiation issues.
	• **Scale/restore capacity (peer or local):** if failures correlate with overload, scale the constrained component(s) or adjust resource limits.
	• **Rollback recent changes (if applicable):**
	  – revert recent configuration, routing, or deployment changes that align with the start of failures
	• **Mitigate overload:**
	  – reduce upstream triggers generating ASRs (where feasible)
	  – coordinate with peer team to increase capacity or adjust overload controls
	• **Verify recovery:** the alert clears automatically once the ASA non-2xxx rate stays below **80%** for the evaluation period.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.16 ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-285 ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA fail count exceeds the minor threshold limit
Summary	Alert ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.44.1.2.17
Metric Used	occnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-285 (Cont.) ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details

Recommended Actions	**Cause:**
	A high failure rate of ASA responses returned by the remote peer indicates that ASR requests are not being successfully handled. Common causes include:
	• **Session does not exist (common):** `responseCode = 5002` means the **session doesn't exist** (already terminated/ aged out, state not found, or session identifier mismatch).
	• **Remote peer issues:** overload, internal errors, session/policy/state problems preventing ASR handling.
	• **Connectivity/routing problems:** intermittent network issues, routing/realm misconfiguration, peer unreachable leading to failed responses.
	• **Configuration mismatch:** incorrect peer configuration, realm/route, application/ capability negotiation issues.
	• **Traffic spike:** increased ASR volume causing the peer to reject requests or return error responses.
	• **Overload condition:** peer-side throttling/rejection or cascading failures due to sudden ASR storms.
	• **Widespread configuration issue:** incorrect routing tables, realm/peer identity mismatch introduced by a change.
	Diagnostic Information:
	1. **Confirm current ASA failure rate** Use the alert expression as-is to validate the observed error percentage.
	2. Identify dominant failure response codes.
	3. Check if overall ASA volume changed
	4. Determine whether the issue is peer-specific
	5. Review application and Diameter logs. Look for:
	  • peer disconnects / flapping connections
	  • timeouts, retransmits, watchdog failures
	  • "unable to route" / realm routing errors
	  • overload/congestion indications
	  • any recent config/deploy changes correlated with onset
	Recovery:
	• **Validate peer health and connectivity:** confirm the remote peer is up, reachable, and accepting traffic; check network/routing and Diameter peer status.
	• **Reduce load if needed:** if ASR volume is abnormal, identify the trigger and throttle upstream behavior where applicable.
	• **Fix routing/realm/config mismatches:** correct peer configuration, routing tables, realm mappings, or capability negotiation issues.
	• **Scale/restore capacity (peer or local):** if failures correlate with overload, scale the constrained component(s) or adjust resource limits.
	• **Rollback recent changes (if applicable):**
	  – revert recent configuration, routing, or deployment changes that align with the start of failures
	• **Mitigate overload:**
	  – reduce upstream triggers generating ASRs (where feasible)
	  – coordinate with peer team to increase capacity or adjust overload controls
	• **Verify recovery:** the alert clears automatically once the ASA non-2xxx rate stays below **60%** for the evaluation period.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.17 ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-286 ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA timeout count exceeds the critical threshold limit
Summary	Alert ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.31
Metric Used	occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-286 (Cont.) ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause:** More than 90% of local Diameter ASA responses over 5 minutes are timing out. This usually means PCRF/Core (or the local Diameter stack) is not receiving ASA in time after sending ASR, most commonly due to peer reachability/latency issues, peer overload, routing/connection problems, or internal congestion causing the transaction to exceed timers. **Diagnostic Information:** 1) Confirm the ASA timeout ratio and volume (ensure denominator isn't near-zero) - Total ASA rate: sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) - ASA timeout rate: sum(rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) 2) Identify which peers/endpoints are driving timeouts (common useful labels: destHost, destRealm, reqDestHost, reqDestRealm, origHost) - sum by (destHost, destRealm) (rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) - If available: sum by (reqDestHost, reqDestRealm) (rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) 3) Check whether this is isolated to ASA or systemic across msgTypes - sum by (msgType, responseCode) (rate(occnp_diam_response_local_total{responseCode="timeout"}[5m])) 4) Correlate with pending/backlog and stale cleanup signals (names vary by deployment; use your actual metric names) - Pending in-flight: occnp_diam_pending_requests (or equivalent) - Stale cleanup: sum(rate(occnp_stale_diam_request_cleanup_total[5m])) (or equivalent) 5) Check related ASR activity (if you also export request-side metrics) - Look for spikes in abort activity leading to more ASR/ASA, and whether ASA timeouts track that spike. 6) Validate timer/transport symptoms - Peer connection flaps, TCP/SCTP retransmits, TLS issues (from Diameter stack logs / node metrics), and latency changes around the alert window. **Recovery:** 1) If timeouts are concentrated on a specific peer (destHost/destRealm). Validate peer health (CPU, thread pools, queue depth), connectivity, routing, firewall/ACL, and Diameter connection state. If supported, fail traffic away from the impacted peer / route to alternate peer. 2) If timeouts correlate with backlog/pending growth. Reduce load (throttling/ admission controls), scale out the impacted service, or address the resource bottleneck (CPU/memory/GC/thread pools). Ensure the Diameter stack isn't saturated (worker threads, queues). 3) If driven by network/transport issues. Fix underlying network faults (loss/latency), stabilize SCTP/TCP sessions, confirm MTU and TLS settings if applicable. 4) If timers are misaligned systemically. Review Diameter transaction timers and peer timeouts; adjust only per established engineering standards to avoid masking real performance problems. 5) Operational action (last resort). Restart/recycle the specific stuck peer process/ component only after addressing the underlying cause; verify ASA timeout % returns to baseline and pending requests drain.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.18 ASA_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-287 ASA_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA timeout count exceeds the major threshold limit
Summary	Alert ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.31
Metric Used	occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-287 (Cont.) ASA_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** More than 80% of local Diameter ASA responses over 5 minutes are timing out. This usually means PCRF/Core (or the local Diameter stack) is not receiving ASA in time after sending ASR, most commonly due to peer reachability/latency issues, peer overload, routing/connection problems, or internal congestion causing the transaction to exceed timers. **Diagnostic Information:** 1) Confirm the ASA timeout ratio and volume (ensure denominator isn't near-zero) - Total ASA rate: sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) - ASA timeout rate: sum(rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) 2) Identify which peers/endpoints are driving timeouts (common useful labels: destHost, destRealm, reqDestHost, reqDestRealm, origHost) - sum by (destHost, destRealm) (rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) - If available: sum by (reqDestHost, reqDestRealm) (rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) 3) Check whether this is isolated to ASA or systemic across msgTypes - sum by (msgType, responseCode) (rate(occnp_diam_response_local_total{responseCode="timeout"}[5m])) 4) Correlate with pending/backlog and stale cleanup signals (names vary by deployment; use your actual metric names) - Pending in-flight: occnp_diam_pending_requests (or equivalent) - Stale cleanup: sum(rate(occnp_stale_diam_request_cleanup_total[5m])) (or equivalent) 5) Check related ASR activity (if you also export request-side metrics) - Look for spikes in abort activity leading to more ASR/ASA, and whether ASA timeouts track that spike. 6) Validate timer/transport symptoms - Peer connection flaps, TCP/SCTP retransmits, TLS issues (from Diameter stack logs / node metrics), and latency changes around the alert window. **Recovery:** 1) If timeouts are concentrated on a specific peer (destHost/destRealm). Validate peer health (CPU, thread pools, queue depth), connectivity, routing, firewall/ACL, and Diameter connection state. If supported, fail traffic away from the impacted peer / route to alternate peer. 2) If timeouts correlate with backlog/pending growth. Reduce load (throttling/ admission controls), scale out the impacted service, or address the resource bottleneck (CPU/memory/GC/thread pools). Ensure the Diameter stack isn't saturated (worker threads, queues). 3) If driven by network/transport issues. Fix underlying network faults (loss/latency), stabilize SCTP/TCP sessions, confirm MTU and TLS settings if applicable. 4) If timers are misaligned systemically. Review Diameter transaction timers and peer timeouts; adjust only per established engineering standards to avoid masking real performance problems. 5) Operational action (last resort). Restart/recycle the specific stuck peer process/ component only after addressing the underlying cause; verify ASA timeout % returns to baseline and pending requests drain.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.19 ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-288 ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA timeout count exceeds the minor threshold limit
Summary	Alert ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.44.1.2.31
Metric Used	occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-288 (Cont.) ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause:** More than 60% of local Diameter ASA responses over 5 minutes are timing out. This usually means PCRF/Core (or the local Diameter stack) is not receiving ASA in time after sending ASR, most commonly due to peer reachability/latency issues, peer overload, routing/connection problems, or internal congestion causing the transaction to exceed timers. **Diagnostic Information:** 1) Confirm the ASA timeout ratio and volume (ensure denominator is not near-zero) - Total ASA rate: sum(rate(occnp_diam_response_local_total{msgType="ASA"}[5m])) - ASA timeout rate: sum(rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) 2) Identify which peers/endpoints are driving timeouts (common useful labels: destHost, destRealm, reqDestHost, reqDestRealm, origHost) - sum by (destHost, destRealm) (rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) - If available: sum by (reqDestHost, reqDestRealm) (rate(occnp_diam_response_local_total{msgType="ASA",responseCode="timeout"}[5m])) 3) Check whether this is isolated to ASA or systemic across msgTypes - sum by (msgType, responseCode) (rate(occnp_diam_response_local_total{responseCode="timeout"}[5m])) 4) Correlate with pending/backlog and stale cleanup signals (names vary by deployment; use your actual metric names) - Pending in-flight: occnp_diam_pending_requests (or equivalent) - Stale cleanup: sum(rate(occnp_stale_diam_request_cleanup_total[5m])) (or equivalent) 5) Check related ASR activity (if you also export request-side metrics) - Look for spikes in abort activity leading to more ASR/ASA, and whether ASA timeouts track that spike. 6) Validate timer/transport symptoms - Peer connection flaps, TCP/SCTP re-transmits, TLS issues (from Diameter stack logs / node metrics), and latency changes around the alert window. **Recovery:** 1) If timeouts are concentrated on a specific peer (destHost/destRealm) - Validate peer health (CPU, thread pools, queue depth), connectivity, routing, firewall/ACL, and Diameter connection state. If supported, fail traffic away from the impacted peer / route to alternate peer. 2) If timeouts correlate with backlog/pending growth - Reduce load (throttling/ admission controls), scale out the impacted service, or address the resource bottleneck (CPU/memory/GC/thread pools). Ensure the Diameter stack is not saturated (worker threads, queues). 3) If driven by network/transport issues. Fix underlying network faults (loss/latency), stabilize SCTP/TCP sessions, confirm MTU and TLS settings if applicable. 4) If timers are misaligned systemically. Review Diameter transaction timers and peer timeouts; adjust only per established engineering standards to avoid masking real performance problems. 5) Operational action (last resort). Restart/recycle the specific stuck peer process/ component only after addressing the underlying cause; verify ASA timeout % returns to baseline and pending requests drain.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.20 RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 8-289 RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Gx timeout count exceeds the critical threshold limit
Summary	Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expession	sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.32
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"timeout"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-289 (Cont.) RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause:** More than 90% of Gx RAA responses over 5 minutes are timing out. This indicates that Gx re-auth transactions (RARRAA) are overwhelmingly failing to complete, typically due to OCS/PCEF/PGW peer non-responsiveness, severe peer or network degradation, routing issues to a specific Gx peer, or severe internal saturation causing request processing or response handling to miss timeouts. **Diagnostic Information:** 1) Validate volume and ratio- Total Gx RAA rate: sum(rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx"}[5m])) - Timeout Gx RAA rate: sum(rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx",responseCode="timeout"}[5m])) 2) Pinpoint impacted Gx peers - sum by (destHost, destRealm) (rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx",responseCode="timeout"}[5m])) - If available: sum by (reqDestHost, reqDestRealm) (rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx",responseCode="timeout"}[5m])) 3) Confirm if timeouts are specific to RAA or widespread on Gx - sum by (msgType, responseCode) (rate(occnp_diam_response_local_total{appType="Gx",responseCode="timeout"}[5m])) 4) Check re-auth triggering rate and retry patterns (if you export request/process metrics) - Look for spikes in reauth triggers and retries; correlate with timeout onset. 5) Check backlog / stuck transactions - occnp_diam_pending_requests (or equivalent) grouped by app if possible - stale cleanup metric rate increases during the alert window 6) Review Diameter stack / application logs for Gx - Connection down / watchdog failures, route resolution issues, send failed, peer busy, queue full, timer expirations. **Recovery:** 1) If isolated to one Gx peer - Validate PCEF/PGW/peer health and connectivity; fix routing, ACL/firewall, DNS/peer resolution, and confirm Diameter connection is established and stable. - Shift traffic to alternate peer/route if supported. 2) If re-auth storm / load spike is driving it - Apply rate-limiting/backoff (per product guidance), reduce triggering conditions upstream, and/or scale out the affected component. Confirm thread pools/queues arent saturated; address resource exhaustion. 3) If network degradation is the driver - Stabilize transport (SCTP/TCP), fix packet loss/latency, validate MTU, and ensure no intermediate device is dropping long-lived Diameter sessions. 4) If timers are too aggressive vs observed latency - Review and align transaction timers with SLOs and real latency; avoid papering over peer slowness. 5) Operational action (last resort) - Restart only the affected Diameter peer component after restoring network/peer health; validate RAA timeout % drops and successful RAA resumes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.21 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 8-290 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Gx timeout count exceeds the major threshold limit
Summary	Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.44.1.2.32
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"timeout"}
Recommended Actions	**Cause:** Majority of Gx RAA transactions are timing out. Common drivers: Gx peer (PCEF/PGW) not responding, peer overload, network degradation (loss/latency), Diameter connection instability, routing to wrong/unreachable peer, or local backlog causing transactions to exceed timers. **Diagnostic Information:** 1) Validate ratio + volume (ensure denominator is not tiny) - Total: sum(rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx"}[5m])) - Timeouts: sum(rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx",responseCode="timeout"}[5m])) 2) Identify impacted peers/endpoints (use available labels like destHost, destRealm, reqDestHost, reqDestRealm) - sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx",responseCode="timeout"}[5m])) 3) Check if timeouts are isolated to RAA or widespread on Gx - sum by (msgType) (rate(occnp_diam_response_local_total{appType="Gx",responseCode="timeout"}[5m])) 4) Look for congestion / backlog symptoms (metric names vary) - Pending in-flight: occnp_diam_pending_requests (or equivalent) - Stale cleanups: sum(rate(occnp_stale_diam_request_cleanup_total[5m])) (or equivalent) 5) Correlate with Diameter connectivity events (from logs / stack metrics): watchdog failures, reconnect loops, send failures, peer-down. **Recovery:** 1) If concentrated on one peer: validate peer health/connectivity; fail traffic over to alternate peer/routing if supported. 2) If backlog/CPU saturation locally: scale out, reduce trigger rate, tune threadpools/queues per product guidance; confirm pending drains. 3) If network driven: fix transport (SCTP/TCP), loss/latency, ACL/firewall, MTU, TLS; stabilize sessions. 4) Review/align timers only if systemic and validated; avoid masking a slow peer. 5) Last resort: restart affected peer component after underlying issue is resolved; confirm timeout % drops below threshold.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.22 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 8-291 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Gx timeout count exceeds the minor threshold limit
Summary	Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appType="Gx"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.44.1.2.32
Metric Used	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"timeout"}
Recommended Actions	**Cause:** Early indicator of the same failure mode as above, but may be intermittent (bursty peer slowness, brief network impairment, or onset of overload). **Diagnostic Information:** Use the same diagnostics as the MAJOR alert, but add: 1) Trend it (is it rising?) - avg_over_time((sum(rate(…timeout…[5m])) / sum(rate(…total…[5m])) * 100)[30m:]) 2) Compare by peer to see if one peer is degrading first - topk(5, sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{msgType="RAA",appType="Gx",responseCode="timeout"}[5m]))) **Recovery:** 1) Proactively validate peer and network health before it escalates. 2) If one peer shows degradation, preemptively route/failover if allowed. 3) If local resources trending high, scale/relieve load and verify timeouts return to baseline.

8.1.3.23 RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Table 8-292 RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	CCA, AAA, RAA, ASA and STA error rate combined is above 10 percent
Summary	Alert RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total[5m])) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.37
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-292 (Cont.) RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Recommended Actions	**Cause:** A broad service-impacting condition: >10% of all local Diameter answers are non-2xx. Causes typically include peer outages, widespread timeouts, routing/realm issues, auth/credit/policy dependency failures, system overload, or misconfiguration causing systematic rejects/errors. **Diagnostic Information:** 1) Identify top failing response codes and message types - sum by (responseCode) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) - sum by (msgType,responseCode) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) 2) Find which app is driving it (if appType exists on the metric) - sum by (appType) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) 3) Pinpoint impacted peers - sum by (destHost,destRealm,responseCode) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) 4) Separate timeouts vs explicit rejects/errors - Timeouts: sum(rate(occnp_diam_response_local_total{responseCode="timeout"}[5m])) - Other errors: `sum(rate(occnp_diam_response_local_total{responseCode!~"2.*timeout"}[5m])) 5) Correlate with saturation and stuck-transaction symptoms - Pending:occnp_diam_pending_requests(or equivalent) - Stale cleanup:sum(rate(occnp_stale_diam_request_cleanup_total[5m]))(or equivalent) **Recovery:** 1) Stabilize service first (contain impact) - If errors are dominated by timeouts: treat as an availability/latency incident—verify Diameter peer connectivity (TCP/SCTP up, watchdog OK), check packet loss/latency, and remediate network/transport issues. - If concentrated on a specific peer (destHost/destRealm): isolate it (failover/reroute traffic if supported) and engage the peer owner to restore capacity/health. 2) Remove overload / drain backlog - If occnp_diam_pending_requests (or equivalent) is growing or CPU/memory/thread pools are saturated: scale out the service, reduce incoming load (throttle/admission controls), and address bottlenecks so pending requests drain and timeouts fall. 3) Fix systematic rejects / config-induced errors - If non-2xx is driven by specific result codes (not timeouts): verify realm routing, peer configuration, policy/charging dependencies (e.g., OCS/UDR/SPR), and any recent config/deploy changes; roll back or correct configuration as needed. 4) Avoid masking the problem with timer changes - Only adjust Diameter timers if analysis shows they are misaligned with expected latency; do not use timer increases as a substitute for fixing slow/unhealthy peers. 5) Last-resort operational actions - Restart/recycle only the affected component(s) if they are stuck (e.g., wedged Diameter stack) after underlying network/peer issues are corrected; avoid repeated restarts that can amplify load. 6) Recovery validation - Confirm combined non-2xx ratio drops below 10%, timeouts return to baseline, pending/backlog metrics normalize, and per-msgType success rates (2xx) recover across the major peers.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.24 RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Table 8-293 RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Description	CCA, AAA, RAA, ASA and STA error rate combined is above 5 percent
Summary	Alert RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total[5m])) * 100 > 5 and sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total[5m])) * 100 <= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.37
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*"}
Recommended Actions	**Cause:** Same category as CRITICAL but less severe; indicates meaningful degradation (often partial peer impairment, rising timeouts, or one message type failing). **Diagnostic Information:** Same diagnostics as CRITICAL, with focus on identifying the earliest driver: - By msgType: sum by (msgType) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) - By peer: sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) **Recovery:**Same recovery patterns as CRITICAL, typically starting with: isolate peer/appType causing the increase; remediate connectivity/perf; apply failover/rate-limit/scale before it escalates.

8.1.3.25 RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Table 8-294 RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Description	CCA, AAA, RAA, ASA and STA error rate combined is above 1 percent
Summary	Alert RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total[5m])) * 100 > 1 and sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total[5m])) * 100 <= 5
OID	1.3.6.1.4.1.323.5.3.52.1.2.37
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-294 (Cont.) RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Recommended Actions	**Cause:** Early warning of deteriorating conditions: small but non-trivial increase in timeouts, rejects, or application errors. Could be a single peer intermittently failing, a rollout regression, or early overload. **Diagnostic Information:** 1) Quickly determine whether this is timeouts vs non-timeout errors - sum by (responseCode) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) 2) See if it's localized to a msgType/appType/peer - sum by (appType,msgType,responseCode) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) - sum by (destHost,destRealm) (rate(occnp_diam_response_local_total{responseCode!~"2.*"}[5m])) 3) Correlate with recent changes (deployments/config/routing changes) and node health signals. **Recovery:** 1) If timeouts start trending up: validate network/peer health and capacity early; consider proactive reroute/failover. 2) If rejects/errors rise after a change: roll back or fix config; confirm realm/route/policy alignment. 3) Continue monitoring until stable baseline is restored (<1%).

8.1.3.26 Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Table 8-295 Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	Rx error rate combined is above 10 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Rx"}[5m])) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.38
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-295 (Cont.) Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Recommended Actions	**Cause:** more than 10% of Rx local Diameter responses over 5 minutes are non-2xx, meaning PCRF-Core is returning/observing too many failed, rejected, or timed-out Rx answers. **Diagnostic Information:** 1 Check current top failing Rx response codes - Query: `sum by (responseCode, msgType, destHost, destRealm) (rate(occnp_diam_response_local_total{appType="Rx",responseCode!~"2.*"}[5m]))` 2 Compare success vs failure split - Success:`sum(rate(occnp_diam_response_local_total{appType="Rx",responseCode=~"2.*"}[5m]))` - Failure: `sum(rate(occnp_diam_response_local_total{appType="Rx",responseCode!~"2.*"}[5m]))` 3 Identify whether failures are concentrated on a specific Rx message type - Query by `msgType`: - `sum by (msgType, responseCode) (rate(occnp_diam_response_local_total{appType="Rx"}[5m]))` - In this code, Rx message types commonly map to `AAR/AAA`, `RAR/RAA`, `STR/STA`, `ASR/ASA` depending on flow. 4 Identify affected peers/endpoints - Query by `destHost`, `destRealm`, `reqDestHost`, `reqDestRealm`, `origHost` - This helps determine whether one AF/peer is driving the issue. 5 Check for timeouts specifically - Query:`sum by (msgType, reqDestHost, reqDestRealm) (rate(occnp_diam_response_local_total{appType="Rx",responseCode="timeout"}[5m]))` 6 Correlate with internal request/reply metrics - `occnp_app_request_local_process_total` - `occnp_app_response_local_process_total` These carry labels like `reason`, `msgType`, `destHost`, `destRealm`, `retryAttempts`, and help determine whether failures are tied to retries, reauth, or specific internal reasons. 7 Check stale or congestion-related symptoms if suspected - `occnp_stale_diam_request_cleanup_total` (actual full name depends on prefix/suffix rules around `stale_diam_request_cleanup_total`) - `occnp_diam_pending_requests` - congestion reject metrics if request throttling is involved 8 Review logs around rejection paths - Relevant code paths log warnings when: - no PEP / enforcement session found - AN-GW failure - duplicate or stale handling - pending transaction retry / timeout scenarios **Recovery:** Recommended recovery depends on the dominant failing `responseCode` / `msgType`, but generally: 1 If failures are timeout-heavy - verify Diameter peer connectivity and peer health - check whether AF / peer is reachable and responding in time - inspect recent latency increase and pending request growth - validate timer/profile configuration if timeouts are systemic 2 If failures are concentrated on one peer (`destHost`/`destRealm`) - isolate the peer issue - verify peer routing, reachability, and configuration - fail traffic away from the impacted peer if supported 3 If failures are dominated by rejection/result codes

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-295 (Cont.) Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
	- inspect policy rejection, binding, or session-correlation paths - verify enforcement session existence / PEP availability - check for admission/session-limit conditions - verify AN-GW or enforcement-side dependencies 4 If stale or overload symptoms are present - inspect queueing delays and pending Diameter requests - check congestion / resource exhaustion - scale or relieve traffic if the service is saturated 5 Operational recovery actions - restart or recover the affected Diameter peer/component only if the issue is stuck and peer-specific - clear underlying downstream/network fault before restarting PCRF-Core - after recovery, confirm: - Rx non-2xx ratio falls below 10% - timeout counts return to baseline - successful 2xx Rx responses resume

8.1.3.27 Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Table 8-296 Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Description	Rx error rate combined is above 5 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Rx"}[5m])) * 100 > 5 and sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Rx"}[5m])) * 100 <= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.38
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-296 (Cont.) Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Recommended Actions	**Cause:** more than 5% and less than 10% of Rx local Diameter responses over 5 minutes are non-2xx, meaning PCRF-Core is returning/observing too many failed, rejected, or timed-out Rx answers. **Diagnostic Information:** 1 Check current top failing Rx response codes - Query: `sum by (responseCode, msgType, destHost, destRealm) (rate(occnp_diam_response_local_total{appType="Rx",responseCode!~"2.*"}[5m]))` 2 Compare success vs failure split - Success:`sum(rate(occnp_diam_response_local_total{appType="Rx",responseCode=~"2.*"}[5m]))` - Failure: `sum(rate(occnp_diam_response_local_total{appType="Rx",responseCode!~"2.*"}[5m]))` 3 Identify whether failures are concentrated on a specific Rx message type - Query by `msgType`: - `sum by (msgType, responseCode) (rate(occnp_diam_response_local_total{appType="Rx"}[5m]))` - In this code, Rx message types commonly map to `AAR/AAA`, `RAR/RAA`, `STR/STA`, `ASR/ASA` depending on flow. 4 Identify affected peers/endpoints - Query by `destHost`, `destRealm`, `reqDestHost`, `reqDestRealm`, `origHost` - This helps determine whether one AF/peer is driving the issue. 5 Check for timeouts specifically - Query:`sum by (msgType, reqDestHost, reqDestRealm) (rate(occnp_diam_response_local_total{appType="Rx",responseCode="timeout"}[5m]))` 6 Correlate with internal request/reply metrics - `occnp_app_request_local_process_total` - `occnp_app_response_local_process_total` These carry labels like `reason`, `msgType`, `destHost`, `destRealm`, `retryAttempts`, and help determine whether failures are tied to retries, reauth, or specific internal reasons. 7 Check stale or congestion-related symptoms if suspected - `occnp_stale_diam_request_cleanup_total` (actual full name depends on prefix/suffix rules around `stale_diam_request_cleanup_total`) - `occnp_diam_pending_requests` - congestion reject metrics if request throttling is involved 8 Review logs around rejection paths - Relevant code paths log warnings when: - no PEP / enforcement session found - AN-GW failure - duplicate or stale handling - pending transaction retry / timeout scenarios **Recovery:** Recommended recovery depends on the dominant failing `responseCode` / `msgType`, but generally: 1 If failures are timeout-heavy - verify Diameter peer connectivity and peer health - check whether AF / peer is reachable and responding in time - inspect recent latency increase and pending request growth - validate timer/profile configuration if timeouts are systemic 2 If failures are concentrated on one peer (`destHost`/`destRealm`) - isolate the peer issue - verify peer routing, reachability, and configuration - fail traffic away from the impacted peer if supported

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-296 (Cont.) Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
	3 If failures are dominated by rejection/result codes - inspect policy rejection, binding, or session-correlation paths - verify enforcement session existence / PEP availability - check for admission/session-limit conditions - verify AN-GW or enforcement-side dependencies 4 If stale or overload symptoms are present - inspect queueing delays and pending Diameter requests - check congestion / resource exhaustion - scale or relieve traffic if the service is saturated 5 Operational recovery actions - restart or recover the affected Diameter peer/component only if the issue is stuck and peer-specific - clear underlying downstream/network fault before restarting PCRF-Core - after recovery, confirm: - Rx non-2xx ratio falls below 10% - timeout counts return to baseline - successful 2xx Rx responses resume

8.1.3.28 Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Table 8-297 Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Description	Rx error rate combined is above 1 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Rx"}[5m])) * 100 > 1 and sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Rx"}[5m])) * 100 <= 5
OID	1.3.6.1.4.1.323.5.3.52.1.2.38
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-297 (Cont.) Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Recommended Actions	**Cause:** more than 1% and less than 5% of Rx local Diameter responses over 5 minutes are non-2xx, meaning PCRF-Core is returning/observing too many failed, rejected, or timed-out Rx answers. **Diagnostic Information:** 1 Check current top failing Rx response codes - Query: `sum by (responseCode, msgType, destHost, destRealm) (rate(occnp_diam_response_local_total{appType="Rx",responseCode!~"2.*"}[5m]))` 2 Compare success vs failure split - Success:`sum(rate(occnp_diam_response_local_total{appType="Rx",responseCode=~"2.*"}[5m]))` - Failure: `sum(rate(occnp_diam_response_local_total{appType="Rx",responseCode!~"2.*"}[5m]))` 3 Identify whether failures are concentrated on a specific Rx message type - Query by `msgType`: - `sum by (msgType, responseCode) (rate(occnp_diam_response_local_total{appType="Rx"}[5m]))` - In this code, Rx message types commonly map to `AAR/AAA`, `RAR/RAA`, `STR/STA`, `ASR/ASA` depending on flow. 4 Identify affected peers/endpoints - Query by `destHost`, `destRealm`, `reqDestHost`, `reqDestRealm`, `origHost` - This helps determine whether one AF/peer is driving the issue. 5 Check for timeouts specifically - Query:`sum by (msgType, reqDestHost, reqDestRealm) (rate(occnp_diam_response_local_total{appType="Rx",responseCode="timeout"}[5m]))` 6 Correlate with internal request/reply metrics - `occnp_app_request_local_process_total` - `occnp_app_response_local_process_total` These carry labels like `reason`, `msgType`, `destHost`, `destRealm`, `retryAttempts`, and help determine whether failures are tied to retries, reauth, or specific internal reasons. 7 Check stale or congestion-related symptoms if suspected - `occnp_stale_diam_request_cleanup_total` (actual full name depends on prefix/suffix rules around `stale_diam_request_cleanup_total`) - `occnp_diam_pending_requests` - congestion reject metrics if request throttling is involved 8 Review logs around rejection paths - Relevant code paths log warnings when: - no PEP / enforcement session found - AN-GW failure - duplicate or stale handling - pending transaction retry / timeout scenarios **Recovery:** Recommended recovery depends on the dominant failing `responseCode` / `msgType`, but generally: 1 If failures are timeout-heavy - verify Diameter peer connectivity and peer health - check whether AF / peer is reachable and responding in time - inspect recent latency increase and pending request growth - validate timer/profile configuration if timeouts are systemic 2 If failures are concentrated on one peer (`destHost`/`destRealm`) - isolate the peer issue - verify peer routing, reachability, and configuration - fail traffic away from the impacted peer if supported

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-297 (Cont.) Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
	3 If failures are dominated by rejection/result codes - inspect policy rejection, binding, or session-correlation paths - verify enforcement session existence / PEP availability - check for admission/session-limit conditions - verify AN-GW or enforcement-side dependencies 4 If stale or overload symptoms are present - inspect queueing delays and pending Diameter requests - check congestion / resource exhaustion - scale or relieve traffic if the service is saturated 5 Operational recovery actions - restart or recover the affected Diameter peer/component only if the issue is stuck and peer-specific - clear underlying downstream/network fault before restarting PCRF-Core - after recovery, confirm: - Rx non-2xx ratio falls below 10% - timeout counts return to baseline - successful 2xx Rx responses resume

8.1.3.29 Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Table 8-298 Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	Gx error rate combined is above 10 percent
Summary	Alert Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Gx"}[5m])) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.39
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-298 (Cont.) Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Recommended Actions	**Cause:** This means >10% of Gx responses seen by PCRF-Core in the last 5m are non-success Diameter responses or timeouts. **Diagnostic Information:** - Metrics involved: `occnp_diam_response_local_total{appType="Gx",responseCode,...}`; supporting metric: `occnp_diam_response_local_processing_latency{...}`. - Error observed: elevated non-2xx Gx responses / timeouts. - Cause value: `sum(rate(occnp_diam_response_local_total{responseCode!~"2.*",appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{appType="Gx"}[5m])) * 100 > 10`. - Condition: non-success Gx responses exceed 10% of all Gx responses in 5m. - Likely causes: PGW/peer returning Gx failures such as `DIAMETER_PENDING_TRANSACTION`, `DIAMETER_UNABLE_TO_COMPLY`, `UNKNOWN_SESSION_ID`, authorization rejects, peer busy/unavailable, or request timeout. - Verification steps: 1) break down failures by `responseCode,msgType,destHost,destRealm`; 2) check for `responseCode="timeout"`; 3) correlate with logs for CCA/RAA failures and peer issues; 4) review latency spikes in `occnp_diam_response_local_processing_latency`. - Monitoring recommendations: alert separately on top `responseCode`; split by `destHost`/`destRealm`; add dedicated timeout alert; track latency with error ratio. **Recovery:** - Identify dominant failing `responseCode` and impacted Gx peer/realm. - If timeouts / peer transport errors dominate: check Diameter peer connectivity, session state, overload, and transport health. - If `DIAMETER_PENDING_TRANSACTION` dominates: investigate Gx race/retry pressure and pending-transaction behavior. - If `UNKNOWN_SESSION_ID` dominates: verify stale/missing session state, audit/cleanup effects, and session sync. - If `UNABLE_TO_COMPLY` / auth rejects dominate: inspect recent policy/config/data/backend changes and rollback/fix as needed. - Recovery is complete when the non-2xx Gx response ratio drops below 10% and failing codes return to baseline.

8.1.3.30 Gx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Table 8-299 Gx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Description	Gx error rate combined is above 5 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-299 (Cont.) Gx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Gx"}[5m])) * 100 > 5 and sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Gx"}[5m])) * 100 <= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.39
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}
Recommended Actions	**Cause:** This means >5% and <10% of Gx responses seen by PCRF-Core in the last 5m are non-success Diameter responses or timeouts. **Diagnostic Information:** - Metrics involved: `occnp_diam_response_local_total{appType="Gx",responseCode,...}`; supporting metric: `occnp_diam_response_local_processing_latency{...}`. - Error observed: elevated non-2xx Gx responses / timeouts. - Cause value: `sum(rate(occnp_diam_response_local_total{responseCode!~"2.*",appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{appType="Gx"}[5m])) * 100 > 10`. - Condition: non-success Gx responses exceed 10% of all Gx responses in 5m. - Likely causes: PGW/peer returning Gx failures such as `DIAMETER_PENDING_TRANSACTION`, `DIAMETER_UNABLE_TO_COMPLY`, `UNKNOWN_SESSION_ID`, authorization rejects, peer busy/unavailable, or request timeout. - Verification steps: 1) break down failures by `responseCode,msgType,destHost,destRealm`; 2) check for `responseCode="timeout"`; 3) correlate with logs for CCA/RAA failures and peer issues; 4) review latency spikes in `occnp_diam_response_local_processing_latency`. - Monitoring recommendations: alert separately on top `responseCode`; split by `destHost`/`destRealm`; add dedicated timeout alert; track latency with error ratio. **Recovery:** - Identify dominant failing `responseCode` and impacted Gx peer/realm. - If timeouts / peer transport errors dominate: check Diameter peer connectivity, session state, overload, and transport health. - If `DIAMETER_PENDING_TRANSACTION` dominates: investigate Gx race/retry pressure and pending-transaction behavior. - If `UNKNOWN_SESSION_ID` dominates: verify stale/missing session state, audit/cleanup effects, and session sync. - If `UNABLE_TO_COMPLY` / auth rejects dominate: inspect recent policy/config/data/backend changes and rollback/fix as needed. - Recovery is complete when the non-2xx Gx response ratio drops below 10% and failing codes return to baseline.

8.1.3.31 Gx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Table 8-300 Gx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Description	Gx error rate combined is above 1 percent

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-300 (Cont.) Gx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Gx"}[5m])) * 100 > 1 and sum(rate(occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{ appType="Gx"}[5m])) * 100 <= 5
OID	1.3.6.1.4.1.323.5.3.52.1.2.39
Metric Used	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}
Recommended Actions	**Cause:** This means 1>% and <5% of Gx responses seen by PCRF-Core in the last 5m are non-success Diameter responses or timeouts. **Diagnostic Information:** - Metrics involved: `occnp_diam_response_local_total{appType="Gx",responseCode,...}`; supporting metric: `occnp_diam_response_local_processing_latency{...}`. - Error observed: elevated non-2xx Gx responses / timeouts. - Cause value: `sum(rate(occnp_diam_response_local_total{responseCode!~"2.*",appType="Gx"}[5m])) / sum(rate(occnp_diam_response_local_total{appType="Gx"}[5m])) * 100 > 10`. - Condition: non-success Gx responses exceed 10% of all Gx responses in 5m. - Likely causes: PGW/peer returning Gx failures such as `DIAMETER_PENDING_TRANSACTION`, `DIAMETER_UNABLE_TO_COMPLY`, `UNKNOWN_SESSION_ID`, authorization rejects, peer busy/unavailable, or request timeout. - Verification steps: 1) break down failures by `responseCode,msgType,destHost,destRealm`; 2) check for `responseCode="timeout"`; 3) correlate with logs for CCA/RAA failures and peer issues; 4) review latency spikes in `occnp_diam_response_local_processing_latency`. - Monitoring recommendations: alert separately on top `responseCode`; split by `destHost`/`destRealm`; add dedicated timeout alert; track latency with error ratio. **Recovery:** - Identify dominant failing `responseCode` and impacted Gx peer/realm. - If timeouts / peer transport errors dominate: check Diameter peer connectivity, session state, overload, and transport health. - If `DIAMETER_PENDING_TRANSACTION` dominates: investigate Gx race/retry pressure and pending-transaction behavior. - If `UNKNOWN_SESSION_ID` dominates: verify stale/missing session state, audit/cleanup effects, and session sync. - If `UNABLE_TO_COMPLY` / auth rejects dominate: inspect recent policy/config/data/backend changes and rollback/fix as needed. - Recovery is complete when the non-2xx Gx response ratio drops below 10% and failing codes return to baseline.

Copyright © 2019, 2026, Oracle and/or its affiliates.

8.1.3.32 STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL

Table 8-301 STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 30%
Summary	The Diameter requests are being discarded due to timeout processing occurring above 30%
Severity	Critical
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total[24h])) / sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER"}[24h]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.82
Metric Used	occnp_stale_diam_request_cleanup_total
Recommended Actions	**Cause:** More than 30% of Diameter requests sent in the last 24 hours did not receive a response in time and were discarded by the cleanup mechanism. This indicates Diameter peers are slow to respond, unreachable, or the node is overloaded. **Diagnostic Information:** Check the affected pod and microservice for signs of overload or connectivity issues with Diameter peers. Review Diameter peer status, response times, and whether the cleanup rate is increasing over time. Exclude DWR/CER traffic from analysis as these are control-plane messages. **Recovery:** Verify connectivity and health of Diameter peers. If the node is overloaded, consider scaling the affected microservice. Investigate and resolve any network latency or timeout misconfigurations between the node and its Diameter peers.

8.1.3.33 STALE_DIAMETER_REQUEST_CLEANUP_MAJOR

Table 8-302 STALE_DIAMETER_REQUEST_CLEANUP_MAJOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 20%
Summary	The Diameter requests are being discarded due to timeout processing occurring above 20%
Severity	Major
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total[24h])) / sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER"}[24h]))) * 100 >= 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.82
Metric Used	occnp_stale_diam_request_cleanup_total

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 8-302 (Cont.) STALE_DIAMETER_REQUEST_CLEANUP_MAJOR

Field	Details
Recommended Actions	**Cause:** More than 20% of Diameter requests sent in the last 24 hours did not receive a response in time and were discarded by the cleanup mechanism. This indicates Diameter peers are slow to respond, unreachable, or the node is overloaded. **Diagnostic Information:** Check the affected pod and microservice for signs of overload or connectivity issues with Diameter peers. Review Diameter peer status, response times, and whether the cleanup rate is increasing over time. Exclude DWR/CER traffic from analysis as these are control-plane messages. **Recovery:** Verify connectivity and health of Diameter peers. If the node is overloaded, consider scaling the affected microservice. Investigate and resolve any network latency or timeout misconfigurations between the node and its Diameter peers.

8.1.3.34 STALE_DIAMETER_REQUEST_CLEANUP_MINOR

Table 8-303 STALE_DIAMETER_REQUEST_CLEANUP_MINOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 10%
Summary	The Diameter requests are being discarded due to timeout processing occurring above 10%
Severity	Minor
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total[24h])) / sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER"}[24h]))) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.82
Metric Used	occnp_stale_diam_request_cleanup_total
Recommended Actions	**Cause:** More than 10% of Diameter requests sent in the last 24 hours did not receive a response in time and were discarded by the cleanup mechanism. This indicates Diameter peers are slow to respond, unreachable, or the node is overloaded. **Diagnostic Information:** Check the affected pod and microservice for signs of overload or connectivity issues with Diameter peers. Review Diameter peer status, response times, and whether the cleanup rate is increasing over time. Exclude DWR/CER traffic from analysis as these are control-plane messages. **Recovery:** Verify connectivity and health of Diameter peers. If the node is overloaded, consider scaling the affected microservice. Investigate and resolve any network latency or timeout misconfigurations between the node and its Diameter peers.

Copyright © 2019, 2026, Oracle and/or its affiliates.

9
CNC Policy Metrics

This chapter includes information about Metrics for Oracle Communications Cloud Native Core, Policy (CNC Policy).

Policy uses the observability tool Grafana to analyze and visualize data. The Grafana Dashboard consists of panels displaying the data as graphs, charts or other visualizations. A dashboard in Grafana is represented by a JSON object, which stores the metadata of its dashboard. Following Grafana dashboards are created for Policy Observability and debugging purposes:

- **Observability Dashboard**:
  - This dashboard metadata is stored in the `Policy_Observability_Dashboard.json` file.
  - This dashboard has the panels that monitors the overall health status of the setup & contains details like resource utilization, kmps, latency, etc.
  - Customers can use this Dashboard on a regular basis for observing the status of the setup and also for assessing the setup performance with a run.
  - Depending upon the applicability of a panel or row, the customers have the flexibility to either remove, update or add content to the Dashboard.
- **Debug Dashboard**:
  - This dashboard metadata is stored in the `Policy_Debug_Dashboard.json` file.
  - This dashboard has the panels that monitor the operational status of the setup and is used for debugging & troubleshooting purposes.
  - Customers can use this Dashboard when any issue occur in the NF and also when reporting a probable issue to Oracle Customer Support from the setup.
  - Depending upon the applicability of a panel or row, the customers have the flexibility to either remove, update or add content to the Dashboard.

The name of the metrics may contain suffix such as total, seconds, max and so on. It gets added by the Micrometer registry if it is not present in the metrics name. The metric name has the following format for suffix:

The metric name is equal to <Basename of the metric>_<Suffix>

Table 9-1 Metrics type and Suffix

Metric Type	Suffix
Counter	_total
Gauge	N/A
TimerGauge	_seconds
MultiGauge	N/A

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-1 (Cont.) Metrics type and Suffix

Metric Type	Suffix
Timer	_seconds_max or _seconds **Note**: There are two types of suffix used for timer metrics. For example, my_timer_seconds_max gauge and my_timer_seconds summary. In summary type, there will be further addition of suffix such as _count or _sum.
DistributionSummary	N/A or _max **Note**: There are two types of suffix used for DistributionSummary. For example, my_distribution_ratio histogram and my_distribution_ratio_max gauge. In the histogram type there will be further addition of suffix such as bucket, _count, or sum.
LongTaskTimer	_seconds_max or _seconds **Note:** There are two types of suffix used for LongTaskTimer. For example, long_task_timer_seconds_max gauge and long_task_timer_seconds summary. In summary type there will be further addition of suffix such as _active_count or _duration_sum.

Note

Metric names can consist of letters, numbers, underscores, and colons, as defined by the regular expression `[a-zA-Z_:][a-zA-Z0-9_:]*`.

Table 9-2 Dimension Description

Dimension	Description
operation_type	Type of operation Values: • create • get • put • update • terminate • update_notify • terminate_notify • subscribe • unsubscribe • transfer • resubscribe • tdf_notify_create_session_request • tdf_notify_terminate_session_request • tdf_notify_update_session_request
dnn	Data Network Name or Access Point Name
snssai	Single Network Slice Selection Assistance Information

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-2 (Cont.) Dimension Description

Dimension	Description
response_code	Response code **HTTP interfaces:** • 1xx • 2xx • 3xx • 4xx • 5xx **Diameter interfaces:** • 2xxx • 3xxx • 4xxx • 5xxx
latency	The total time in between request and response. If latency between request and response is 203, then bucket number is 4. Max bucket set to 10 (0-9), Range 50ms.
old_state	Pod/Resource congestion state before transition.
new_state	Pod/Resource congestion state after transition.
nf_instance_Id	Unique id of the nf Instance. • ingress: source nfInstanceId • egress: destination nfInstanceId **HTTP interfaces:** **Diameter interfaces:** • ingress: Origin-Host AVP • egress: Destination-Host AVP
nf_name	This represents the FQDN corresponding to the NF InstanceID present in the nf_instance_id dimension. **HTTP interface:** egress: NF FQDN
sbi_priority	Service Based Interface
service_version	Service version Value: [UDR = "v1,v2", CHF = "v1"]
service	The complete name of current service. Value: string
namespace	The namespace of current service. Value: string
category	The category of current service. Value: • database • common • infra • pcf • bsf
destHost	Value of destination Host received or sent in the corresponding request message
destRealm	Value of destination Realm received or sent in the corresponding request message
origHost	Value of origination Host received or sent in the corresponding request message
origRealm	Value of origination Realm received or sent in the corresponding request message
reqDestHost	Value of destination Host in corresponding request message of response message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-2 (Cont.) Dimension Description

Dimension	Description
reqDestRealm	Value of destination Realm in corresponding request message of response message.
reqOrigHost	Value of origination Host in corresponding request message of response message.
reqOrigRealm	Value of origination Realm in corresponding request message of response message.
direction	Indicates direction of message flow. • "In" means coming towards POD/micro-service • "Out" means going out from POD/micro-service
appId	Application ID exchanged in CEX messages or used in the respective message of an application.
applicationName	Human readable name of corresponding application ID 16777236 => Rx 16777238 => Gx 16777302 => Sy 0xffffffff => Relay
cmdCode	Command code value in the received or sent, request or answer message
msgType	Type of the message, for example CCRT-T, CCR-I etc.
responseCode	Result code such as 2xx,5xx,4xx in diameter messages. It indicates the response received/sent for HTTP messages or exceptions.
spendingLimitDataSource	Specifies the source from which PCF fetches policy counters. Value: OCS
retry	Identify message is a retry message. Value: • true • false
retryAnswer	Reason for the retry message. Value: • error code • timeout
level	Indicates the current load level or the level of pod congestion. Value: • 0 = Normal • 1 = DOC • 2 = Congested
type	Resource type Value: • PendingRequest • CPU • Memory
le	le is abbreviated as "Less than equal to".Value of a defined bucket for a Histogram.
sessRuleReports	Indicates that session rule report is received at PCF.
policyDecFailureReports	Indicates that Policy decision failure report is received at PCF.
isLeaderPod	Indicates if the pod calculating the threshold level is a leader pod.
prevLevel	Indicates the previous load level prior to current load level calculation.
levelChangeType	Indicates the level change type. The value of this dimension can be: • None: when load level is same • Increment: when level changes to higher level
servicenameNon3gpp	

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-2 (Cont.) Dimension Description

Dimension	Description
serviceResource	
params	Lists the API parameters.
outcome	Shows the outcome of an operation such as SUCCESS, FAILURE, TIMEOUT.
cause	Contains the error cause.
sourceUri	NF Service URI that leads to this service request. Format of this dimension is the same as that of uri attribute. For example: /npcf-smpolicycontrol/v1/sm-policies The value of this dimension is included in the `oc-x-source-uri` header in the incoming request. For locally originated requests such as timer based, value of this dimension can be "" or the timer name. if sourceUri is not received in the header from the core service, the value of this dimension will be same as uri dimension.
sourceOperationType	NF Service HTTP verb or operation type that leads to this service request. Value is included in the oc-x-source-operation header in the incoming request such as CREATE, UPDATE, or DELETE. For locally originated requests such as timer based, value of this dimension can be "" or the timer name. If sourceOperationType is not received in the header from Core service, the value remains the same as operationType dimension.
Uri	Includes the resource URI in generic format. For example: /binding/v1/contextBinding/context-owner/{contextOwner}
serviceResource	
responseCause	In case of responseCode as exception, this dimension provides additional cause such as Timeout and Server Internal Error. **Note** This dimension is used only for exceptions. In case of successful operation, this dimension value will become empty.
Duration	Only applicable to "processing_latency_ms" metrics. This is to indicate bucket, that are managed by promclient as "le" dimension. Example: Bucket as 3ms, 5ms, 10ms, 15ms, 20ms, 30ms, 50ms, 100ms
Stage	
result_code	Indicates received LDAP response code. Example values: 32, 85, 91
destination_host	Indicates the IP address or FQDN of LDAP server.
peerHost	Indicates the value of peer host received or sent in corresponding connection request message.
peerRealm	Indicates the value of peer realm received or sent in corresponding connection request message.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-2 (Cont.) Dimension Description

Dimension	Description
accessType access_type	Access Type. • 3GPP_ACCESS • NON_3GPP_ACCESS
policyControlRequestTrigger	Policy Control Request Trigger can have single value or comma separated list of values ordered alphabetically. • AC_TY_CH • AN_CH_COR • AN_INFO • APP_STA • APP_STO • CM_SES_FAIL • DEF_QOS_CH • NO_CREDIT • NUM_OF_PACKET_FILTER • PLM_CH • PRA_CH • PS_DA_OFF • QOS_NOTIF • RAT_TY_CH • RE_TIMEOUT • REF_QOS_IND_CH • RES_MO_RE • RES_RELEASE • SAREA_CH • SCELL_CH • SCNN_CH • SE_AMBR_CH • SUCC_RES_ALLO • UE_IP_CH • UE_MAC_CH • UE_STATUS_RESUME • UE_TZ_CH • US_RE

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-2 (Cont.) Dimension Description

Dimension	Description
rat_type ratType	Radio Access Type. • EUTRA • EUTRA_U • GERA • LTE-M • NBIOT • NR • NR_GEO • NR_LEO • NR_MEO • NR_OTHER_SAT • NR_REDCAP • NR_U • TRUSTED_N3GA • TRUSTED_WLAN • UTRA • VIRTUAL • WLAN
sourceAccessType	Previous access type before the update. • Dimension: accessType
sourceRatType	Previous radio access type before the update. • Dimension: ratType
reattempt_timer_expiry_notification	This value in **source** dimension indicates consolidation done on receiving Timer Expiry Notification from Timer Service.
isReattempt	Set to true/false. `True` indicates that the sequencing of policyDecisions occurred due to a re-attempt timer. This can be triggered either by a Retry-After IE received from the AMF or by the PCF-configured reattempt profile (configured on **Reattempt Profiles** page under **Common** category for **Service Configurations** on CNC Console. In this case, the decision is not sent immediately, but will instead be sent to the AMF in a reattempted request. `False` indicates that sequencing occurred when an ongoing transfer was ongoing with the T3501 timer running waiting for N1 Notification and then an external trigger arrived.
isRetryAttempt	Set to true/false based on first or subsequent alternate attempt towards host.
reattemptType	Set to String. It tells the type of reattempt requests, whether it is for Subscribe/Transfer/TransferFailureNotification. Its value is the timerName - for which the timer was created and was reattempted .
priority	This dimension indicates message priority, when available. It supports both oc-message-priority and 3gpp-sbi-message-priority. 3gpp-sbi-message-priority must have higher precedence.
reason	The values: • MSGTYPE_CREATE • PRIMARY_SESSION_DELETED • MSGTYPE_MODIFY • MSGTYPE_REAUTH • REMOTE_DELETE
sponId	Includes the sponId received through the N5 interface.
aspId	Includes the aspId received through the N5 interface.
servicename3gpp	The value of this dimension is the service name and version. For example: `npcf-smpolicycontrol`.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-2 (Cont.) Dimension Description

Dimension	Description
umcDataIncluded	This dimension reflects whether the sponsored session contained UMC data, last status received through the N5 interface is reflected for DELETE operation if UMC not received. Possible values: True, False
sponStatus	This dimension indicates the last status received through the N5 interface. Even if the request arrived is Delete, the last *sponStatus* received is displayed in order to indicate whether it was a sponsored session or not. For example, SPONSOR_ENABLED/ SPONSOR_DISABLED.
operationTypeN5	The value in this dimension is the operation type that triggers the update_notify towards the SMF that is received through N5 interface. For example: CREATE, UPDATE, DELETE.
application	The name of application from which the metric is triggered. For example: policyds
application_exception	The class name of the exception container in which the real exception is wrapped and send to error-handler. For example: HttpException
wrapped_exception	The class name of real exception that needs to be handled by error-handler. This will be wrapped inside the application exception. For example: ServiceUnavailable, TimeoutException, HttpClientResponseException **Note**: After migrating the framework from Springboot to Micronaut, the WebClientResponseException is changed to HttpClientResponseException.
error_type	Type of the error handled.
operation	The tagged operation during which the error occurred.
origin	The tagged origin of error.
rule_name	The name of rule configured and evaluated by error-handler to resolve the issue.
source_interface	The name of interface/NF from which the communication started.
target_interface	The name of interface/NF to which the communication targeted.
error_resolved	Boolean flag which determines if the error is resolved by error-handler.
search_key_type	Key used during the search operation. Possible Values: SUPI, PDS_LOCATION, GPSI, SSVID, SUPI/GPSI, PDS_PROFILE_ID, PDS_USER_ID, SY_SESSION_ID, NA (used when operation is not SEARCH)
migration_enabled	Indicates if migration is in progress. Possible values:true, false
mode	Indicates current mode, which includes the selected typeOfSearch or preferenceKey in the UI.Possible values are listed in below Mode table: **Table 9-3 Format of different modes** **Mode** / **PK generated format** 0 or NULL / Multi-UE Id - UUID 16832 / Single-UE Id (supi##gpsi##src_type##siteid) 16768 / Single-UE Id (supi##src_type##siteid) 16704 / Single-UE Id (gpsi##src_type##siteid) 17088 / Partition based Single-UE Id (supi##gpsi) 17024 / Partition based Single-UE Id (supi) 16960 / Partition based Single-UE Id (gpsi)
prev_mode	Previous mode, which includes the earlier selected typeOfSearch or preferenceKey in the UI.Possible values are listed in above Mode table. Migration type (single → multi, multi → single, or single → single) is derived by comparing prev_mode and mode.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-2 Dimension Description

Dimension	Description
response_content	Indicates whether the DB query response content is empty or not. Possible values: EMPTY, NON_EMPTY

9.1 TLS Metrics

The following table describes the TLS metrics and the respective dimensions:

Table 9-4 oc_ingressgateway_incoming_tls_connections

Field	Details
Description	Number of TLS Connections received on the Ingress Gateway and their negotiated TLS versions. The versions can be TLSv1.3 or TLSv1.2
Type	Gauge
Dimensions	• NegotiatedTLSVersion • direction • instanceIdentifier
Example	-

Table 9-5 oc_egressgateway_incoming_tls_connections

Field	Details
Description	Number of TLS Connections received on the Egress Gateway and their negotiated TLS versions. The versions can be TLSv1.3 or TLSv1.2
Type	Gauge
Dimensions	• NegotiatedTLSVersion • direction • instanceIdentifier
Example	-

Table 9-6 security_cert_x509_expiration_seconds

Field	Details
Description	Indicates the time to certificate expiry in epoch seconds.
Type	Histogram
Dimensions	serialNumber
Example	-

Table 9-7 diam_conn_network

Field	Details
Description	Indicates the number of TLS connections per TLS version.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-7 (Cont.) diam_conn_network

Field	Details
Dimensions	• tlsversion • peerHost • peerRealm
Example	-

Table 9-8 diam_failed_conn_network

Field	Details
Description	Indicates the number of failed TLS connections. **Note:** It is applicable when we configure **Initiate Connection** to `true` in peer node configurations in the CNC Console.
Type	Gauge
Dimensions	• tlsversion • reason
Example	diam_failed_conn_network{peerName="dgw",reason="SSL Handshake Exception",} 1.0

Table 9-9 diam_conn_network_responder

Field	Details
Description	Indicates the number of allowed TLS responder connections with or without the peer configuration.
Type	Gauge
Dimensions	• tlsversion • peerconfigvalidated • peerHost • peerRealm
Example	-

Table 9-10 dgw_tls_cert_expiration_seconds

Field	Details
Description	Indicates the number of allowed TLS responder connections with or without the peer configuration.
Type	Gauge
Dimensions	• serialNumber (a number assigned by CA to each certificate) • subject (information about the cert issuer)
Example	dgw_tls_cert_expiration_seconds{serialNumber="122859034516052844067924392230910496431389299229",subject="OU=CGIU, O=ORCL, L=BLR, ST=KA, C=IN",} 1.797882352E9

Copyright © 2019, 2026, Oracle and/or its affiliates.

9.2 Egress Gateway Metrics for SCP

> **Note**
>
> Peer health pings happen in Primary pod only and not in secondary pod due to which metrics are getting pegged in Primary pod only.

This section provides details about SCP health monitoring metrics and the respective dimensions.

Table 9-11 oc_egressgateway_peer_health_status

Field	Details
Description	It defines Egress Gateway peer health status. • This metric is set to 1, if a peer is unhealthy. • This metric is reset to 0, when it becomes healthy again. • This metric is set to -1, if peer is removed from peerconfiguration.
Metric Type	Gauge
Dimensions	• peer • vfqdn

Examples:

- oc_egressgateway_peer_health_status{"peer":"10.75.213.172:8080"} 1.0
- oc_egressgateway_peer_health_status{"peer":"10.75.213.172:8080"} 0.0
- oc_egressgateway_peer_health_status{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 1.0
- oc_egressgateway_peer_health_status{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 0.0

Table 9-12 oc_egressgateway_peer_health_ping_request_total

Field	Details
Description	This metric is incremented every time a health ping is sent toward a peer.
Metric Type	Counter
Dimensions	• peer • vfqdn

Examples:

- oc_egressgateway_peer_health_ping_request_total{"peer":"10.75.213.172:8080"} 389.0
- oc_egressgateway_peer_health_ping_request_total{"peer":"10.75.213.172:8080"} 439.0
- oc_egressgateway_peer_health_ping_request_total{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 389.0
- oc_egressgateway_peer_health_ping_request_total{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 439.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-13 oc_egressgateway_peer_health_ping_response_total

Field	Details
Description	This metric is incremented every time a health ping response is received from a peer irrespective of success or failure.
Metric Type	Counter
Dimensions	• peer • vfqdn • statusCode • cause

Examples:

- oc_egressgateway_peer_health_ping_response_total{"peer":"10.75.213.172:8080","status":"httpstatus","cause":""} 89.0
- oc_egressgateway_peer_health_ping_response_total{"peer":"10.75.213.172:8080","status":"Exception","cause":"exception cause"} 39.0
- oc_egressgateway_peer_health_ping_response_total{"vfqdn":"http://abc.com","status":"httpstatus","cause":""} 89.0
- oc_egressgateway_peer_health_ping_response_total{"vfqdn":"http://abc.com","status":"Exception","cause":"exception cause"} 39.0

Table 9-14 oc_egressgateway_peer_health_status_transitions_total

Field	Details
Description	This metric is incremented every time a peer is transitioned from Available to Unavailable or from Unavailable to Available.
Metric Type	Counter
Dimensions	• peer • vfqdn • from • to

Examples:

- oc_egressgateway_peer_health_status_transitions_total{"identifier":"10.75.213.172:8080","from":"available","to":"unavailable"} 14.0
- oc_egressgateway_peer_health_status_transitions_total{"identifier":"10.75.213.172:8080","from":"unavailable","to":"available"} 34.0
- oc_egressgateway_peer_health_status_transitions_total{"vfqdn":"http://abc.com",*"peer":"10.75.213.172:8080",*"from":"unavailable","to":"available"} 34.0
- oc_egressgateway_peer_health_status_transitions_total{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080","from":"available","to":"unavailable"} 14.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-15 counterespionage

Field	Details
Description	This metric is incremented every time for the peer count.
Metric Type	Gauge
Dimensions	• peerset

Examples:

- counterespionage{"peerset":"set-0"} 3.0

Table 9-16 oc_egressgateway_peer_available_count

Field	Details
Description	This metric is incremented every time for the available peer count.
Metric Type	Gauge
Dimensions	• peerset

Examples:

- oc_egressgateway_peer_available_count{"peerset":"set-0"} 4.0

9.3 Correlation-Info Header Metrics

For every correlation-info header received or newly generated, a metric is pegged. Following are the list of metrics:

Below table lists the metrics that is implemented as part of this feature with the following Dimensions:

1. operation_type= {"create","update","delete","subscribe","unsubscribe","terminate","register","deregister"}
2. correlation_info_type={"imsi", "msisdn", "imsi,msisdn"}

Table 9-17 occnp_correlation_info_header_received

Field	Details
Description	PCF reports the total incoming requests that are carrying the correlation-info header.
Metric Type	Counter
Dimensions	• operation_type • correlation_info_type

Example:

- occnp_correlation_info_header_received_total '{correlation_info_type="imsi", operation_type="create"}',2
- occnp_correlation_info_header_received_total '{correlation_info_type="imsi", operation_type="update"}',1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-18 occnp_correlation_info_header_forwarded

Field	Details
Description	PCF reports the total outgoing requests that are carrying the correlation-info header.
Metric Type	Counter
Dimensions	• operation_type • correlation_info_type

Example:

- occnp_correlation_info_header_forwarded_total '{correlation_info_type="imsi", operation_type="subscribe"}',2

Table 9-19 occnp_correlation_info_header_generated

Field	Details
Description	PCF reports the total responses that are carrying the correlation-info header.
Metric Type	Counter
Dimensions	• operation_type • correlation_info_type

Example:

- occnp_correlation_info_header_generated_total '{correlation_info_type="imsi", operation_type="create"}',2

9.4 Config Server Metrics

The following table describes the Config Server metrics and respective dimensions:

Table 9-20 topic_version

Field	Details
Description	Config-service will have this metrics a database value from each topic version. The Services fetching the configurations from Configuration Server, will have its current topic version till which configurations has been fetched successfully. **Note**: This counter metric keep updating on every successful iteration.
Metric Type	Gauge
Dimensions	• Service Name • Pod Name

Examples:

- topic_version{topicName="pcf.public.sessionrule",} 77.0
- topic_version{topicName="common.logging.diam-connector",} 53.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

- topic_version{topicName="pcf.userservice.cfg",} 35.0
- topic_version{topicName="pcrf.public.networkelement.pgw",} 2.0
- topic_version{topicName="NRF.BSF",} 20.0
- topic_version{topicName="common.bindingservice.cfg",} 6.0
- topic_version{topicName="common.logging.policy-ds",} 21.0
- topic_version{topicName="NRF.UDR",} 22.0
- topic_version{topicName="common.logging.diam-gateway",} 93.0
- topic_version{topicName="common.logging.pcf-user",} 35.0
- topic_version{topicName="common.logging.pcf-sm",} 78.0
- topic_version{topicName="pcrf.coreservice",} 3.0
- topic_version{topicName="public.policy.project",} 148.0
- topic_version{topicName="Subscriptions",} 14.0
- topic_version{topicName="pcf.smservice.cfg",} 126.0
- topic_version{topicName="common.public.feature1",} 10.0
- topic_version{topicName="common.public.diampeernode",} 2.0
- topic_version{topicName="common.logging.pcrf-core",} 2.0
- topic_version{topicName="pcf.public.authorizeddefaultqos",} 77.0
- topic_version{topicName="public.policy.project.content",} 85.0
- topic_version{topicName="pcf.public.pccrule",} 85.0
- topic_version{topicName="NRF.CHF",} 52.0
- topic_version{topicName="config.level",} 1053.0
- topic_version{topicName="pds.public.settings",} 2.0

Table 9-21 occnp_config_server_overall_processing_time_seconds

Field	Details
Description	Configuration server's overall processing time.
Type	Summary
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-22 occnp_config_server_overall_processing_time_seconds_max

Field	Details
Description	Configuration service overall processing time.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-22 (Cont.) occnp_config_server_overall_processing_time_seconds_max

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Examples:

- occnp_config_server_overall_processing_time_seconds_max{error="none", exception="none", method="POST", outcome="SUCCESS", status="201", uri="/binding/v1/contextBinding/context-owner/{contextOwner}",} 2.595594434
- occnp_config_server_overall_processing_time_seconds_max{error="none", exception="none", method="DELETE", outcome="SUCCESS", status="204", uri="/binding/v1/contextBinding/contextId/{contextId}",} 0.276239293
- occnp_config_server_overall_processing_time_seconds_max{error="ContextBindingNotFound", exception="ContextBindingNotFound", method="DELETE", outcome="CLIENT_ERROR", status="404", uri="/binding/v1/contextBinding/cleanup",} 0.115288423

Table 9-23 occnp_config_server_overall_processing_time_seconds_count

Field	Details
Description	Configuration service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Examples:

- occnp_config_server_overall_processing_time_seconds_count{error="none", exception="none", method="POST", outcome="SUCCESS", status="201", uri="/binding/v1/contextBinding/context-owner/{contextOwner}",} 3.0
- occnp_config_server_overall_processing_time_seconds_count{error="none", exception="none", method="DELETE", outcome="SUCCESS", status="204", uri="/binding/v1/contextBinding/contextId/{contextId}",} 3.0
- occnp_config_server_overall_processing_time_seconds_count{error="ContextBindingNotFound", exception="ContextBindingNotFound",method="DELETE",outcome="CLIENT_ERROR",status="404",uri="/binding/v1/contextBinding/cleanup",} 6.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-24 occnp_config_server_overall_processing_time_seconds_sum

Field	Details
Description	Configuration service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Examples:

- occnp_config_server_overall_processing_time_seconds_sum{error="none",exception="none",method="POST", outcome="SUCCESS", status="201", uri="/binding/v1/contextBinding/context-owner/{contextOwner}",} 5.861114721
- occnp_config_server_overall_processing_time_seconds_sum{error="none", exception="none",method="DELETE",outcome="SUCCESS",status="204",uri="/binding/v1/contextBinding/contextId/{contextId}",} 0.349598291
- occnp_config_server_overall_processing_time_seconds_sum{error="ContextBindingNotFound",exception="ContextBindingNotFound", method="DELETE",outcome="CLIENT_ERROR",status="404", uri="/binding/v1/contextBinding/cleanup",} 0.203103476

Table 9-25 occnp_config_server_db_operation_time_seconds_count

Field	Details
Description	Configuration service overall database processing time.
Type	Gauge
Dimension	• exception • method • repository • state

Examples:

- occnp_config_server_db_operation_time_seconds_count{exception="None",method="findByTopicInfo",repository="ConfigurationItemRepository",state="SUCCESS",} 7721880.0
- occnp_config_server_db_operation_time_seconds_count{exception="None",method="findByName",repository="TopicInfoRepository",state="SUCCESS",} 8190322.0

Table 9-26 occnp_config_server_db_operation_time_seconds_sum

Field	Details
Description	Configuration service overall database processing time.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-26 (Cont.) occnp_config_server_db_operation_time_seconds_sum

Field	Details
Dimension	• exception • method • repository • state

Examples:

- occnp_config_server_db_operation_time_seconds_sum{exception="None",method="findByTopicInfo",repository="ConfigurationItemRepository",state="SUCCESS",} 4713.01
- occnp_config_server_db_operation_time_seconds_sum{exception="None",method="findByName",repository="TopicInfoRepository",state="SUCCESS",} 6328.74490

Table 9-27 occnp_config_server_db_operation_time_seconds_max

Field	Details
Description	Configuration service overall database processing time.
Type	Gauge
Dimension	• exception • method • repository • state

9.5 SM Service Metrics

The following table describes the SM Service metrics and respective dimensions:

Table 9-28 ocpm_ingress_request_total

Field	Details
Description	Total number of ingress requests received.
Metric Type	Counter
Dimensions	• operation_type • dnn • snssai • nf_instance_id • sbi_priority • servicename_3gpp • application • hostname • rat_type • access_type

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-28 (Cont.) ocpm_ingress_request_total

Field	Details
Examples	• ocpm_ingress_request_total{access_type="",application="pcf_smservice",dnn="internet",nf_instance_id="",operation_type="delete",rat_type="",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",} 1.0 • ocpm_ingress_request_total{access_type="",application="pcf_smservice",dnn="",nf_instance_id="",operation_type="update",rat_type="NR",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="",} 1.0 • ocpm_ingress_request_total{access_type="",application="pcf_smservice",dnn="internet",nf_instance_id="",operation_type="update",rat_type="NR",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",} 1.0 • ocpm_ingress_request_total{access_type="",application="pcf_smservice",dnn="",nf_instance_id="",operation_type="delete",rat_type="NR",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="",} 1.0 • ocpm_ingress_request_total{access_type="",application="pcf_smservice",dnn="",nf_instance_id="",operation_type="update",rat_type="",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="",} 1.0 • ocpm_ingress_request_total{access_type="",application="pcf_smservice",dnn="internet",nf_instance_id="",operation_type="update",rat_type="WLAN",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",} 1.0 • ocpm_ingress_request_total{access_type="3GPP_ACCESS",application="pcf_smservice",dnn="internet",nf_instance_id="",operation_type="create",rat_type="EUTRA",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",} 3.0

Table 9-29 ocpm_ingress_response_total

Field	Details
Description	Total number of ingress responses.
Metric Type	Counter
Dimensions	• operation_type • dnn • snssai • nf_instance_id • sbi_priority • servicename_3gpp • response_code • binding_level • binding_id • application • hostname • spendingLimitDataSource • cause • rat_type • access_type

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-29 (Cont.) ocpm_ingress_response_total

Field	Details
Examples	• ocpm_ingress_response_total{access_type="",application="pcf_smservice",binding_id="",binding_level="",cause="UNSPECIFIED_MSG_FAILURE",dnn="",nf_instance_id="",operation_type="update",rat_type="",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="",spendingLimitDataSource="",} 1.0 • ocpm_ingress_response_total{access_type="3GPP_ACCESS",application="pcf_smservice",binding_id="",binding_level="",cause="",dnn="internet",nf_instance_id="",operation_type="create",rat_type="EUTRA",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",spendingLimitDataSource="",} 2.0 • ocpm_ingress_response_total{access_type="",application="pcf_smservice",binding_id="",binding_level="",cause="SUBSCRIPTION_NOT_FOUND",dnn="",nf_instance_id="",operation_type="update",rat_type="NR",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="",spendingLimitDataSource="",} 1.0 • ocpm_ingress_response_total{access_type="3GPP_ACCESS",application="pcf_smservice",binding_id="",binding_level="",cause="WWW-Authenticate",dnn="internet",nf_instance_id="",operation_type="create",rat_type="EUTRA",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",spendingLimitDataSource="",} 1.0 • ocpm_ingress_response_total{access_type="",application="pcf_smservice",binding_id="",binding_level="",cause="",dnn="internet",nf_instance_id="",operation_type="update",rat_type="NR",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",spendingLimitDataSource="",} 1.0 • ocpm_ingress_response_total{access_type="",application="pcf_smservice",binding_id="",binding_level="",cause="",dnn="internet",nf_instance_id="",operation_type="delete",rat_type="",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",spendingLimitDataSource="",} 1.0 • ocpm_ingress_response_total{access_type="",application="pcf_smservice",binding_id="",binding_level="",cause="SUBSCRIPTION_NOT_FOUND",dnn="",nf_instance_id="",operation_type="delete",rat_type="NR",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="",spendingLimitDataSource="",} 1.0 • ocpm_ingress_response_total{access_type="",application="pcf_smservice",binding_id="",binding_level="",cause="",dnn="internet",nf_instance_id="",operation_type="update",rat_type="WLAN",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="1-null",spendingLimitDataSource="",} 1.0

Table 9-30 ocpm_egress_request_total

Field	Details
Description	Total number of egress requests received.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-30 (Cont.) ocpm_egress_request_total

Field	Details
Dimensions	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exported_application • helm_sh_chart • hostname • instance • io_kompose_service • job • microservice • mktgVersion • namespace • nf_name • operation_type • pod • pod_template_hash • servicename_3gpp • vendor • reason

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-30 (Cont.) ocpm_egress_request_total

Field	Details
Examples	• ocpm_egress_request_total{app_kubernetes_io_instance = "ocpcf",app_kubernetes_io_managed_by = "Helm",app_kubernetes_io_name = "sm-service",app_kubernetes_io_part_of = "occnp",app_kubernetes_io_version = "1.0.0",application = "occnp",container = "sm-service",endpoint = "cnc-metrics",engVersion = "23.4.0",exported_application = "pcf_smservice",helm_sh_chart = "sm-service-23.4.0",hostname = "ocpcf-pcf-smservice-8576fc787-8z6zl",instance = "10.233.103.137:9000",io_kompose_service = "ocpcf-pcf-smservice",job = "occne-infra/occne-nf-cnc-podmonitor",microservice = "occnp_pcf_sm",mktgVersion = "1.0.0",namespace = "gg-pcf1",nf_name = "svc-perfgo.gg-perfgo-client",operation_type = "update_notify",pod = "ocpcf-pcf-smservice-8576fc787-8z6zl",pod_template_hash = "8576fc787",servicename_3gpp = "npcf-smpolicycontrol",vendor = "Oracle"} 1.0 ; Type-Counter • ocpm_egress_request_total{application="pcf_smservice",binding_id="",binding_level="",dnn="dnn1",nf_instance_id="null",nf_name="",operation_type="tdf_notify_create_session_request",retry="",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",spendingLimitDataSource="",} 1.0 • ocpm_egress_request_total{application="pcf_smservice",binding_id="",binding_level="",dnn="dnn1",nf_instance_id="null",nf_name="",operation_type="tdf_notify_terminate_session_request",retry="",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",reason="PRIMARY_SESSION_DELETED",snssai="11-abc123",spendingLimitDataSource="",} 1.0 • ocpm_egress_request_total{application="pcf_smservice",binding_id="",binding_level="",dnn="dnn1",nf_instance_id="null",nf_name="",operation_type="tdf_notify_update_session_request",retry="",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",reason="MSGTYPE_MODIFY",snssai="11-abc123",spendingLimitDataSource="",} 3.0

Table 9-31 ocpm_egress_response_total

Field	Details
Description	Total number of egress responses.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-31 (Cont.) ocpm_egress_response_total

Field	Details
Dimensions	• operation_type • dnn • snssai • nf_instance_id • sbi_priority • servicename_3gpp • response_code • latency • reason

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-31 (Cont.) ocpm_egress_response_total

Field	Details
Examples	• ocpm_egress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",nf_name="smf-xxxx.com",latency="9",operation_type="update_notify",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter • ocpm_egress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",nf_name="smf-xxxx.com",latency="6",operation_type="terminate_notify",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter • ocpm_egress_response_total{application="pcf_smservice",cause="PENDING_TRANSACTION",dnn="",hostname="jiandong-pcf-smservice-6dbcc9bb9b-swdvj",latency="0",nf_instance_id="",nf_name="",operation_type="update_notify",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="",} 1.0 • ocpm_egress_response_total{application="pcf_smservice",cause="",dnn="dnn1",latency="0",nf_instance_id="null",nf_name="",operation_type="tdf_notify_create_session_request",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 • ocpm_egress_response_total{application="pcf_smservice",cause="",dnn="dnn1",latency="0",nf_instance_id="null",nf_name="",operation_type="tdf_notify_terminate_session_request",response_code="2xx",sbi_priority="",reason="PRIMARY_SESSION_DELETED",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 • ocpm_egress_response_total{application="pcf_smservice",cause="",dnn="dnn1",latency="0",nf_instance_id="null",nf_name="",operation_type="tdf_notify_update_session_request",response_code="2xx",sbi_priority="",reason="MSGTYPE_MODIFY",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",}

Table 9-32 occnp_sm_binding_request_total

Field	Details
Description	Total number of binding requests.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-32 (Cont.) occnp_sm_binding_request_total

Field	Details
Dimensions	• application • dnn • mode • operation_type • snssai

Examples:

- occnp_sm_binding_request_total{application="pcf_smservice",dnn="dnn1",hostname="a-pcf-smservice-fbbfccdf-vvdr6",mode="synchronous",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",nf_name="bsf.xxxx.com",operation_type="create",snssai="11-abc111",} 1.0; Type-Counter
- occnp_sm_binding_request_total{application="pcf_smservice",dnn="dnn1",hostname="a-pcf-smservice-fbbfccdf-vvdr6",mode="synchronous",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",nf_name="bsf.xxxx.com",operation_type="update",snssai="11-abc111",} 1.0; Type-Counter
- occnp_sm_binding_request_total{application="pcf_smservice",dnn="dnn1",hostname="a-pcf-smservice-fbbfccdf-vvdr6",mode="synchronous",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",nf_name="bsf.xxxx.com",operation_type="delete",snssai="11-abc111",} 1.0; Type-Counter

Table 9-33 occnp_sm_binding_response_total

Field	Details
Description	Total number of binding responses.
Metric Type	Counter
Dimensions	• application • dnn • mode • operation_type • snssai • response code

Examples:

- occnp_sm_binding_response_total{application="pcf_smservice",dnn="dnn1",hostname="a-pcf-smservice-fbbfccdf-vvdr6",mode="synchronous",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",nf_name="bsf.xxxx.com",operation_type="create",response_code="2xx",snssai="11-abc111",} 1.0; Type-Counter
- occnp_sm_binding_response_total{application="pcf_smservice",dnn="dnn1",hostname="a-pcf-smservice-fbbfccdf-vvdr6",mode="synchronous",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",nf_name="bsf.xxxx.com",operation_type="update",response_code="2xx",snssai="11-abc111",} 1.0; Type-Counter
- occnp_sm_binding_response_total{application="pcf_smservice",dnn="dnn1",hostname="a-pcf-smservice-fbbfccdf-vvdr6",mode="synchronous",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",nf_name="bsf.xxxx.com",operation_type="delete",response_code="2xx",snssai="11-abc111",} 1.0; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-34 occnp_sm_binding_ex_total

Field	Details
Description	The number of binding operations that cannot be performed due to an exception (timeout).
Metric Type	Counter
Dimensions	• application • dnn • snssai • operation_type • mode

Examples:

- occnp_sm_binding_ex_total{application="pcf_smservice",dnn="dnn1",snssai="1-000001",operation_type="create",mode="asynchronous",} 1.0 ; Type-Counter
- occnp_sm_binding_ex_total{application="pcf_smservice",dnn="dnn1",snssai="1-000001",operation_type="update",mode="asynchronous",} 1.0 ; Type-Counter
- occnp_sm_binding_ex_total{application="pcf_smservice",dnn="dnn1",snssai="1-000001",operation_type="delete",mode="asynchronous",} 1.0 ; Type-Counter

Table 9-35 ocpm_egress_request_timeout_total

Field	Details
Description	Total number of request timeouts from SMF.
Metric Type	Counter
Dimensions	• application • dnn • egress_service • hostname • nf_instance_id • operation_type • resource_name • sbi_priority • service_name • snssai

Examples:

- ocpm_egress_request_timeout_total{application="pcf_smservice",dnn="dnn1",egress_service="SMF",hostname="pcf_smservice",nf_instance_id="",nf_name="smf-xxxx.com",operation_type="POST",resource_name="SmPolicyNotification",sbi_priority="",service_name="notification",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0; Type-Counter
- ocpm_egress_request_timeout_total{application="pcf_smservice",dnn="dnn1",egress_service="SMF",hostname="pcf_smservice",nf_instance_id="",nf_name="smf-xxxx.com",operation_type="POST",resource_name="TerminationNotification",sbi_priority="",service_name="notification",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0; Type-Counter
- ocpm_egress_request_timeout_total{application="pcf_smservice",dnn="dnn1",egress_service="BSF",hostname="pcf_smservice",nf_instance_id="fe7d992b-0541-4c7d-

Copyright © 2019, 2026, Oracle and/or its affiliates.

ab84-6d70b1babc1",nf_name="bsf-xxxx.com",operation_type="POST",resource_name="PCFSessionBindings",sbi_priority="",service_name="nbsf-management",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0; Type-Counter

- ocpm_egress_request_timeout_total{application="pcf_smservice",dnn="dnn1",egress_service="BSF",hostname="pcf_smservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",nf_name="bsf-xxxx.com",operation_type="DELETE",resource_name="IndividualPCFSessionBinding",sbi_priority="",service_name="nbsf-management",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0; Type-Counter
- ocpm_egress_request_timeout_total{application="pcf_smservice",dnn="", egress_service="TDF",nf_instance_id="",nf_name="localhost",operation_type="tdf_notify_create_session_request",resource_name="",sbi_priority="",service_name="notification",servicename_3gpp="npcf-smpolicycontrol",snssai="",} 1.0

Table 9-36 remote_delete_notify_total

Field	Details
Description	Total number of notifications for session delete requests at SM service.
Metric Type	Counter
Dimensions	• Code • Request • SessionType • application • hostname

Examples:

- remote_delete_notify_total{Code="2xx",Request="DeleteNotify",SessionType="SM",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0
- remote_delete_notify_total{Code="4xx",Request="DeleteNotify",SessionType="SM",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0
- remote_delete_notify_total{Code="5xx",Request="DeleteNotify",SessionType="SM",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0
- remote_delete_notify_total{Code="N/A",Request="EmulateDelete",SessionType="SM",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0

Table 9-37 audit_notifications_sent_total

Field	Details
Description	Number of audit notifications to SM service that are processed.
Metric Type	Counter
Dimensions	• ServiceType • SiteId • Request • SessionType • SvcType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-38 audit_update_notify_session_not_found_total

Field	Details
Description	Number of 404 response sent by SMF for the records which are identified as stale by Audit Service.
Metric Type	Counter
Dimensions	• ServiceType • SiteId • Request • SessionType • ResponseCode

Table 9-39 audit_update_notify_session_found_total

Field	Details
Description	Number of 204 response sent by SMF for the records which are identified as stale by Audit Service.
Metric Type	Counter
Dimensions	• ServiceType • SiteId • Request • SessionType • ResponseCode

Table 9-40 audit_update_notify_response_error_total

Field	Details
Description	Number of update notify requests sent to SMF by SM service that were responded with an error code (except 404)
Metric Type	Counter
Dimensions	• ServiceType • SiteId • SessionType • ResponseCode

Table 9-41 audit_update_timestamp_cnt_total

Field	Details
Description	Number of records whose LASTACESSTIME column is updated by SM Service when it receives 204 response from SMF
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-41 (Cont.) audit_update_timestamp_cnt_total

Field	Details
Dimensions	• ServiceType • SiteId • Request • ResponseCode • SessionType

Table 9-42 audit_delete_records_count_total

Field	Details
Description	Number of records deleted by SM Service when it receives 404 response from SMF.
Metric Type	Counter
Dimensions	• ServiceType: SM • SiteId: <siteId> • Request: UpdateNotify/"" • ResponseCode: <ResponseCode> • SessionType • Cause: QueryTdfDisable/ PrimarySessionDoesNotExist/ SessionNotfound/ ""

Table 9-43 audit_delete_records_max_ttl_count_total

Field	Details
Description	Number of records deleted by SM Service when the max TTL was reached
Metric Type	Counter
Dimensions	• ServiceType • SiteId • Request • SessionType

Table 9-44 session_oam_request_total

Field	Details
Description	Number of session requests for SM Service
Metric Type	Request
Dimensions	• Response Code • Operation Type • SessionType
Examples	• session_oam_request_total{application="pcf_smservice",operationType="get",session_type="TDF",} 1.0 • session_oam_request_total{application="pcf_smservice",operationType="terminate",session_type="TDF",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-45 session_oam_response_total

Field	Details
Description	Number of session responses for SM Service
Metric Type	Response
Dimensions	• Response Code • Operation Type • SessionType
Examples	• session_oam_response_total{application="pcf_smservice",operationType="get",responseCode="2xx",session_type="TDF",} 1.0 • session_oam_response_total{application="pcf_smservice",operationType="get",responseCode="4xx",session_type="TDF",} 1.0 • session_oam_response_total{application="pcf_smservice",operationType="terminate",responseCode="2xx",session_type="SM",} 2.0 • session_oam_response_total{application="pcf_smservice",operationType="terminate",responseCode="2xx",session_type="TDF",} 1.0

Table 9-46 occnp_http_sm_request_total

Field	Details
Description	Total number of http requests.
Metric Type	Request
Dimensions	• application • nf_instance_id • nfName • operationType • operation_type • service_name
Examples	• occnp_http_sm_request_total{application="pcf_smservice",nfInstanceId="", nfName="",operationType="bulwark_lock",request="update_notify",retry="false",servicenameNon3gpp="npcf-smpolicycontrol",} 3.0 • occnp_http_sm_request_total{application="pcf_smservice",nfInstanceId="",nfName="", operationType="bulwark_unlock",request="create",retry="false",servicenameNon3gpp="npcf-smpolicycontrol",} 1.0

Table 9-47 occnp_http_sm_response_total

Field	Details
Description	Total number of http responses.
Metric Type	Response

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-47 (Cont.) occnp_http_sm_response_total

Field	Details
Dimensions	• application • nf_instance_id • nfName • operationType • operation_type • service_name
Examples	• occnp_http_sm_response_total{application="pcf_smservice",dnn="",nfInstanceId="",nfName="", operationType="bulwark_lock",request="update_notify",responseCode="423",servicenameNon3gpp="npcf-smpolicycontrol",snssai="",} 1.0 • occnp_http_sm_response_total{application="pcf_smservice",dnn="dnn1",nfInstanceId="", nfName="",operationType="bulwark_unlock",request="create",responseCode="204", servicenameNon3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0

Table 9-48 occnp_http_in_conn_request_total

Field	Details
Description	The requests received by a micro-service from downstream.
Metric Type	Counter
Dimensions	• application • dnn • hostname • operationType • priority • sessRuleReports • rattype • accesstype

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-48 (Cont.) occnp_http_in_conn_request_total

Field	Details
Examples	• occnp_http_in_conn_request_total{accessType="",application="pcf_smservice",dnn="internet",nfInstanceId="",operationType="update",priority="",ratType="NR",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",} 1.0 • occnp_http_in_conn_request_total{accessType="3GPP_ACCESS",application="pcf_smservice",dnn="internet",nfInstanceId="",operationType="create",priority="",ratType="EUTRA",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",} 3.0 • occnp_http_in_conn_request_total{accessType="",application="pcf_smservice",dnn="",nfInstanceId="",operationType="delete",priority="",ratType="NR",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",} 1.0 • occnp_http_in_conn_request_total{accessType="",application="pcf_smservice",dnn="internet",nfInstanceId="",operationType="delete",priority="",ratType="",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",} 1.0 • occnp_http_in_conn_request_total{accessType="3GPP_ACCESS",application="pcf_smservice",dnn="internet",nfInstanceId="",operationType="create",priority="",ratType="NR",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",} 1.0 • occnp_http_in_conn_request_total{accessType="NON_3GPP_ACCESS",application="pcf_smservice",dnn="",nfInstanceId="",operationType="update",priority="",ratType="EUTRA",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",} 1.0 • occnp_http_in_conn_request_total{accessType="",application="pcf_smservice",dnn="",nfInstanceId="",operationType="update",priority="",ratType="NR",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",} 1.0 • occnp_http_in_conn_request_total{accessType="",application="pcf_smservice",dnn="",nfInstanceId="",operationType="delete",priority="",ratType="",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-49 occnp_http_in_conn_response_total

Field	Details
Description	The response sent for incoming requests to a micro-service.
Metric Type	Counter
Dimensions	• application • bindingId • bindingLevel • dnn • hostname • nfInstanceId • operationType • priority • responseCode • servicename3gpp • sessRuleReports • snssai • spendingLimitDataSource • ratType • accessType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-49 (Cont.) occnp_http_in_conn_response_total

Field	Details
Example	• occnp_http_in_conn_response_total{accessType="NON_3GPP_ACCESS",application="pcf_smservice",bindingId="",bindingLevel="",cause="SUBSCRIPTION_NOT_FOUND",dnn="",nfInstanceId="",operationType="update",priority="",ratType="EUTRA",responseCode="404",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="",application="pcf_smservice",bindingId="",bindingLevel="",cause="SUBSCRIPTION_NOT_FOUND",dnn="",nfInstanceId="",operationType="update",priority="",ratType="NR",responseCode="404",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="",application="pcf_smservice",bindingId="",bindingLevel="",cause="SUBSCRIPTION_NOT_FOUND",dnn="",nfInstanceId="",operationType="delete",priority="",ratType="",responseCode="404",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="",application="pcf_smservice",bindingId="",bindingLevel="",cause="",dnn="internet",nfInstanceId="",operationType="update",priority="",ratType="NR",responseCode="200",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="3GPP_ACCESS",application="pcf_smservice",bindingId="",bindingLevel="",cause="WWW-Authenticate",dnn="internet",nfInstanceId="",operationType="create",priority="",ratType="EUTRA",responseCode="401",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="",application="pcf_smservice",bindingId="",bindingLevel="",cause="",dnn="internet",nfInstanceId="",operationType="delete",priority="",ratType="",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="",application="pcf_smservice",bindingId="",bindingLevel="",cause="SUBSCRIPTION_NOT_FOUND",dnn="",nfInstanceId="",operationType="delete",priority="",ratType="NR",respon

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-49 (Cont.) occnp_http_in_conn_response_total

Field	Details
	seCode="404",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="3GPP_ACCESS",application="pcf_smservice",bindingId="",bindingLevel="",cause="",dnn="internet",nfInstanceId="",operationType="create",priority="",ratType="NR",responseCode="201",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",spendingLimitDataSource="",} 1.0 • occnp_http_in_conn_response_total{accessType="3GPP_ACCESS",application="pcf_smservice",bindingId="",bindingLevel="",cause="",dnn="internet",nfInstanceId="",operationType="create",priority="",ratType="EUTRA",responseCode="201",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",snssai="1-null",spendingLimitDataSource="",} 2.0

Table 9-50 http_in_conn_ext_request_total

Field	Details
Description	The requests received by a micro-service to update the ratType or accessType on receiving policyControlRequestTrigger as "AC_TY_CH", "PRA_CH", "RAT_TY_CH" or multiple values separated by comma. For delete requests policyControlRequestTrigger is not mandatory. This metric will be pegged after we know the source radio access type or the source access type during the update process. **Note**: This metric is not pegged if any of these values do not come as part of `policyControlRequestTrigger` dimension: • AC_TY_CH • PRA_CH • RAT_TY_CH They can come individually, together, or along other values. When list of values is received, at least one of the previous values must be present; otherwise, the metric is not be pegged.
Metric Type	Counter
Dimensions	• accessType • operationType • policyControlRequestTrigger • ratType • sourceAccessType • sourceRatType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-50 (Cont.) http_in_conn_ext_request_total

Field	Details
Examples	• occnp_http_in_conn_ext_request_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH",ratType="NR",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA"} 1.0 • occnp_http_in_conn_ext_request_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="PRA_CH",ratType="NR",sourceAccessType="3GPP_ACCESS",sourceRatType="NR"} 2.0 • occnp_http_in_conn_ext_request_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH,PRA_CH",ratType="NR",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA"} 1.0 • occnp_http_in_conn_ext_request_total{accessType="NON_3GPP_ACCESS",application="pcf_smservice",operationType="update",policyControlRequestTrigger="AC_TY_CH,NO_CREDIT,RAT_TY_CH,PRA_CH,UE_IP_CH",ratType="NR",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA"} 1.0 • occnp_http_in_conn_ext_request_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH",ratType="WLAN",sourceAccessType="3GPP_ACCESS",sourceRatType="NR",} 1.0 • occnp_http_in_conn_ext_request_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH",ratType="NR",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA",} 1.0 • occnp_http_in_conn_ext_request_total{accessType="",application="pcf_smservice",operationType="delete",policyControlRequestTrigger="",ratType="",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA",} 1.0

Table 9-51 http_in_conn_ext_response_total

Field	Details
Description	The response sent for incoming requests to a micro-service after update the ratType or when we receive the value of policyControlRequestTrigger as "AC_TY_CH", "PRA_CH", "RAT_TY_CH" or multiple values separated by comma. For delete requests policyControlRequestTrigger is not mandatory. **Note**: This metric is not pegged if any of these values do not come as part of `policyControlRequestTrigger` dimension: • AC_TY_CH • PRA_CH • RAT_TY_CH They can come individually, together, or along other values. When list of values is received, at least one of the previous values must be present; otherwise, the metric is not be pegged.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-51 (Cont.) http_in_conn_ext_response_total

Field	Details
Dimensions	• accessType • operationType • policyControlRequestTrigger • ratType • responseCode • sourceAccessType • sourceRatType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-51 (Cont.) http_in_conn_ext_response_total

Field	Details
Examples	• occnp_http_in_conn_ext_response_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH",ratType="NR", responseCode="204",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA"} 1.0 • occnp_http_in_conn_ext_response_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH,PRA_CH",ratType="NR", responseCode="204",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA"} 1.0 • occnp_http_in_conn_ext_response_total{accessType="3GPP_ACCESS",application="pcf_smservice",operationType="update",policyControlRequestTrigger="AC_TY_CH,NO_CREDIT,RAT_TY_CH,PRA_CH,UE_IP_CH",ratType="NR", responseCode="204",sourceAccessType="NON_3GPP_ACCESS",sourceRatType="EUTRA"} 1.0 • occnp_http_in_conn_ext_response_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="PRA_CH",ratType="NR",responseCode="400",sourceAccessType="3GPP_ACCESS",sourceRatType="NR"} 1.0 • occnp_http_in_conn_ext_response_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH,PRA_CH",ratType="NR",responseCode="400",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA"} 1.0 • occnp_http_in_conn_ext_response_total{accessType="NON_3GPP_ACCESS",application="pcf_smservice",operationType="update",policyControlRequestTrigger="AC_TY_CH,NO_CREDIT,RAT_TY_CH,PRA_CH,UE_IP_CH",ratType="EUTRA",responseCode="400",sourceAccessType="3GPP_ACCESS",sourceRatType="NR"} 1.0 • occnp_http_in_conn_ext_response_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH",ratType="WLAN",responseCode="200",sourceAccessType="3GPP_ACCESS",sourceRatType="NR",} 1.0 • occnp_http_in_conn_ext_response_total{accessType="",application="pcf_smservice",operationType="update",policyControlRequestTrigger="RAT_TY_CH",ratType="NR",responseCode="200",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA",} 1.0 • occnp_http_in_conn_ext_response_total{accessType="",application="pcf_smservice",operationType="delete",policyControlRequestTrigger=

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-51 (Cont.) http_in_conn_ext_response_total

Field	Details
	"",ratType="",responseCode="200",sourceAccessType="3GPP_ACCESS",sourceRatType="EUTRA",} 1.0

Table 9-52 occnp_http_out_conn_request_total

Field	Details
Description	Total number of http connection requests.
Metric Type	Counter
Dimensions	• application • bindingId • bindingLevel • hostname • nfInstanceId • operationType • priority • servicename3gpp • sessRuleReports • snssai • reason • isReattempt • isRetryAttempt • reattemptType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-52 (Cont.) occnp_http_out_conn_request_total

Field	Details
Examples	• occnp_http_out_conn_request_total{application="pcf_smservice",bindingId="",bindingLevel="",dnn="dnn1",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",nfInstanceId="",nfName="",operationType="update_notify",priority="",retry="Yes",servicename3gpp="npcf-smpolicycontrol",snssai="",} • occnp_http_out_conn_request_total{application="pcf_smservice",bindingId="",bindingLevel="",dnn="dnn1",nfInstanceId="",nfName="",operationType="tdf_notify_create_session_request",priority="",retry="",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="",snssai="11-abc123",spendingLimitDataSource="",} 1.0 • occnp_http_out_conn_request_total{application="pcf_smservice",bindingId=""bindingLevel="",dnn="dnn1",nfInstanceId="",nfName="",operationType="tdf_notify_terminate_session_request",priority="",retry="",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="",reason="PRIMARY_SESSION_DELETED",snssai="11-abc123",spendingLimitDataSource="",} 1.0 • occnp_http_out_conn_request_total{application="pcf_smservice",bindingId="",bindingLevel="",dnn="dnn1",nfInstanceId="",nfName="",operationType="tdf_notify_update_session_request",priority="",retry="",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="",snssai="11-abc123",reason="MSGTYPE_MODIFY",spendingLimitDataSource="",} 3.0 • occnp_http_in_conn_request_total{application="pcf_smservice",dnn="",nfInstanceId="",operationType="tdf_session_terminate_request",priority="",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="",snssai="",} 1.0

Table 9-53 occnp_http_out_conn_response_total

Field	Details
Description	Total number of http connection responses.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-53 (Cont.) occnp_http_out_conn_response_total

Field	Details
Dimensions	• application • cause • hostname • latency • nfInstanceId • operationType • responseCode • servicename3gpp • responseCode • reason
Examples	• occnp_http_out_conn_response_total{application="pcf_smservice",dnn="dnn1",cause="PENDING_TRANSACTION",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",latency="2",nfInstanceId="",nfName="",operationType="update_notify",responseCode="400",priority="",servicename3gpp="npcf-smpolicycontrol",snssai="",} • http_out_conn_response_total{application="pcf_smservice",cause="",dnn="dnn1",latency="0",nfInstanceId="",nfName="",operationType="tdf_notify_create_session_request",priority="",responseCode="200",servicename3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 • http_out_conn_response_total{application="pcf_smservice",cause="",dnn="dnn1",latency="0",nfInstanceId="",nfName="",operationType="tdf_notify_terminate_session_request",priority="",responseCode="200",reason="PRIMARY_SESSION_DELETED",servicename3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 • http_out_conn_response_total{application="pcf_smservice",cause="",dnn="dnn1",latency="0",nfInstanceId="",nfName="",operationType="tdf_notify_update_session_request",priority="",responseCode="200",reason="MSGTYPE_MODIFY",servicename3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 3.0 • occnp_http_in_conn_response_total{application="pcf_smservice",bindingId="",bindingLevel="",cause="NA",dnn="",nfInstanceId="",operationType="tdf_session_terminate_request",priority="",responseCode="200",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="",snssai="",spendingLimitDataSource="",} 1.0

Table 9-54 occnp_sm_sess_rule_failure_total

Field	Details
Description	Indicates failure count because of session rule failure

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-54 (Cont.) occnp_sm_sess_rule_failure_total

Field	Details
Metric Type	Counter
Dimensions	• application • failure • hostname • operationType • rule_id • rule_status

Table 9-55 lock_request_total

Field	Details
Description	Number of times the SM Service tries to acquire the lock
Metric Type	Counter
Dimensions	• application • podName • requestType • serviceName

Table 9-56 lock_response_total

Field	Details
Description	Number of times the Bulwark Service responds to SM Service for the lock request
Metric Type	Counter
Dimensions	• application • podName • requestType • serviceName • responseStatus • responseType

Table 9-57 occnp_http_sm_request_total

Field	Details
Description	Number of times the SM Service sends an update request
Metric Type	Counter
Dimensions	• application • nfInstanceId • nfName • operationType • request • servicenameNon3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-58 occnp_http_sm_response_total

Field	Details
Description	Number of times the SM Service receives a response
Metric Type	Counter
Dimensions	• application • latency • nfInstanceId • nfName • operationType • request • responseCode • servicenameNon3gpp

Table 9-59 occnp_lease_duration_seconds_bucket

Field	Details
Description	Time in seconds for which SM Service holds the lock
Metric Type	Histogram
Dimensions	• Lock_Lease_Duration • Message_Type • application • quartile

Table 9-60 rule_action

Field	Details
Description	Provides metric for: • `SUCC_RES_ALLO` sent in `lastreqruledata` • `SUCC_RES_ALLO` received from SMF
Metric Type	-
Dimensions	• ruleType • Type • Action

Examples:

- rule_action_total{action="SUCC_RES_ALLO",application="pcf_smservice",rule_type="pcc",type="request",} 1.0
- rule_action_total{action="SUCC_RES_ALLO",application="pcf_smservice",rule_type="pcc",type="report",} 1.0

Table 9-61 ocpm_timeout_total

Field	Details
Description	Total number of increments whenever a timeout is detected

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-61 (Cont.) ocpm_timeout_total

Field	Details
Metric Type	Counter
Dimensions	• operation • interface
Example	• ocpm_timeout_total{application="pcf_smservice",hostname="pdmayanspolicy-pcf-smservice-6b64cbdd8b-pzxkq",operationType="query_subs",servicename3gpp="npcf-sm-policy-control",targetService="USER_SERVICE",} 1.0

Table 9-62 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Metric Type	Gauge
Dimensions	• Service Name • Pod Name

Table 9-63 occnp_db_overall_processing_time_seconds_max

Field	Details
Description	Overall processing time of a database.
Metric Type	Counter
Dimensions	• Table • Method • status • compressionScheme
Example	• occnp_db_overall_processing_time_seconds_max{Method="put",Status="Success",Table="SmPolicyAssociation",application="pcf_smservice",compressionScheme="ZLIB_COMPRESSION_APPLICATION",} 0.314998

Table 9-64 audit_delete_records_max_ttl_count

Field	Details
Description	Indicates number of audit notifications sent by Audit service to SM service that are processed with MaxTTL as true (delete Rx Session, NO ASR).
Metric Type	Counter
Dimensions	• SvcType (SM Service, PA Service) • requestType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-65 audit_terminate_notify

Field	Details
Description	ASA response code metrics
Metric Type	Counter
Dimensions	• SvcType (PA Service) • request (TerminateNotify) • responseCode (2xx, 4xx, or 5xx)

Table 9-66 occnp_internal_delete_request_total

Field	Details
Description	Total number of internal delete request triggered on remote cleanup when forceDeleteOnError is true or forceDeleteOnExpiryOfWaitTimer is true.
Metric Type	Counter
Dimensions	• application • cause (waitforSMDeleteExpired or forceDeleteOnErrortoNotifySMF
Examples	• occnp_internal_delete_request_total{application="pcf_smservice",cause="waitforSMDeleteExpired",} 1.0 • occnp_internal_delete_request_total{application="pcf_smservice",cause="forceDeleteOnErrortoNotifySMF",} 1.0

Table 9-67 occnp_internal_delete_response_total

Field	Details
Description	Total number of internal delete response when forceDeleteOnError is true or forceDeleteOnExpiryOfWaitTimer is true.
Metric Type	Counter
Dimensions	• application • response_code
Examples	• occnp_internal_delete_response_total{application="pcf_smservice",response_code="204 NO_CONTENT",} 1.0 • occnp_internal_delete_response_total{application="pcf_smservice",response_code="404 NOT_FOUND",} 1.0

Table 9-68 occnp_error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-68 (Cont.) occnp_error_handler_in_total

Field	Details
Dimension	• application • application_exception • wrapped_exception
Example	• occnp_error_handler_in_total{application="pcf_smservice",application_exception="DiameterException",wrapped_exception="DiameterClientResponseException",} 1.0

Table 9-69 occnp_error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter
Dimension	• application • application_exception • error_type • operation • origin • rule_name • source_interface • target_interface • wrapped_exception
Example	• error_handler_exec_total{application="pcf_smservice",application_exception="DiameterException",error_type="INTERNAL",hostname="gi-frank-pcf-pcf-smservice-6496bc6d6d-n4v4p",operation="RAR",origin="DIAMETER",rule_name="TERMINATE_TRANSACTION",source_interface="RX",status="5010",target_interface="ANY",wrapped_exception="DiameterClientResponseException",} 1.0

Table 9-70 occnp_error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter
Dimension	• application • application_exception • error_resolved • hostname • wrapped_exception
Example	• occnp_error_handler_out_total{application="pcf_smservice",application_exception="DiameterException",error_resolved="false",hostname="rigelns2-pcf-smservice-d846c5cdb-ps5s9",wrapped_exception="DiameterClientResponseException",} 1.0

Table 9-71 occnp_pcf_smservice_overall_processing_time_seconds

Field	Details
Description	SM service overall processing time.
Type	Summary

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-71 (Cont.) occnp_pcf_smservice_overall_processing_time_seconds

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-72 occnp_pcf_smservice_overall_processing_time_seconds_max

Field	Details
Description	SM service overall processing time.
Type	Gauge
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Example	• occnp_pcf_smservice_overall_processing_time_seconds_max{application="pcf_smservice",error="none",exception="none",method="DELETE",outcome="SUCCESS",status="204",uri="/occnp-sm/v1/tdf-session/terminate",} 0.527015333

Table 9-73 occnp_pcf_smservice_overall_processing_time_seconds_count

Field	Details
Description	SM service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Example	• occnp_pcf_smservice_overall_processing_time_seconds_count{application="pcf_smservice",error="none",exception="none",method="DELETE",outcome="SUCCESS",status="204",uri="/occnp-sm/v1/tdf-session/terminate",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-74 occnp_pcf_smservice_overall_processing_time_seconds_sum

Field	Details
Description	SM service overall processing time.
Type	Gauge
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Example	• occnp_pcf_smservice_overall_processing_time_seconds_sum{application="pcf_smservice",error="none",exception="none",method="DELETE",outcome="SUCCESS",status="204",uri="/occnp-sm/v1/tdf-session/terminate",} 0.527015333

Table 9-75 update_notify_total

Field	Details
Description	This metrics is pegged for to show that there is no notification being sent when there is an AAR message with the flow status as REMOVED and the Message type as either AUDIO, MESSAGE, or OTHER.
Type	Counter
Dimension	• application • cause • hostname • optimized
Example	update_notify_total{application="pcf_smservice",cause="FLOW_STATUS_REMOVED",hostname="gmtommy-pcf-smservice-56cb4584df-clsfd",optimized="Yes",} 2.0

Table 9-76 collision_detection_local_delete

Field	Details
Description	Measures number of internal deletes due to duplicate session request.
Type	Counter
Dimension	• ServiceType • Request
Example	-

Table 9-77 collision_detection_terminate_notify

Field	Details
Description	Measures number of session terminate request sent due to duplicate session deletion.
Type	Counter
Dimension	• ServiceType • Request
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-78 audit_max_ttl_terminate_notify

Field	Details
Description	Measures number of session terminate request sent due to Stale Session Deletion Request
Type	Counter
Dimension	• ServiceType • Request
Example	-

Table 9-79 occnp_feature_info_received_total

Field	Details
Description	Measures sessRuleReports and policyDecFailureReports in request and response.
Type	Counter
Dimension	• application • hostname • servicename3gpp • operationType • responseCode • sessRuleReports • policyDecFailureReports
Example	occnp_feature_info_received_total{application="pcf_smservice",hostname="sky8-pcf-smservice-75df58b555-srm7q",operationType="update",policyDecFailureReports="true",responseCode="",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",} 2.0 occnp_feature_info_received_total{application="pcf_smservice",hostname="sky8-pcf-smservice-75df58b555-srm7q",operationType="update_notify",policyDecFailureReports="true",responseCode="200",servicename3gpp="npcf-smpolicycontrol",sessRuleReports="false",} 2.0

Table 9-80 error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter
Dimensions	• application • applicationException • wrapped_exception
Example	occnp_error_handler_in_total{application="pcf_smservice",application_exception="HttpException",status="404",wrapped_exception="NotFound",} 18.0

Table 9-81 error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-81 (Cont.) error_handler_exec_total

Field	Details
Dimensions	• application • applicationException • error_type • operation • origin • rule_name • source_interface • target_interface • wrapped_exception
Example	occnp_error_handler_exec_total{application="pcf_smservice",application_exception="JavaException",error_type="INTERNAL",operation="UPDATE",origin="JAVA",rule_name="REJECT_WITH_ENHANCED_DETAIL",source_interface="SMF",status="404",target_interface="POLICY",wrapped_exception="ServiceException",} 1.0

Table 9-82 error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter
Dimensions	• application • applicationException • error_resolved • wrapped_exception
Example	occnp_error_handler_out_total{application="pcf_smservice",application_exception="HttpException",error_resolved="false",status="423",wrapped_exception="HttpClientResponseException",} 4.0

Table 9-83 occnp_late_processing_rejection_total

Field	Details
Description	This metric is pegged when stale requests cleanup functionality is enabled and the late processing found that a session has become stale.
Type	Counter
Dimensions	• cause • servicename_3gpp • operation_type • stage
Example	occnp_late_processing_rejection_total': cause="timed_out_smf_request",servicename_3gpp="npcf-smpolicycontrol", stage="PRE_PDS" operation_type="create"

Table 9-84 ocpm_late_arrival_rejection_total

Field	Details
Description	This metric provides the number of requests rejected due to late arrival.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-84 (Cont.) ocpm_late_arrival_rejection_total

Field	Details
Dimensions	• cause • operation_type

Table 9-85 jvm_memory_committed_bytes

Field	Details
Description	The amount of memory in bytes that is committed for the Java virtual machine to use.
Type	Gauge
Dimensions	• application • area • hostname • id
Example	• jvm_memory_committed_bytes{application="pcf_smservice",area="nonheap",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="CodeHeap 'profiled nmethods'",} 4.096E7 • jvm_memory_committed_bytes{application="pcf_smservice",area="heap",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="G1 Survivor Space",} 1048576.0

Table 9-86 jvm_threads_daemon_threads

Field	Details
Description	The current number of live daemon threads.
Type	Gauge
Dimensions	• application • hostname
Example	jvm_threads_daemon_threads{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 14.0

Table 9-87 jvm_gc_pause_seconds_max

Field	Details
Description	Time spent in Garbage Collector (GC) pause.
Type	Gauge
Dimensions	• action • application • cause • gc • hostname
Example	jvm_gc_pause_seconds_max{action="end of minor GC",application="pcf_smservice",cause="G1 Evacuation Pause",gc="G1 Young Generation",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 0.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-88 jvm_buffer_count_buffers

Field	Details
Description	An estimate of the number of buffers in the pool.
Type	Gauge
Dimensions	• application • hostname • id
Example	• jvm_buffer_count_buffers{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="mapped - 'non-volatile memory'",} 0.0 • jvm_buffer_count_buffers{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="direct",} 87.0 • jvm_buffer_count_buffers{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="mapped",} 0.0

Table 9-89 jetty_client_request_size_max

Field	Details
Description	Content sizes for Jetty HTTP client requests.
Type	Gauge
Dimensions	• application • exception • hostname • method • outcome • status • uri
Example	• jetty_client_request_size_max{application="pcf_smservice",exception="None",host="10.233.76.11",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="POST",outcome="SERVER_ERROR",status="500",uri="",} 0.0 • jetty_client_request_size_max{application="pcf_smservice",exception="None",host="10.233.90.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="DELETE",outcome="SUCCESS",status="204",uri="",} 0.0 • jetty_client_request_size_max{application="pcf_smservice",exception="None",host="10.233.76.11",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="POST",outcome="SUCCESS",status="200",uri="",} 0.0 • jetty_client_request_size_max{application="pcf_smservice",exception="None",host="10.233.90.30",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="POST",outcome="SERVER_ERROR",status="503",uri="",} 0.0 • jetty_client_request_size_max{application="pcf_smservice",exception="None",host="10.233.109.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="GET",outcome="SUCCESS",status="204",uri="",} 0.0

Table 9-90 jetty_client_request_size_sum

Field	Details
Description	Content sizes for Jetty HTTP client requests.
Type	Summary

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-90 (Cont.) jetty_client_request_size_sum

Field	Details
Dimensions	• application • exception • host • hostname • method • outcome • status • uri
Example	• jetty_client_request_size_sum{application="pcf_smservice",exception="None",host="10.233.76.11",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="POST",outcome="SERVER_ERROR",status="500",uri="",} 0.0 • jetty_client_request_size_count{application="pcf_smservice",exception="None",host="10.233.90.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="DELETE",outcome="SUCCESS",status="204",uri="",} 32.0 • jetty_client_request_size_sum{application="pcf_smservice",exception="None",host="10.233.109.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="GET",outcome="SUCCESS",status="204",uri="",} 0.0 • jetty_client_request_size_sum{application="pcf_smservice",exception="None",host="10.233.109.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="GET",outcome="CLIENT_ERROR",status="400",uri="",} 0.0

Table 9-91 jetty_client_request_size_count

Field	Details
Description	Content sizes for Jetty HTTP client requests.
Type	Summary
Dimensions	• application • exception • host • hostname • method • outcome • status • uri
Example	• jetty_client_request_size_count{application="pcf_smservice",exception="None",host="10.233.76.11",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="POST",outcome="SERVER_ERROR",status="500",uri="",} 4.0 • jetty_client_request_size_count{application="pcf_smservice",exception="None",host="10.233.90.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="DELETE",outcome="SUCCESS",status="204",uri="",} 32.0 • jetty_client_request_size_count{application="pcf_smservice",exception="None",host="10.233.109.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="GET",outcome="SUCCESS",status="204",uri="",} 25.0 • jetty_client_request_size_count{application="pcf_smservice",exception="None",host="10.233.109.51",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="GET",outcome="CLIENT_ERROR",status="400",uri="",} 2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-92 jvm_buffer_total_capacity_bytes

Field	Details
Description	An estimate of the total capacity of the buffers in this pool.
Type	Gauge
Dimensions	• application • hostname • id
Example	• jvm_buffer_total_capacity_bytes{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="mapped - 'non-volatile memory'",} 0.0 • jvm_buffer_total_capacity_bytes{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="direct",} 751288.0 • jvm_buffer_total_capacity_bytes{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",id="mapped",} 0.0

Table 9-93 executor_seconds_max

Field	Details
Description	Maximum executors in seconds.
Type	Gauge
Dimensions	• application • hostname • name • reactor_scheduler_id
Example	• executor_seconds_max{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",name="parallel(2,\"parallel\")-0",reactor_scheduler_id="parallel(2,\"parallel\")",} 0.0 • executor_seconds_max{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",name="parallel(2,\"parallel\")-1",reactor_scheduler_id="parallel(2,\"parallel\")",} 0.0

Table 9-94 hikaricp_connections_usage_seconds_count

Field	Details
Description	Connection usage time
Type	Summary
Dimensions	• application • hostname • pool
Example	hikaricp_connections_usage_seconds_count{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",pool="HikariPool-1",} 763.0

Table 9-95 hikaricp_connections_usage_seconds_sum

Field	Details
Description	Connection usage time

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-95 (Cont.) hikaricp_connections_usage_seconds_sum

Field	Details
Type	Summary
Dimensions	• application • hostname • pool
Example	hikaricp_connections_usage_seconds_sum{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",pool="HikariPool-1",} 4.867

Table 9-96 hikaricp_connections_usage_seconds_max

Field	Details
Description	Connection usage time
Type	Gauge
Dimensions	• application • hostname • pool
Example	hikaricp_connections_usage_seconds_max{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",pool="HikariPool-1",} 0.0

Table 9-97 http_server_requests_active_seconds_active_count

Field	Details
Description	Active Server requests
Type	Counter
Dimensions	• application • exception • hostname • method • outcome • status • uri
Example	• http_server_requests_active_seconds_active_count{application="pcf_smservice",exception="none",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="GET",outcome="SUCCESS",status="200",uri="UNKNOWN",} 0.0 • http_server_requests_active_seconds_active_count{application="pcf_smservice",exception="none",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="POST",outcome="SUCCESS",status="200",uri="UNKNOWN",} 0.0

Table 9-98 http_server_requests_active_seconds_duration_sum

Field	Details
Description	Active Server requests
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-98 (Cont.) http_server_requests_active_seconds_duration_sum

Field	Details
Dimensions	• application • exception • hostname • method • outcome • status • uri
Example	• http_server_requests_active_seconds_duration_sum{application="pcf_smservice",exception="none",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="GET",outcome="SUCCESS",status="200",uri="UNKNOWN",} 0.0 • http_server_requests_active_seconds_duration_sum{application="pcf_smservice",exception="none",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",method="POST",outcome="SUCCESS",status="200",uri="UNKNOWN",} 0.0

Table 9-99 system_cpu_count

Field	Details
Description	The number of processors available to the Java virtual machine
Type	Gauge
Dimensions	• application • hostname
Example	system_cpu_count{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 2.0

Table 9-100 db_operations_total

Field	Details
Description	Total database operations
Type	Counter
Dimensions	• Operation • application • hostname
Example	• db_operations_total{Operation="Create",application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 0.0 • db_operations_total{Operation="Put",application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 363.0 • db_operations_total{Operation="Delete",application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 32.0 • db_operations_total{Operation="Get",application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 358.0

Table 9-101 process_cpu_usage

Field	Details
Description	The "recent cpu usage" for the Java Virtual Machine process.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-101 (Cont.) process_cpu_usage

Field	Details
Type	Gauge
Dimensions	• application • hostname
Example	process_cpu_usage{application="pcf_smservice",hostname="occnp-pcf-smservice-7d6c7bdcb8-zhxsh",} 0.0

Table 9-102 occnp_suppress_notify_total

Field	Details
Description	To measure the number of ASR not sent, ASR sent, and RAR sent when the feature is enabled.
Type	Counter
Dimensions	• Action • OperationType • SuppressionCause • ErrorCode • MsgType • ExceptionType
Example	occnp_suppress_notify_total{Action="deliver",ErrorCode="",ExceptionType="",MsgType="MSGTYPE_CREATE",SuppressionCause="ExceptionMismatch",application="pcf_smservice",hostname="titans-pcf-smservice-c7bc54fc7-xckwn",operationType="terminateNotify",} 1.0

Table 9-103 ocpm_handle_update_notify_timeout_as_pending_confirmation_total

Field	Details
Description	This metric is incremented when SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED flag is enabled enable and the response from SMF to PCF times out during update notify triggered by AAR-I and AAR-U.
Type	Counter
Dimensions	• OperationType Possible value: `update_notify` • Cause Possible value: `Update Notify Time Out handled as PendingConfirmation` • application • hostname • servicename3gpp
Example	{"instant":{"epochSecond":1742514782,"nanoOfSecond":805725000},"thread":"boundedElastic-1","level":"DEBUG","loggerName":"ocpm.pcf.service.sm.domain.component.metrics.SmMetrics","message":"Pegging Handle Update Notify timeout as Success metric, Operation Type: update_notify, Cause: Update Notify Time Out handled as PendingConfirmation","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","threadId":77,"threadPriority":5,"messageTimestamp":"2025-03-20T17:53:02.805-0600","ocLogId":"${ctx:ocLogId}"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-104 ocpm_handle_update_notify_error_response_as_pending_confirmation_total

Field	Details
Description	This is incremented when configuration flag `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED` is enabled and specific error is added in `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPOMNSE_CODE` and configured response code received during update notify triggered by AAR-I and AAR-U.
Type	Counter
Dimensions	• OperationType Possible value: `update_notify` • Cause Possible value: `Update Notify Error Response handled as Pending Confirmation` • responseCode Possible value: Update Notify error code • application • hostname • servicename3gpp
Example	ocpm_handle_update_notify_error_response_as_pending_confirmation_total{application="pcf_smservice",cause="Update Notify Error Response handled as Pending Confirmation",hostname="my-cnpolicy-pcf-smservice-7f7bcdb89-hhjbr",operationType="update_notify",responseCode="408",servicename3gpp="nf1stub.ch2-ns04.svc",} 4.0

Table 9-105 ocpm_process_pending_confirmation_rules_on_pa_update_total

Field	Details
Description	This metric is incremented when rules as processed during PA update based on `pendingConfirmationAction` and flag `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.PROCESS_ON_UPDATE` is enabled.
Type	Counter
Dimensions	• OperationType Possible value: `update_notify` • Cause Possible value: `Pending Confirmation rules processed on Pa Update` • responseCode Possible value: Update Notify error code • application • hostname • servicename3gpp
Example	ocpm_process_pending_confirmation_rules_on_pa_update_total{application="pcf_smservice",cause="Pending Confirmation rules processed on Pa Update",hostname="my-cnpolicy-pcf-smservice-7f7bcdb89-hhjbr",operationType="update_notify",servicename3gpp="nf1stub.ch2-ns04.svc",} 8.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-106 ocpm_process_pending_configuration_rules_on_pa_delete_total

Field	Details
Description	This metric is incremented when a rule with `pendingConfirmation` flag as `true` and `pendingConfirmation` rules are sent in update notify triggered by STR.
Type	Counter
Dimensions	• OperationType Possible value: `update_notify` • Cause Possible value: `Pending Confirmation rules sent to delete on Pa Delete` • application • hostname • servicename3gpp
Example	ocpm_process_pending_configuration_rules_on_pa_delete_total{application="pcf_smservice",cause="Pending Confirmation rules sent to delete on Pa Delete",hostname="my-cnpolicy-pcf-smservice-7f7bcdb89-hhjbr",operationType="update_notify",servicename3gpp="nf1stub.ch2-ns04.svc",} 16.0

Table 9-107 ocpm_rx_update_notify_request_total

Field	Details
Description	This metric is incremented only if the update notify request is triggered by Rx and request is AAR-I or AAR-U.
Type	Counter
Dimensions	• OperationType Possible value: `update_notify` • Cause Possible value: `Update Notify request triggered by Rx` • application • hostname • servicename3gpp
Example	ocpm_rx_update_notify_request_total{application="pcf_smservice",cause="Update Notify request triggered by Rx",hostname="my-cnpolicy-pcf-smservice-7f7bcdb89-hhjbr",operationType="update_notify",servicename3gpp="nf12stub.ch2-ns04.svc",} 24.0

Table 9-108 occnp_pds_location_info_notification_total

Field	Details
Description	This metric gets incremented when SM core service gets notification from PDS to update PDS Location info in case of concurrency.
Type	Counter
Dimensions	• application • hostname • operation_type • response_code • session_type

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-108 (Cont.) occnp_pds_location_info_notification_total

Field	Details
Example	• occnp_pds_location_info_notification_total{application="pcf_smservice",hostname="pcf-pcf-smservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="5xx",session_type="sm_session",} 1.0 • occnp_pds_location_info_notification_total{application="pcf_smservice",hostname="pcf-pcf-smservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="2xx",session_type="sm_session",} 1.0 • occnp_pds_location_info_notification_total{application="pcf_smservice",hostname="pcf-pcf-smservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="4xx",session_type="sm_session",} 1.0

Table 9-109 occnp_optimized_smpolicyAssociation_lookup_query_total

Field	Details
Description	This metric is incremented only when `ENABLE_N7_SESSION_LOOKUP_COOKIE` advanced settings key is enabled at SM service and Policy receives AAR-I with custom AVP.
Type	Counter
Dimensions	• MsgType Possible value: PA Create • status Possible values: – Success – Failed • cause Possible values: – If the value of `status` is `Success`, value of `cause` is `NA`. – If the value of `status` is `Failed`, value of `cause` can be one of the following: * IPV4 mismatch * IPD mismatch * IPV6 mismatch * DNN mismatch * SUPI mismatch * MAC mismatch (Not Applicable for RX call flows) * SNSSAI mismatch (Not Applicable for RX call flows) * Session Not Found • application
Examples	occnp_optimized_smpolicyAssociation_lookup_query_total{MsgType="PA create",application="occnp",cause="IPV4 mismatch",status="failed",} 1.0 occnp_optimized_smpolicyAssociation_lookup_query_total{MsgType="PA create",application="occnp",cause="NA",status="success",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-110 jvm_gc_overhead

Field	Details
Description	An approximation of the percent of CPU time used by GC activities over the last lookback period or since monitoring began, whichever is shorter, in the range [0..1].
Type	Gauge
Dimensions	• application
Example	-

Table 9-111 jvm_memory_usage_after_gc

Field	Details
Description	The percentage of long-lived heap pool used after the last GC event, in the range [0..1].
Type	Gauge
Dimensions	• application • hostname • area • pool
Example	jvm_memory_usage_after_gc{application="occnp",area="heap",pool="long-lived",

Table 9-112 occnp_usr_loc_ch_supp_feat_in_sm_create_req_total

Field	Details
Description	This metric provides the number of SM Policy Create requests received from SMF with `AggregatedUELocChanges` enabled. **Note**: Invalid requests are rejected at the controller level and excluded from this count. This metric is incremented when a given SM request (CREATE) contains `suppFeat=(020000000000)` corresponding to `AggregatedUELocChanges`.
Type	Counter
Dimensions	• operationType • cause • application • hostname • servicename3gpp
Example	occnp_usr_loc_ch_supp_feat_in_sm_create_req_total{application="pcf_smservice",cause="AggregatedUELocChanges",hostname="my-cnpolicy-pcf-smservice-79f9d6f89c-k7cmh",operationType="create",servicename3gpp=""} 8.0

Table 9-113 usr_loc_ch_sent_in_response

Field	Details
Description	This metric provides the number of SM Policy Create or Update responses sent by PCF with `USER_LOCATION_CH` event. This metric is incremented when the feature `AggregatedUELocChanges` is enabled for this `SmPolicyAssociation` and event `USER_LOCATION_CH` is sent to SMF for SM Create and SM Update response.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-113 (Cont.) usr_loc_ch_sent_in_response

Field	Details
Type	Counter
Dimensions	• OperationType: update • Cause: USER_LOCATION_CH • application • hostname • servicename3gpp
Example	occnp_usr_loc_ch_in_update_notify_total{application="pcf_smservice",cause="USER_LOCATION_CH",hostname="my-cnpolicy-pcf-smservice-79f9d6f89c-k7cmh",operationType="update_notify",servicename3gpp=""} 14.0 occnp_usr_loc_ch_sent_in_response_total{application="pcf_smservice",cause="USER_LOCATION_CH",hostname="my-cnpolicy-pcf-smservice-79f9d6f89c-k7cmh",operationType="create",servicename3gpp=""} 3.0 occnp_usr_loc_ch_sent_in_response_total{application="pcf_smservice",cause="USER_LOCATION_CH",hostname="my-cnpolicy-pcf-smservice-79f9d6f89c-k7cmh",operationType="update",servicename3gpp=""} 1.0

Table 9-114 usr_loc_ch_in_update_notify

Field	Details
Description	This metric provides the number of SM Policy Update Notify requests sent by PCF with `USER_LOCATION_CH` event. This metric is incremented when the feature `AggregatedUELocChanges` is enabled for this `SmPolicyAssociation` and event `USER_LOCATION_CH` is sent to SMF in update_notify.
Type	Counter
Dimensions	• OperationType: update_notify • Cause: USER_LOCATION_CH • application • hostname • servicename3gpp
Example	occnp_usr_loc_ch_in_update_notify_total{application="pcf_smservice",cause="USER_LOCATION_CH",hostname="my-cnpolicy-pcf-smservice-79f9d6f89c-k7cmh",operationType="update_notify",servicename3gpp=""} 14.0

Table 9-115 usr_loc_ch_in_sm_update

Field	Details
Description	This metric provides the number of SM Policy Update requests received from SMF with `USER_LOCATION_CH` event. This metric is incremented when the feature `AggregatedUELocChanges` is enabled for this `SmPolicyAssociation` and `USER_LOCATION_CH` is received in SM Update request from SMF.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-115 (Cont.) usr_loc_ch_in_sm_update

Field	Details
Dimensions	• OperationType: update • Cause: USER_LOCATION_CH • application • hostname • servicename3gpp
Example	occnp_usr_loc_ch_in_sm_update_total{application="pcf_smservice",cause="USER_LOCATION_CH",hostname="my-cnpolicy-pcf-smservice-79f9d6f89c-k7cmh",operationType="update",servicename3gpp=""} 2.0

Table 9-116 occnp_enhanced_overload_reject_total

Field	Details
Description	This metric is used to track reject action in SM Service for N7, Diameter Rx and BSF Audit Notify Requests. This is a counter metric which will be pegged when incoming request will be discarded by Overload Load Filter within pcf-sm service. **Note**: In case of `Npcf_SMPolicyControl` and `Diamter_Rx` interface type for Update and Delete request, DNN, SNSSAI, and ServiceURN dimensions in the metric are optional. These dimensions are populated only if DNN, S-NSSAI, or Service Urn based filtering is configured, corresponding DNN, S-NSSAI, Service URN Message Attributes are configured in GUI and matched message attribute encoded in `associationID` during create request is present.
Type	Counter
Dimensions	• Overload Level • InterfaceType (such as Npcf_SMPolicyControl, Diameter_Rx, Other) • operationType • dnn • snssai • serviceUrn
Example	occnp_enhanced_overload_reject_total{application="pcf_smservice",dnn="internet",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",interfaceType="Npcf_SMPolicyControl",loadLevel="1",operationType="Create",serviceUrn="",snssai="1-000007"} 20786.0

Table 9-117 occnp_service_load_level

Field	Details
Description	This metric is used to track Load level changes with in SM Service. This metric may not be changed for each polling response, If response is from non-leader pod and will be dependent on nonLeaderPodSampleCount.
Type	Gauge
Dimensions	• application • hostname
Example	occnp_service_load_level{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg"} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-118 occnp_load_level_polling_request_total

Field	Details
Description	This metric is used to track load level requests. It provides the count of requests sent to perf-info.
Type	Counter
Dimensions	• application • hostname
Example	occnp_load_level_polling_request_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg"} 264238.0

Table 9-119 occnp_load_level_polling_response_total

Field	Details
Description	This metric is used to track load level responses. It provides the count of responses received from perf-info.
Type	Counter
Dimensions	• application • hostname • responseCode
Example	occnp_load_level_polling_response_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",responseCode="200"} 48822.0 occnp_load_level_polling_response_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",responseCode="500"} 97746.0 occnp_load_level_polling_response_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",responseCode="503"} 117670.0

Table 9-120 occnp_load_level_polling_exception_total

Field	Details
Description	This metric is used to track load level polling exceptions. It provides the count of exceptions (e.g. TimeoutException) occurred while sending request.
Type	Counter
Dimensions	• application • hostname
Example	occnp_load_level_polling_exception_total{application="pcf_smservice",hostname="pcf-pcf-smservice-69c7578d6-vrmfb"} 96.0

Table 9-121 occnp_polled_load_level_total

Field	Details
Description	This metric is used to track polled load level. This metric pegged in case of success response with all the details of the response like isLeader, loadLevel, serviceName.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-121 (Cont.) occnp_polled_load_level_total

Field	Details
Dimensions	• application • hostname • isLeader • loadLevel • serviceName
Example	occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="false",loadLevel="L0",serviceName="pcf-occnp-pcf-sm"} 9501.0 occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="false",loadLevel="L1",serviceName="pcf-occnp-pcf-sm"} 6534.0 occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="false",loadLevel="L2",serviceName="pcf-occnp-pcf-sm"} 1565.0 occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="false",loadLevel="L3",serviceName="pcf-occnp-pcf-sm"} 6796.0 occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="true",loadLevel="L0",serviceName="pcf-occnp-pcf-sm"} 9554.0 occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="true",loadLevel="L1",serviceName="pcf-occnp-pcf-sm"} 6510.0 occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="true",loadLevel="L2",serviceName="pcf-occnp-pcf-sm"} 1551.0 occnp_polled_load_level_total{application="pcf_smservice",hostname="pcf-pcf-smservice-787c59b54f-qw7xg",isLeader="true",loadLevel="L3",serviceName="pcf-occnp-pcf-sm"} 6811.0

Table 9-122 occnp_pending_binding_site_takeover

Field	Details
Description	This metric provides the current count of pending site takeover operations.
Type	Gauge
Dimensions	• application • hostname
Example	occnp_pending_binding_site_takeover_total{application="pcf_smservice",hostname="pcf-pcf-smservice-7fdd6f6797-c4pzd",} 1.0

Table 9-123 occnp_enhanced_overload_ssv_update_skipped_total

Field	Details
Description	This is a counter metric which is pegged when SSV UPDATE operation to PDS is skipped due to applicable Enhanced overload assume positive restriction on User data.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-123 (Cont.) occnp_enhanced_overload_ssv_update_skipped_total

Field	Details
Dimensions	• interfaceType • operationType • dnn • snssai
Example	{interfaceType="Npcf_SMPolicyControl",operationType="Create" ,dnn="dnn1",snssai="11-abc123"}

Table 9-124 occnp_enhanced_overload_service_interaction_total

Field	Details
Description	This metric increments once for each incoming request when an SM-related request is subjected to an Assume Positive restriction by the Overload Load Filter within the pcf-sm service.
Type	Counter
Dimensions	• interfaceType • operationType • loadLevel • dnn • snssai • userData • spendingLimitData • policyEvaluation Service interaction dimensions mentioned above is an indication of the restriction configured in the mapped overload rule. A value of ‘false’ ensures that no interaction was performed with the respective service (UserData, SpendingLimit, or PolicyEvaluation), while a value of ‘true’ indicates that no restriction was applied due to overload handling. However, a value of ‘true’ does not guarantee that an interaction actually occurred, as other processes or features besides Enhanced Overload may have blocked the interaction. One of the example feature is the 'Exclude DNN' feature which can stop User Data interaction for a particular DNN.
Example	{interfaceType="Npcf_SMPolicyControl",operationType="Create" ,loadLevel="1",dnn="dnn1",snssai="11-abc123",userData=true,spendingLimitData=false,policyEvaluation=true}

Table 9-125 occnp_sm_qosmon_update_notify_sent_total

Field	Description
Description	This metric is incremented when PCF sends an updateNotify request to SMF with QoS Monitoring subscription.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-125 (Cont.) occnp_sm_qosmon_update_notify_sent_total

Field	Description
Dimensions	• **repFreq:** Reporting frequency requested for QOS_MONITORING in updateNotify operation (PERIODIC, EVENT_TRIGGERED or PERIODIC_AND_EVENT_DETECTION) • **notifTarget:** The target NF instructed to SMF to send the packet delay notifications (AF_NEF) • **operation_type:** Create or delete operation that triggered the update_notify
Examples	occnp_sm_qosmon_update_notify_sent_total(repFreq="EVENT_TRIGGERED", notifTarget="AF_NEF")

Table 9-126 occnp_sm_qosmon_decs_error_total

Field	Description
Description	This metric is incremented when PCF receives QOS_MON_DECS_ERR as PolicyDecisionFailureCode to the updateNotify requests or when PCF receives a Npcf_SMPolicyControl_Update requests received from SMF with QOS_MON_DECS_ERR as PolicyDecisionFailureCode for Policy decision failures
Metric Type	Counter
Dimensions	• **policyDecsFailureCode:** The error code received (QOS_MON_DECS_ERR) • **operation_type:** The operation involved in this interaction (update, update_notify) • **response_code**: Code received from SMF on updateNotify (400 or 200). Empty for SM Update operation.
Examples	occnp_sm_qosmon_decs_error_total{application="pcf_smservice",hostname="my-cnpolicy-pcf-smservice-858595cbdc-t8vgx",operation_type="update",policyDecsFailureCode="QOS_MON_DECS_ERR",response_code=""} 1.0 occnp_sm_qosmon_decs_error_total{application="pcf_smservice",hostname="my-cnpolicy-pcf-smservice-858595cbdc-t8vgx",operation_type="update_notify",policyDecsFailureCode="QOS_MON_DECS_ERR",response_code="200"} 1.0

For more information about Dimensions, see CNC Policy Metrics.

9.6 AM Service Metrics

The following table describes the AM Service metrics and respective dimensions:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-127 ocpm_ingress_request_total

Field	Details
Description	Total number of ingress requests received.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • sbi_priority • service name_ 3gpp
Example	: 1. ocpm_ingress_request_total{operation_type="create",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter 2. ocpm_ingress_request_total{operation_type="get",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter

Table 9-128 ocpm_ingress_response_total

Field	Details
Description	Total number of ingress responses.
Metric Type	Counter
Dimensions	• Cause • operation_type • nf_instance_id • sbi_priority • servicename_3gpp • response_code
Example	• ocpm_ingress_response_total{operation_type="create",response_code="2xx",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter • ocpm_ingress_response_total{operation_type="get",response_code="2xx",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter

Table 9-129 ocpm_egress_request_total

Field	Details
Description	Total number of egress requests received.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • sbi_priority • servicename_3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-129 (Cont.) ocpm_egress_request_total

Field	Details
Example	• ocpm_egress_request_total{operation_type="update_notify",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter • ocpm_egress_request_total{operation_type="terminate_notify",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter

Table 9-130 ocpm_egress_response_total

Field	Details
Description	Total number of egress responses.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • sbi_priority • servicename_3gpp • response_code • latency
Example	• ocpm_egress_response_total{operation_type="terminate_notify",response_code="2xx",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter • ocpm_egress_response_total{operation_type="update_notify",response_code="2xx",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter

Table 9-131 am_audit_update_notify_sent_total

Field	Details
Description	Total number of audit notifications sent.
Metric Type	Counter
Dimensions	Request
Example	• am_audit_update_notify_sent_total{} 1.0 ; Type-Counter

Table 9-132 am_audit_update_notify_session_not_found_total

Field	Details
Description	Total number of 'session not found' notifications.
Metric Type	Counter
Dimensions	Request
Example	• am_audit_update_notify_session_not_found_total{} 1.0 ; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-133 am_audit_update_notify_session_found_total

Field	Details
Description	Total number of 'session found' notifications.
Metric Type	Counter
Dimensions	Request
Example	• am_audit_update_notify_session_found_total{ } 1.0 ; Type-Counter

Table 9-134 am_audit_update_timestamp_cnt_total

Field	Details
Description	Total number of timestamp count for audit requests.
Metric Type	Counter
Dimensions	Request
Example	• am_audit_update_timestamp_cnt_total{} 1.0 ; Type-Counter

Table 9-135 am_audit_delete_records_count_total

Field	Details
Description	Total number of delete audit records requests
Metric Type	Counter
Dimensions	Request
Example	• am_audit_delete_records_count_total{notification="true",} 1.0 ; Type-Counter • am_audit_delete_records_count_total{notification="false",} 1.0 ; Type-Counter

Table 9-136 am_audit_delete_records_max_ttl_count_total

Field	Details
Description	Number of records deleted by AM service when the max TTL was reached.
Metric Type	Counter
Dimensions	Request
Example	• am_audit_delete_records_max_ttl_count_total{} 1.0 ; Type-Counter

Table 9-137 am_audit_amf_query_total

Field	Details
Description	-
Metric Type	Counter
Dimensions	Request

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-137 (Cont.) am_audit_amf_query_total

Field	Details
Example	• am_audit_amf_query_total{} 1.0 ; Type-Counter

Table 9-138 am_audit_update_notify_response_error_total

Field	Details
Description	Number of update notify requests sent to AMF by AM service that were responded with an error code.
Metric Type	Counter
Dimensions	Request
Example	• am_audit_update_notify_response_error_total{} 1.0 ; Type-Counter

Table 9-139 session_oam_request_total

Field	Details
Description	Number of session requests for AM Service
Metric Type	Request
Dimensions	• Response Code • Operation Type • Session Type

Table 9-140 session_oam_response_total

Field	Details
Description	Number of session responses for AM Service
Metric Type	Response
Dimensions	• Response Code • Operation Type • Session Type

Table 9-141 session_info_request_total

Field	Details
Description	Total number of sessions to be deleted as requested by the AM Service
Metric Type	Counter
Dimensions	• Application • Cause • Operation Type • Session Type

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-141 (Cont.) session_info_request_total

Field	Details
Example	• session_info_request_total{application="pcf_amservice",cause="local_limiting_session",operation_type="cleanup",session_type="am_session",} 3.0

Table 9-142 occnp_lease_duration_seconds_bucket

Field	Details
Description	Time in seconds for which AM Service holds the lock
Metric Type	Histogram
Dimensions	• Lock_Lease_Duration • Message_Type • application • quartile

Table 9-143 session_info_response_total

Field	Details
Description	Total number of sessions deleted as requested by the AM Service
Metric Type	Counter
Dimensions	• Application • Cause • Operation Type • Response Code • Session Type
Example	• session_info_response_total{application="pcf_amservice",cause="local_limiting_session",operation_type="cleanup",response_code="5xx",session_type="am_session",} 2.0

Table 9-144 http_out_conn_request_total

Field	Details
Description	Total number of connection requests received
Metric Type	Counter
Dimensions	• Application • bindingId • bindingLevel • discoveryId • discoveryParameter • hostname • operationType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-144 (Cont.) http_out_conn_request_total

Field	Details
Example	• http_out_conn_request_total{application="pcf_amservice",bindingId="",bindingLevel="",discoveryId="set001.region01.amfset.5gc.mnc012.mcc345",discoveryParameter="target-nf-set-id",hostname="my-cnpolicy-pcf-amservice-6c54cd7d4d-kp295",operationType="get",servicename3gpp="npcf-am-policy-control",} 2.0

Table 9-145 http_out_conn_response_total

Field	Details
Description	Total number of connection response sent
Metric Type	Counter
Dimensions	• Application • hostname • operationType • responseCode
Example	• http_out_conn_response_total{application="pcf_amservice",hostname="my-cnpolicy-pcf-amservice-6c54cd7d4d-kp295",operationType="update_notify",responseCode="5xx",servicename3gpp="npcf-am-policy-control",} 2.0

Table 9-146 ocpm_ar_request_total

Field	Details
Description	Total number of ar requests received
Metric Type	Counter
Dimensions	• Application • fqdn • hostname • scheme • servicename3gpp
Example	• ocpm_ar_request_total{application="pcf_amservice",fqdn="nf12stub.harald-ns.svc",hostname="my-cnpolicy-pcf-amservice-6c54cd7d4d-kp295",scheme="http",servicename3gpp="npcf-am-policy-control",} 1.0 • ocpm_ar_request_total{application="pcf_amservice",fqdn="nf12stub.harald-ns.svc",hostname="my-cnpolicy-pcf-amservice-6c54cd7d4d-kp295",scheme="http",servicename3gpp="npcf-am-policy-control",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-147 ocpm_ar_response_total

Field	Details
Description	Total number of ar response sent
Metric Type	Counter
Dimensions	• Application • fqdn • hostname • scheme • servicename3gpp

Table 9-148 occnp_http_in_conn_response_total

Field	Details
Description	Number of http responses for AM Service
Metric Type	Counter
Dimensions	• application • bindingId • bindingLevel • hostname • nfInstanceId • operationType • responseCode • priority • servicename3gpp
Example	• **occnp_http_in_conn_response_total**{application="pcf_amservice",bindingId="",bindingLevel="",dnn="dnn1",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",nfInstanceId="", ,operationType="update",responseCode="400",priority="",servicename3gpp="npcf-amservice",snssai="11-abc123",***cause="PENDING_TRANSACTION"***

Table 9-149 http_bulwark_lock_request_total

Field	Details
Description	Number of bulwark lock requests
Metric Type	Counter
Dimensions	• application • hostname • operationType • servicenameNon3gpp
Example	• **http_bulwark_lock_request_total**{application="pcf_amservice",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",operationType="**bulwark_lock**",servicenameNon3gpp="npcf-amservice"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-150 http_bulwark_unlock_request_total

Field	Details
Description	Number of bulwark unlock requests
Metric Type	Counter
Dimensions	• application • hostname • operationType • servicenameNon3gpp
Example	• **http_bulwark_unlock_request_total**{application="pcf_amservice",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",operationType="**bulwark_unlock**",servicenameNon3gpp="npcf-amservice"}

Table 9-151 http_bulwark_lock_response_total

Field	Details
Description	Number of bulwark lock responses
Metric Type	Counter
Dimensions	• application • hostname • operationType • servicenameNon3gpp
Example	• **http_bulwark_lock_response_total**{application="pcf_amservice",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",operationType="**bulwark_lock**",responseCode="201",servicenameNon3gpp="npcf-smpolicycontrol"}

Table 9-152 http_bulwark_lock_request_retry_total

Field	Details
Description	Number of bulwark lock request retries
Metric Type	Counter
Dimensions	• application • hostname • operationType • servicenameNon3gpp
Example	• **http_bulwark_lock_request_retry_total**{application="pcf_amservice",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",operationType="**bulwark_lock**",responseCode="204",servicenameNon3gpp="npcf-amservice"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-153 http_bulwark_unlock_request_retry_total

Field	Details
Description	Number of bulwark unlock request retries
Metric Type	Counter
Dimensions	• application • hostname • operationType • servicenameNon3gpp
Example	• **http_bulwark_unlock_request_retry_total**{application="pcf_amservice",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",operationType="**bulwark_unlock**",responseCode="204",servicenameNon3gpp="npcf-amservice"}

Table 9-154 occnp_http_out_conn_request_total

Field	Details
Description	Number of http requestd for AM Service
Metric Type	Counter
Dimensions	• application • bindingId • bindingLevel • hostname • nfInstanceId • operationType • responseCode • priority • servicename3gpp
Example	• **occnp_http_out_conn_request_total**{application="pcf_amservice",bindingId="",bindingLevel="",dnn="dnn1",hostname="jiandong-pcf-smservice-5878554dc7-wgvc7",nfInstanceId="",nfName="",operationType="update_notify",priority="",servicename3gpp="npcf-amservice",snssai="",***retry="Yes"***}

Table 9-155 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Metric Type	Gauge
Dimensions	• Service Name • Pod Name

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-156 occnp_db_overall_processing_time_seconds_count

Field	Details
Description	This metric is incremented when PCF performs GET, INSERT, UPDATE, and DELETE operation on an Association
Metric Type	Counter
Dimensions	• Method • Status • Table
Example	• occnp_db_overall_processing_time_seconds_count{Method="delete", Status="Success", Table="UePolicyAssociation", container="ue-service"}

Table 9-157 occnp_db_overall_processing_time_seconds_sum

Field	Details
Description	This metric is incremented when PCF performs DELETE operation on an Association
Metric Type	Counter
Dimensions	• Method • Status • Table
Example	• occnp_db_overall_processing_time_seconds_sum{Method="delete", Status="Success", Table="UePolicyAssociation", container="ue-service"}

Table 9-158 occnp_db_overall_processing_time_seconds_sum

Field	Details
Description	This metric is incremented when PCF performs DELETE operation on an Association
Metric Type	Counter
Dimensions	• Method • Status • Table
Example	• occnp_db_overall_processing_time_seconds_sum{Method="delete", Status="Success", Table="UePolicyAssociation", container="ue-service"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-159 occnp_amservice_overall_processing_time_seconds_max

Field	Details
Description	This metric is incremented for AM service to calculate processing's duration of HTTP request arrived on rest controller. **Note**: occnp_amservice_overall_processing_time_seconds_max metric replaces http_server_requests_seconds_max.
Metric Type	Counter
Dimensions	• Method • Status • uri • container
Example	• occnp_amservice_overall_processing_time_seconds_max{method="DELETE", status="204", uri="/npcf-am-policy-control/v1/policies/{polAssoId}", container="am-service"}

Table 9-160 occnp_amservice_overall_processing_time_seconds_sum

Field	Details
Description	This metric is incremented for AM service to calculate processing's duration of HTTP request arrived on rest controller. **Note**: occnp_amservice_overall_processing_time_seconds_sum metric replaces http_server_requests_seconds_sum.
Metric Type	Counter
Dimensions	• Method • Status • uri • container
Example	• occnp_amservice_overall_processing_time_seconds_max{method="DELETE", status="204", uri="/npcf-am-policy-control/v1/policies/{polAssoId}", container="am-service"}

Table 9-161 occnp_amervice_overall_processing_time_seconds_count

Field	Details
Description	This metric is incremented for AM service to calculate processing's duration of HTTP request arrived on rest controller. **Note**: occnp_amservice_overall_processing_time_seconds_count metric replaces http_server_requests_seconds_count.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-161 (Cont.) occnp_amervice_overall_processing_time_seconds_count

Field	Details
Dimensions	• Method • Status • uri • container
Example	• occnp_amservice_overall_processing_time_seconds_max{method="DELETE", status="204", uri="/npcf-am-policy-control/v1/policies/{polAssoId}", container="am-service"}

Table 9-162 error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter
Dimensions	• application • applicationException • wrapped_exception
Example	occnp_error_handler_in_total{application="pcf_amservice",application_exception="HttpException",status="404",wrapped_exception="NotFound",} 1.0

Table 9-163 error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter
Dimensions	• application • applicationException • error_type • operation • origin • rule_name • source_interface • target_interface • wrapped_exception
Example	occnp_error_handler_exec_total{application="pcf_amservice",application_exception="JavaException",error_type="INTERNAL",operation="CREATE",origin="JAVA",rule_name="REJECT_WITH_ENHANCED_DETAIL",source_interface="AMF",status="400",target_interface="POLICY",wrapped_exception="ServiceException",} 2.0

Table 9-164 error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-164 (Cont.) error_handler_out_total

Field	Details
Dimensions	• application • applicationException • error_resolved • wrapped_exception
Example	occnp_error_handler_out_total{application="pcf_amservice",application_exception="HttpException",error_resolved="false",status="404",wrapped_exception="NotFound",} 1.0

Table 9-165 occnp_policy_retry_exhausted_total

Field	Details
Description	This metric is incremented when AM service to PRE service interaction is retried (for resiliency) and exhausted due to the below factors: • AM service caught an exception (Any Exception apart from TimeoutException) while waiting for PRE response. • PRE service is down due to environmental factors. • PRE is closing the connections with EOFException.
Type	Counter
Dimensions	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exported_application • helm_sh_chart • hostname • instance • io_kompose_service • job • microservice • mktgVersion • namespace • operation_type • pod • pod_template_hash • vendor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-165 (Cont.) occnp_policy_retry_exhausted_total

Field	Details
Example	occnp_policy_retry_exhausted_total {app_kubernetes_io_instance="my-cnpolicy", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="am-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="1.0.0", application="occnp", container="am-service", endpoint="cnc-metrics", engVersion="24.2.0-rc.7", exported_application="pcf_amservice", helm_sh_chart="am-service-24.2.0-rc.7", hostname="my-cnpolicy-pcf-amservice-54db5bfdf8-cphjm", instance="10.233.127.9:9000", io_kompose_service="my-cnpolicy-pcf-amservice", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_am", mktgVersion="1.0.0", namespace="hi-manim", operation_type="create", pod="my-cnpolicy-pcf-amservice-54db5bfdf8-cphjm", pod_template_hash="54db5bfdf8", vendor="Oracle"}

Table 9-166 occnp_pds_location_info_notification_total

Field	Details
Description	This metric gets incremented when AM core service gets notification from PDS to update PDS Location info in case of concurrency.
Type	Counter
Dimensions	• application • hostname • operation_type • response_code • session_type
Example	• occnp_pds_location_info_notification_total{application="pcf_amservice",hostname="pcf-pcf-amservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="5xx",session_type="am_session",} 1.0 • occnp_pds_location_info_notification_total{application="pcf_amservice",hostname="pcf-pcf-amservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="2xx",session_type="am_session",} 1.0 • occnp_pds_location_info_notification_total{application="pcf_amservice",hostname="pcf-pcf-amservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="4xx",session_type="am_session",} 1.0

Table 9-167 dnn_replacement_total

Field	Details
Description	This metric gets incremented for AM Create and AM Updated when DNN replacement feature is negotiated successfully between the AMF and PCF network functions.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-167 (Cont.) dnn_replacement_total

Field	Details
Dimensions	• operation_type • dnn_replacement_sent Possible values: – true – false – null • unsupp_dnn_sent Possible values: – true – false • allowed_snssai_ch_received Possible values: – true – false – null • candidate_for_replacement_sent Possible values: – true – false – null • smf_select_ch_sent Possible values: – true – false – null • smf_select_ch_received Possible values: – true – false – null • incoming_dnn Possible value can be dnnValue or "" • incoming_snssai Possible value can be snssaiValue or "" • mandatory_ie_missing Possible values: – snssai – dnn – allowedSnssai • smf_selection_data_set Possible values: – true – false – null

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-167 (Cont.) dnn_replacement_total

Field	Details
Example	{application="pcf_amservice",candidate_for_replacement_sent="false",hostname="sm-pcf-amservice-7c8d6c9b44-9lnr8",incoming_dnn="",incoming_snssai="",operation_type="create",smf_select_ch_received="false",unsup p_dnn_sent="false"} {application="pcf_amservice",candidate_for_replacement_sent="false",hostname="sm-pcf-amservice-7c8d6c9b44-9lnr8",incoming_dnn="",incoming_snssai="",operation_type="create",smf_select_ch_received="false",unsup p_dnn_sent="true"} {application="pcf_amservice",candidate_for_replacement_sent="true",hostname="sm-pcf-amservice-7c8d6c9b44-9lnr8",incoming_dnn="",incoming_snssai="",operation_type="create",smf_select_ch_received="false",unsupp _dnn_sent="true"}

For more information about Dimensions, see CNC Policy Metrics.

9.7 CM Service Metrics

The following table describes the CM Service metrics and respective dimensions:

Table 9-168 system_operational_state

Field	Details
Description	This metric indicates the current operational state
Metric Type	Gauge
Dimensions	• application • eng_version • namespace • node • pod • vendor

For more information about Dimensions, see CNC Policy Metrics.

Examples

- system_operational_state{application="config-server",eng_version="",microservice="",namespace="",node="",pod="occnp-config-mgmt",vendor="oracle",} 1.0

Table 9-169 data_repository_invocations_seconds_max

Field	Details
Description	This metric is used to track the maximum execution time of Data repository invocations. It is a useful metric for monitoring the performance of data repositories and identifying slow-running queries.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-169 (Cont.) data_repository_invocations_seconds_max

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_max{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-170 data_repository_invocations_seconds_sum

Field	Details
Description	The seconds_sum metric for Data repository invocations is a measure of the total time spent executing repository methods.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-170 (Cont.) data_repository_invocations_seconds_sum

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_sum{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.84.88:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nshv9", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-171 data_repository_invocations_seconds_count

Field	Details
Description	This metric measures the total time spent in Data JPA repository invocations. It is a counter metric, which means that it increments each time a repository method is invoked. The metric is reported in seconds.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-171 (Cont.) data_repository_invocations_seconds_count

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • service • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_count{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="findAll", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditRegistrationsRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

9.8 PA Service Metrics

The following table describes the PA Service metrics and respective dimensions:

Table 9-172 ocpm_ingress_request_total

Field	Details
Description	Total number of ingress requests received.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-172 (Cont.) ocpm_ingress_request_total

Field	Details
Dimensions	• application • dnn • nf_instance_id • operation_type • sbi_priority • servicename_3gpp • snssai

Examples:

•

- ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="create",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",} 1.0 ; Type-Counter
- ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="update",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",} 1.0 ; Type-Counter
- ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="delete",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",} 1.0 ; Type-Counter
- ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="get",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",} 1.0 ; Type-Counter

Table 9-173 ocpm_ingress_response_total

Field	Details
Description	Total number of ingress responses.
Metric Type	Counter
Dimensions	• application • dnn • nf_instance_id • operation_type • response_code • sbi_priority • servicename_3gpp • snssai • binding_level • binding_id

Examples:

- ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="create",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",} 1.0 ; Type-Counter
- ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="update",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-

Copyright © 2019, 2026, Oracle and/or its affiliates.

policyauthorization",snssai="11-abc123",binding_level="", binding_id=""} 1.0 ; Type-Counter

- ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="", operation_type="delete",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",binding_level="", binding_id=""} 1.0 ; Type-Counter
- ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="", operation_type="get",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",binding_level="", binding_id=""} 1.0 ; Type-Counter

Table 9-174 remote_delete_notify_total

Field	Details
Description	Total number of delete requests.
Metric Type	Counter
Dimensions	• Code • Request • SessionType • hostname

Examples:

- remote_delete_notify_total{Code="2xx",Request="DeleteNotify",SessionType="PA",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0
- remote_delete_notify_total{Code="4xx",Request="DeleteNotify",SessionType="PA",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0
- remote_delete_notify_total{Code="5xx",Request="DeleteNotify",SessionType="PA",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0
- remote_delete_notify_total{Code="N/A",Request="EmulateDelete",SessionType="PA",application="pcf_smservice",hostname="4dfc2dfc25da",} 0.0

Table 9-175 session_oam_request_total

Field	Details
Description	Number of session requests for PA Service
Metric Type	Request
Dimensions	• Response Code • Operation Type • SessionType

Table 9-176 session_oam_response_total

Field	Details
Description	Number of session responses for PA Service
Metric Type	Response

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-176 (Cont.) session_oam_response_total

Field	Details
Dimensions	• Response Code • Operation Type • SessionType

Table 9-177 occnp_pa_sponsored_sessions_total

Field	Details
Description	This metric is incremented when PCF responds to AF for sponsored sessions, irrespective of whether the request is processed successfully or rejected during the request evaluation. The value of the `sponId` and `aspId` dimensions are set to *NotSpecified* if the value of `SYSTEM.INCLUDE_SPONID_ASPID_DIMENSIONS` advanced settings key is set to *false* or if the limit defined by `SPONID_ASPID_PAIR_CARDINALITY_LIMIT` Helm parameter is exceeded. **Note:** This metric is pegged if a local delete is triggered because the AF does not send PA Delete on receiving *terminate_notify* from PCF within 3 seconds.
Metric Type	Counter
Dimensions	• application • hostname • operationTypeN5 • sponId • aspId • sponStatus • umcDataIncluded • responseCode • cause

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-177 (Cont.) occnp_pa_sponsored_sessions_total

Field	Details
Example	occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="CREATE",responseCode="201",sponId="",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 1.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="",cause="MANDATORY_IE_MISSING",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="CREATE",responseCode="400",sponId="",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 2.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test109test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="CREATE",responseCode="201",sponId="test109test",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 20.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test109test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="DELETE",responseCode="204",sponId="test109test",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 1.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test109test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="DELETE",responseCode="204",sponId="test109test",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 9.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test109test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="MODIFY",responseCode="204",sponId="test109test",sponStatus="SPONSOR_DISABLED",umcDataIncluded="true"} 1.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test109test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="MODIFY",responseCode="204",sponId="test109test",sponStatus="SPONSOR_ENABLED",umcDataIncluded="true"} 7.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test110R",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="CREATE",responseCode="201",sponId="test110R",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 3.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test110test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="CREATE",responseCode="201",sponId="test110test",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 1.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test110test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="DELETE",responseCode="204",sponId="test110test",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 1.0 occnp_pa_sponsored_sessions_total{application="pcf_smservice",aspId="test110test",cause="",hostname="ocpcf-pcf-smservice-5dc7b7dfb5-kzclr",operationType="MODIFY",responseCode="204",sponId="test110test",sponStatus="SPONSOR_DISABLED",umcDataIncluded="true"} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-178 occnp_pa_sponsored_session_update_notify_total

Field	Details
Description	This metric is incremented when PCF receives a response from SMF. It is counted exclusively for sponsored sessions. This metric is not counted for update_notify during a normal flow. The value of the `sponId` and `aspId` dimensions are set to *NotSpecified* if the value of `SYSTEM.INCLUDE_SPONID_ASPID_DIMENSIONS` is set to *false* or if the limit defined by `SPONID_ASPID_PAIR_CARDINALITY_LIMIT` Helm parameter is exceeded. **Note**: *terminate_notify* will not be considered, since it only goes to AF.
Metric Type	Counter
Dimensions	• application • hostname • operationTypeN5 • servicename3gpp • sponId • aspId • sponStatus • umcDataIncluded • responseCode • cause

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-178 (Cont.) occnp_pa_sponsored_session_update_notify_total

Field	Details
Example	occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="CREATE",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 7.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="CREATE",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 10.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="CREATE",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_ENABLED",umcDataIncluded="true"} 20.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="CREATE",responseCode="500",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 2.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="CREATE",responseCode="500",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_ENABLED",umcDataIncluded="true"} 1.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="DELETE",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 7.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="DELETE",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 30.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="MODIFY",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 5.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="MODIFY",responseCode="204",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 27.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-178 (Cont.) occnp_pa_sponsored_session_update_notify_total

Field	Details
	smservice-844b694f98-9cgh8",operationTypeN5="MODIFY",responseCode="500",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_DISABLED",umcDataIncluded="false"} 2.0 occnp_pa_sponsored_session_update_notify_total{application="pcf_smservice",aspId="NotSpecified",cause="",hostname="ocpcf-pcf-smservice-844b694f98-9cgh8",operationTypeN5="MODIFY",responseCode="500",servicename3gpp="npcf-smpolicycontrol",sponId="NotSpecified",sponStatus="SPONSOR_ENABLED",umcDataIncluded="false"} 1.0

Table 9-179 occnp_pa_qosmon_request_total

Field	Description
Description	This metric is incremented when PCF receives requests from AF/NEF with subscription to QoS Monitoring.
Metric Type	Counter
Dimensions	• **notificationMethod:** The notification method passed for QOS_MONITORING event (PERIODIC, EVENT_DETECTION or PERIODIC_AND_EVENT_TRIGGERED) • **operation_type:** The operation type for the request • **incompleteQosMonAttr:** true or false based on the QosMonitoring attributes provided in the app session creation request regardless of the request being rejected or not based on ACCEPT_REQUEST_ON_MISSING_QOS_MON_ATTR config
Examples	occnp_pa_qosmon_request_total(notificationMethod="EVENT_DETECTION", operationType="CREATE", incompleteQosMonAttr="false")

Table 9-180 occnp_pa_qosmon_response_total

Field	Description
Description	This metric is incremented when PCF replies to requests from AF/NEF with subscription to Qos Monitoring
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-180 (Cont.) occnp_pa_qosmon_response_total

Field	Description
Dimensions	• **operation_type:** The operation type for the create request • **response_code:** Http code returned in response • **cause:** Populated when the response was unsuccessful, values can be: MISSING_ATTR,FEATURE_UNSUPPORTED, REJECTED. For success responses the dimension is not populated
Examples	occnp_pa_qosmon_response_total(operation_type="CREATE", response_code="201")

For more information about Dimensions, see CNC Policy Metrics.

9.9 UE Service Metrics

The following table describes the new UE Service metrics and the respective dimensions:

Table 9-181 ue_n1_ursp_rule_delivery

Field	Details
Description	This metric is incremented when a URSP rule is selected for delivery to UE.
Metric Type	Counter
Dimensions	ruleName

Table 9-182 ue_n1_transfer_request_total

Field	Details
Description	This metric shall be incremented when PCF sends an encoded N1 message (fragment) to AMF for delivery to UE.
Metric Type	Counter
Dimensions	• fragCount • fragIdx

Table 9-183 ue_n1_transfer_response_total

Field	Details
Description	This metric shall be incremented when PCF receives a response from AMF for an N1 message (fragment) delivery to UE.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-183 (Cont.) ue_n1_transfer_response_total

Field	Details
Dimensions	• fragCount • fragIdx • responseCode • latency • cause

Table 9-184 ue_n1_transfer_exception

Field	Details
Description	This metric shall be incremented when PCF encounters an exception and fails to initiate an N1 message (fragment) delivery.
Metric Type	Counter
Dimensions	• fragCount • fragIdx

Table 9-185 ue_n1_transfer_retransmit_total

Field	Details
Description	This metric shall be incremented when PCF re-transmits an encoded N1 message (fragment) to AMF for delivery to UE.
Metric Type	Counter
Dimensions	• fragCount • fragIdx

Table 9-186 ue_n1_transfer_abort

Field	Details
Description	This metric shall be incremented when PCF aborts an N1 message delivery procedure.
Metric Type	Counter
Dimensions	reason

Table 9-187 ue_n1_transfer_skip

Field	Details
Description	This metric shall be incremented when PCF skips an N1 message fragment.
Metric Type	Counter
Dimensions	NA

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-188 ue_n1_transfer_failure_notification

Field	Details
Description	This metric shall be incremented when PCF receives a transfer failure notification from the AMF.
Metric Type	Counter
Dimensions	cause

Table 9-189 ue_n1_transfer_ue_notification_total

Field	Details
Description	This metric shall be incremented when PCF receives an N1 notification from the UE.
Metric Type	Counter
Dimensions	commandType

The following table describes the UE Service metrics and respective dimensions:

Table 9-190 ocpm_ingress_request_total

Field	Details
Description	Total number of ingress requests received
Metric Type	Counter
Dimensions	• operation_type • service name_ 3gpp
Example	• ocpm_ingress_request_total{operation_type="get",servicename_3gpp="npcf-ue-policy-control",} 2.0 ; Type-Counter

Table 9-191 ocpm_ingress_response_total

Field	Details
Description	Total number of ingress responses
Metric Type	Counter
Dimensions	• cause • operation_type • servicename_3gpp • response_code
Example	• ocpm_ingress_response_total{operation_type="get",response_code="5xx",servicename_3gpp="npcf-ue-policy-control",} 4.0 ; Type-Counter • ocpm_ingress_response_total{cause="Internal Server Error",operation_type="get",response_code="5xx",servicename_3gpp="npcf-ue-policy-control",} 4.0 ; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-192 ocpm_egress_request_total

Field	Details
Description	Total number of egress requests received
Metric Type	Counter
Dimensions	• operation_type • dnn • snssai • nf_instance_id • sbi_priority • servicename_3gpp
Example	• ocpm_egress_request_total{application="pcf_ueservice",binding_id="",binding_level="",discovery_id="",discovery_parameter="target-nf-set-id",hostname="pcf-pcf-ueservice-7988ccfbd9-zn8hs",nf_instance_id="13515195-c537-4645-9b97-96ec797fbbbf",nf_name="nf1stub.gunther-ns.svc",operation_type="audit_notification",servicename_3gpp="npcf-ue-policy-control",} 1.0

Table 9-193 ocpm_egress_response_total

Field	Details
Description	Total number of egress responses.
Metric Type	Counter
Dimensions	• operation_type • dnn • snssai • nf_instance_id • sbi_priority • servicename_3gpp • response_code • latency • cause
Example	• ocpm_egress_response_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-7988ccfbd9-zn8hs",nf_instance_id="13515195-c537-4645-9b97-96ec797fbbbf",nf_name="nf1stub.gunther-ns.svc",operation_type="audit_notification",response_code="5xx",servicename_3gpp="npcf-ue-policy-control",} 1.0

Table 9-194 session_viewer_request_total

Field	Details
Description	This metric shows the total number of query requests made using the Session Viewer.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-194 (Cont.) session_viewer_request_total

Field	Details
Dimensions	• operation_type (GET or DELETE) • response_code (2xx, 5xx) • session_type(ue_session)

Table 9-195 session_viewer_response_total

Field	Details
Description	This metric shows the total number of responses to query requests made using the Session Viewer.
Metric Type	Counter
Dimensions	-

Table 9-196 session_oam_request_total

Field	Details
Description	Number of session requests for UE Service
Metric Type	Request
Dimensions	• Response Code • Operation Type • SessionType

Table 9-197 session_oam_response_total

Field	Details
Description	Number of session responses for UE Service
Metric Type	Response
Dimensions	• Response Code • Operation Type • SessionType

Table 9-198 occnp_ue_audit_stale_records_count_total

Field	Details
Description	Total number of stale records received from Audit Service in all notifications
Metric Type	Counter
Dimensions	• application • hostname
Example	• occnp_ue_audit_stale_records_count_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-58f8bd57d5-frggs",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-199 occnp_ue_audit_deleted_records_count_total

Field	Details
Description	Total number of stale records deleted.
Metric Type	Counter
Dimensions	• application • hostname
Example	• occnp_ue_audit_deleted_records_count_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-58f8bd57d5-frggs",} 1.0

Table 9-200 occnp_ue_update_notify_rcvd_error_response_total

Field	Details
Description	Total number of update notify requests that can not be sent to AMF or timed out
Metric Type	Counter
Dimensions	• application • hostname • response_code
Example	• occnp_ue_update_notify_rcvd_error_response_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-7988ccfbd9-zn8hs",response_code="5xx",} 1.0

Table 9-201 audit_recs_stale_total

Field	Details
Description	Total number of records detected as stale
Metric Type	Counter
Dimensions	• ServiceName • TableName
Example	• audit_recs_stale_total{ServiceName="pcf-ueservice",TableName="UePolicyAssociation",} 1.0

Table 9-202 occnp_ue_audit_notif_sent_to_amf_count_total

Field	Details
Description	Total number of notifications sent to AMF on receiving stale session notification from audit
Metric Type	Counter
Dimensions	• application • hostname
Example	• occnp_ue_audit_notif_sent_to_amf_count_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-7988ccfbd9-zn8hs",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-203 occnp_ue_audit_update_notify_session_found_total

Field	Details
Description	Total number of sessions found at AMF on sending update notify request (that is, when received 204 response from AMF)
Metric Type	Counter
Dimensions	• application • hostname
Example	• occnp_ue_audit_update_notify_session_found_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-58f8bd57d5-frggs",} 1.0

Table 9-204 occnp_ue_audit_update_notify_session_not_found_total

Field	Details
Description	Total number of sessions not found at AMF on sending update notify request (that is, received 404 response from AMF)
Metric Type	Counter
Dimensions	• application • hostname
Example	• occnp_ue_audit_update_notify_session_not_found_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-58f8bd57d5-frggs",} 1.0

Table 9-205 occnp_ue_audit_deleted_records_maxttl_reached_count_total

Field	Details
Description	Total number of records deleted as maxTTL expired
Metric Type	Counter
Dimensions	• application • hostname
Example	• occnp_ue_audit_deleted_records_maxttl_reached_count_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-58f8bd57d5-frggs",} 1.0

Table 9-206 session_info_request_total

Field	Details
Description	Total number of sessions to be deleted as requested by the UE Policy Service
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-206 (Cont.) session_info_request_total

Field	Details
Dimensions	• application • cause • operation_type • session_type
Example	• session_info_request_total{application="pcf_ueservice",cause="local_limiting_session",operation_type="cleanup",session_type="ue_session",} 3.0

Table 9-207 occnp_lease_duration_seconds_bucket

Field	Details
Description	Time in seconds for which UE Service holds the lock
Metric Type	Histogram
Dimensions	• Lock_Lease_Duration • Message_Type • application • quartile

Table 9-208 session_info_response_total

Field	Details
Description	Total number of sessions deleted as requested by the UE Policy Service
Metric Type	Counter
Dimensions	• application • cause • operation_type • response_code • session_type
Example	• session_info_response_total{application="pcf_ueservice",cause="local_limiting_session",operation_type="cleanup",response_code="5xx",session_type="ue_session",} 2.0

Table 9-209 occnp_ue_discovery_success_count_total

Field	Details
Description	Enables Policy to report how many discoveries based in AMF Region ID and AMF Set ID or GUAMI were successful
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-209 (Cont.) occnp_ue_discovery_success_count_total

Field	Details
Dimensions	• discoveryType • setID • regionID • mcc • mnc • amfId
Example	• occnp_ue_discovery_success_count_total '{discoveryType="setIdRegionId", setID="2", regionID="1",mcc="",mnc="",amfId=""}',2 • occnp_ue_discovery_success_count_total '{discoveryType="guami",setID="",regionID="", mcc="450",mnc="05",amfId="010041"}',2

Table 9-210 occnp_ue_discovery_failure_count_total

Field	Details
Description	Enables Policy to report how many discoveries based in AMF Region ID and AMF Set ID or GUAMI failed
Metric Type	Counter
Dimensions	• discoveryType • setID • regionID • mcc • mnc • amfId
Example	• occnp_ue_discovery_failure_count_total '{discoveryType="setIdRegionId", setID="1", regionID="2",mcc="",mnc="",amfId=""}',1

Table 9-211 occnp_http_ue_request_total

Field	Details
Description	Number of http UE requests
Metric Type	Counter
Dimensions	• application • hostname • operationType • servicenameNon3gpp
Example	• occnp_http_ue_request_total{application="pcf_ueservice",hostname="jiandong-pcf-ueservice-5878554dc7-wgvc7",operationType="bulwark_lock",servicenameNon3gpp="npcf-ueservice"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-212 occnp_http_ue_response_total

Field	Details
Description	Number of http UE responses
Metric Type	Counter
Dimensions	• application • hostname • operationType • servicenameNon3gpp
Example	• occnp_http_ue_response_total{application="pcf_ueservice",hostname="ueservice-5878554dc7-wgvc7",operationType="bulwark_unlock", responseCode="204",servicenameNon3gpp="npcf-ueservice", retry=false}

Table 9-213 occnp_http_out_conn_request_total

Field	Details
Description	Total number of connection requests received
Metric Type	Counter
Dimensions	• Application • bindingId • bindingLevel • discoveryId • discoveryParameter • hostname • nfInstanceId • nfName • operationType • servicename3gpp • isReattempt • isRetryAttempt • reattemptType
Example	• http_out_conn_request_total{application="pcf_ueservice",bindingId="set001.region48.amfset.5gc.mnc012.mcc345",bindingLevel="nf-set",discoveryId="set001.region48.amfset.5gc.mnc012.mcc345",discoveryParameter="target-nf-set-id",hostname="my-cnpolicy-pcf-ueservice-6696fd4bf4-6mf8v",nfInstanceId="13515195-c537-4645-9b97-96ec797f2222",nfName="nf1stub.harald-ns.svc",operationType="transfer",servicename3gpp="npcf-ue-policy-control",} 3.0

Table 9-214 occnp_http_out_conn_response_total

Field	Details
Description	Total number of connection response sent
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-214 (Cont.) occnp_http_out_conn_response_total

Field	Details
Dimensions	• Application • hostname • nfInstanceId • nfName • operationType • servicename3gpp • isReattempt • isRetryAttempt • reattemptType
Example	• http_out_conn_response_total{application="pcf_ueservice",hostname="my-cnpolicy-pcf-ueservice-7d5bc8d8d4-gsnr4",nfInstanceId="13515195-c537-4645-9b97-96ec797f2222",nfName="nf1stub.harald-ns.svc",operatione="2xx",servicename3gpp="npcf-ue-policy-control",} 3.0

Table 9-215 ocpm_ar_request_total

Field	Details
Description	Total number of ar requests received
Metric Type	Counter
Dimensions	• Application • fqdn • hostname • scheme • servicename3gpp
Example	• ocpm_ar_request_total{application="pcf_ueservice",fqdn="nf22stub.harald-ns.svc",hostname="my-cnpolicy-pcf-ueservice-7d5bc8d8d4-gsnr4",scheme="http",servicename3gpp="npcf-ue-policy-control",} 1.0

Table 9-216 ocpm_ar_response_total

Field	Details
Description	Total number of ar response sent
Metric Type	Counter
Dimensions	• Application • fqdn • hostname • scheme • servicename3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-216 (Cont.) ocpm_ar_response_total

Field	Details
Example	• ocpm_ar_response_total{application="pcf_ueservice",fqdn="nf22stub.harald-ns.svc",hostname="my-cnpolicy-pcf-ueservice-7d5bc8d8d4-gsnr4",responseCode="4xx",scheme="http",servicename3gpp="npcf-ue-policy-control",} 1.0

Table 9-217 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Metric Type	Counter
Dimensions	• Service Name • Pod Name

Table 9-218 n1_message_policy_evaluation

Field	Details
Description	Metric that increments each time there was a policy evaluated for skip, abort and retransmit n1 notification message.
Metric Type	Counter
Dimensions	• action (action that has been taken skip/abort/retransmit/retransmit_fragment) • message_type (MANAGE UE POLICY COMMAND REJECT/ N1N2MessageTransferFailure)

Table 9-219 occnp_db_overall_processing_time_seconds_sum

Field	Details
Description	This metric is incremented when PCF performs DELETE operation on an Association
Metric Type	Counter
Dimensions	• Method • Status • Table
Example	• occnp_db_overall_processing_time_seconds_sum{Method="delete", Status="Success", Table="UePolicyAssociation", container="ue-service"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-220 occnp_db_overall_processing_time_seconds_sum

Field	Details
Description	This metric is incremented when PCF performs DELETE operation on an Association
Metric Type	Counter
Dimensions	• Method • Status • Table
Example	• occnp_db_overall_processing_time_seconds_sum{Method="delete", Status="Success", Table="UePolicyAssociation", container="ue-service"}

Table 9-221 occnp_ueservice_overall_processing_time_seconds_max

Field	Details
Description	This metric is incremented for UE service to calculate processing's duration of HTTP request arrived on rest controller. **Note**: occnp_ueservice_overall_processing_time_seconds_max metric replaces http_server_requests_seconds_max.
Metric Type	Counter
Dimensions	• Method • Status • uri • container
Example	• occnp_ueservice_overall_processing_time_seconds_max{method="DELETE", status="204", uri="/npcf-ue-policy-control/v1/policies/{polAssoId}", container="ue-service"}

Table 9-222 occnp_ueservice_overall_processing_time_seconds_sum

Field	Details
Description	This metric is incremented for UE service to calculate processing's duration of HTTP request arrived on rest controller. **Note**: occnp_ueservice_overall_processing_time_seconds_sum metric replaces http_server_requests_seconds_sum.
Metric Type	Counter
Dimensions	• Method • Status • uri • container

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-222 (Cont.) occnp_ueservice_overall_processing_time_seconds_sum

Field	Details
Example	• occnp_ueservice_overall_processing_time_seconds_sum{method="DELETE", status="204", uri="/npcf-ue-policy-control/v1/policies/{polAssoId}", container="ue-service"}

Table 9-223 occnp_ueservice_overall_processing_time_seconds_count

Field	Details
Description	This metric is incremented for UE service to calculate processing's duration of HTTP request arrived on rest controller. **Note**: occnp_ueservice_overall_processing_time_seconds_count metric replaces http_server_requests_seconds_count.
Metric Type	Counter
Dimensions	• Method • Status • uri • container
Example	• occnp_ueservice_overall_processing_time_seconds_count{method="DELETE", status="204", uri="/npcf-ue-policy-control/v1/policies/{polAssoId}", container="ue-service"}

Table 9-224 ue_n1_unsubscribe_request_total

Field	Details
Description	This metric is incremented while UE service sends request to NAS-AMF for N1 UNSUBSCRIBE.
Metric Type	Counter
Dimensions	• servingPlmn
Example	• ue_n1_unsubscribe_request_total{servingPlmn="450005"}

Table 9-225 ue_n1_unsubscribe_response_total

Field	Details
Description	This metric is incremented when NAS-AMF sends back HTTP response to UE service for N1 UNSUBSCRIBE.
Metric Type	Counter
Dimensions	• latency • responseCode • servingPlmn

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-225 (Cont.) ue_n1_unsubscribe_response_total

Field	Details
Example	• ue_n1_unsubscribe_response_total{latency="3",servingPlmn="450005",responseCode="204"}

Table 9-226 ue_n1_unsubscribe_exception_total

Field	Details
Description	This metric is incremented in case of any exception occurred while sending N1 UNSUBSCRIBE request to NAS-AMF.
Metric Type	Counter
Dimensions	• servingPlmn
Example	• ue_n1_unsubscribe_exception_total{servingPlmn="450005"}

Table 9-227 error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter
Dimensions	• application • applicationException • wrapped_exception
Example	occnp_error_handler_in_total{application="pcf_ueservice",application_exception="JavaException",status="400",wrapped_exception="ServiceException",} 6.0

Table 9-228 error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter
Dimensions	• application • applicationException • error_type • operation • origin • rule_name • source_interface • target_interface • wrapped_exception
Example	occnp_error_handler_exec_total{application="pcf_ueservice",application_exception="JavaException",error_type="INTERNAL",operation="UPDATE",origin="JAVA",rule_name="REJECT_WITH_ENHANCED_DETAIL",source_interface="AMF",status="411",target_interface="POLICY",wrapped_exception="ServiceException",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-229 error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter
Dimensions	• application • applicationException • error_resolved • wrapped_exception
Example	occnp_error_handler_out_total{application="pcf_ueservice",application_exception="JavaException",error_resolved="false",status="500",wrapped_exception="Service Exception",} 11.0

Table 9-230 occnp_http_congestion_message_reject_total

Field	Details
Description	Track the count of rejected HTTP messages due to congestion.
Type	Counter
Dimension	• message priority (priority) • response code (responseCode) • operation (operation) • rest endpoint (uri) • congestion state
Example	• occnp_http_congestion_message_reject_total_seconds_count{application="pcf_ueservice",congestion_state="DANGER_OF_CONGESTION",hostname="hm-manim-helm-pcf-ueservice-5cf4654675-hh5b9",message_priority="28",operation_type="POST",request_uri="/audit/notify",response_code="503",} 1.0;

Table 9-231 occnp_http_congestion_message_reject_total_seconds_bucket

Field	Details
Description	Track the count of rejected HTTP messages due to congestion.
Type	Counter
Dimension	• message priority (priority) • response code (responseCode) • operation (operation) • rest endpoint (uri) • congestion state
Example	• http_congestion_message_reject_total_seconds_bucket{application="pcf_ueservice",congestion_state="DANGER_OF_CONGESTION",hostname="hm-manim-helm-pcf-ueservice-5cf4654675-hh5b9",message_priority="30",operation_type="POST",request_uri="/audit/notify",response_code="504",le="+Inf",} 1.0; Type-Histogram

Table 9-232 occnp_http_congestion_message_reject_total_seconds_count

Field	Details
Description	Track the count of rejected HTTP messages due to congestion.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-232 (Cont.) occnp_http_congestion_message_reject_total_seconds_count

Field	Details
Dimension	• message priority (priority) • response code (responseCode) • operation (operation) • rest endpoint (uri) • congestion state
Example	• http_congestion_message_reject_total_seconds_count{application="pcf_ueservice",congestion_state="DANGER_OF_CONGESTION",hostname="hm-manim-helm-pcf-ueservice-5cf4654675-hh5b9",message_priority="30",operation_type="POST",request_uri="/audit/notify",response_code="504",} 1.0; Type-Histogram

Table 9-233 occnp_http_congestion_message_reject_total_seconds_sum

Field	Details
Description	Track the count of rejected HTTP messages due to congestion.
Type	Histogram
Dimension	• message priority (priority) • response code (responseCode) • operation (operation) • rest endpoint (uri) • congestion state
Example	• http_congestion_message_reject_total_seconds_sum{application="pcf_ueservice",congestion_state="DANGER_OF_CONGESTION",hostname="hm-manim-helm-pcf-ueservice-5cf4654675-hh5b9",message_priority="30",operation_type="POST",request_uri="/audit/notify",response_code="504",} 0.029; Type-Histogram

Table 9-234 occnp_http_congestion_message_reject_total_seconds_max

Field	Details
Description	Track the count of rejected HTTP messages due to congestion.
Type	Histogram
Dimension	• message priority (priority) • response code (responseCode) • operation (operation) • rest endpoint (uri) • congestion state
Example	• http_congestion_message_reject_total_seconds_max{application="pcf_ueservice",congestion_state="DANGER_OF_CONGESTION",hostname="hm-manim-helm-pcf-ueservice-5cf4654675-hh5b9",message_priority="30",operation_type="POST",request_uri="/audit/notify",response_code="504",} 0.0; Type-Histogram

Table 9-235 occnp_http_congestion_message_reject_total_second

Field	Details
Description	Track the count of rejected HTTP messages due to congestion.
Type	Histogram

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-235 (Cont.) occnp_http_congestion_message_reject_total_second

Field	Details
Dimension	• message priority (priority) • response code (responseCode) • operation (operation) • rest endpoint (uri) • congestion state
Example	• http_congestion_message_reject_total_seconds{application="pcf_ueservice",congestion_state="DANGER_OF_CONGESTION",hostname="hm-manim-helm-pcf-ueservice-5cf4654675-hh5b9",message_priority="30",operation_type="POST",request_uri="/audit/notify",response_code="504",quartile="0.5",} 0.0; Type-Histogram

Table 9-236 occnp_pds_location_info_notification_total

Field	Details
Description	This metric gets incremented when UE core service gets notification from PDS to update PDS Location info in case of concurrency.
Type	Counter
Dimensions	• application • hostname • operation_type • response_code • session_type
Example	• occnp_pds_location_info_notification_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="5xx",session_type="ue_session",} 1.0 • occnp_pds_location_info_notification_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="2xx",session_type="ue_session",} 1.0 • occnp_pds_location_info_notification_total{application="pcf_ueservice",hostname="pcf-pcf-ueservice-699fc555db-tm9k8",operation_type="pds_location_info_notify",response_code="4xx",session_type="ue_session",} 1.0

Table 9-237 ue_n1_subscribe_request_total

Field	Details
Description	This metric is incremented when PCF sends a request to AMF for N1 subscription.
Type	Counter
Dimensions	servingPlmn
Example	ue_n1_subscribe_request_total{application="pcf_ueservice",hostname="rel-pcf-ueservice-67d4fd6b49-sqz57",servingPlmn="330042",}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-238 ue_n1_subscribe_response_total

Field	Details
Description	This metric is incremented when PCF receives a response from AMF for N1 subscription request.
Type	Counter
Dimensions	• latency • responseCode • servingPlmn
Example	ue_n1_subscribe_response_total{application="pcf_ueservice",hostname="rel-pcf-ueservice-67d4fd6b49-sqz57",latency="5",responseCode="201",servingPlmn="330042",}

Table 9-239 ue_n1_policy_sequencing

Field	Details
Description	This metric tracks each time a UE policy decision is placed into the pending queue for later delivery. That is, when the system needs to hold the decision for a future N1 transfer. It is recorded whenever a Timer due to `RetryAfterIE` or `Reattempt and Backoff` is actively running, even if the consolidation feature flag (**Enable Consolidation of UE Policy Decisions** field under section **AMF** on **PCF UE Policy** for **Service Configurations** on CNC Console) is on, and only omitted when consolidation is enabled and no timer is running, because the decisions are then sent together in a single batch.
Type	Counter
Dimensions	• source Possible values: – N1MESSAGENOTIFY_COMMAND_COMPLETE – NCHF_SPENDINGLIMITCONTROL_NOTIFY – NPCF_UEPOLICYCONTROL_UPDATE – UDR_POLICY_DATA_CHANGE_NOTIFICATION • isReattempt
Example	ue_n1_policy_sequencing_total{app_kubernetes_io_instance="ocpcf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="ue-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="1.0.0", application="occnp", container="ue-service", endpoint="cnc-metrics", engVersion="25.1.0-beta.4", exported_application="pcf_ueservice", helm_sh_chart="ue-service-25.1.0-beta.4", hostname="ocpcf-pcf-ueservice-7f697f6797-f6962", instance="10.233.105.239:9000", io_kompose_service="ocpcf-pcf-ueservice", job="occne-infra/occne-nf-cnc-podmonitor", microservice="pcf_ueservice", mktgVersion="1.0.0", namespace="hi-ns01", pod="ocpcf-pcf-ueservice-7f697f6797-f6962", pod_template_hash="7f697f6797", source="nchf_spendinglimitcontrol_notify", vendor="Oracle"}

Table 9-240 ue_n1_policy_consolidation_total

Field	Details
Description	This metric tracks the number of consolidated N1N2 transfers performed. **Note:** The consolidated N1N2 transfer may not be sent to UE if install optimization is enabled.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-240 (Cont.) ue_n1_policy_consolidation_total

Field	Details
Dimensions	• source Possible values: – N1MESSAGENOTIFY_COMMAND_COMPLETE – N1MESSAGENOTIFY_COMMAND_REJECT – N1N2TRANSFER_FAILURE_NOTIFICATION – T3501_EXPIRY – NPCF_UEPOLICYCONTROL_UPDATE • reattempt_timer_expiry_notification: This value in **source** dimension indicates consolidation done on receiving Timer Expiry Notification from Timer Service.
Examples	ue_n1_policy_consolidation_total{app_kubernetes_io_instance="ocpcf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="ue-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="1.0.0", application="occnp", container="ue-service", endpoint="cnc-metrics", engVersion="25.1.0-beta.4", exported_application="pcf_ueservice", helm_sh_chart="ue-service-25.1.0-beta.4", hostname="ocpcf-pcf-ueservice-7f697f6797-f6962", instance="10.233.105.239:9000", io_kompose_service="ocpcf-pcf-ueservice", job="occne-infra/occne-nf-cnc-podmonitor", microservice="pcf_ueservice", mktgVersion="1.0.0", namespace="hi-ns01", pod="ocpcf-pcf-ueservice-7f697f6797-f6962", pod_template_hash="7f697f6797", source="t3501_expiry", vendor="Oracle"}

Table 9-241 ue_n1_policy_backed_off_collation_total

Field	Details
Description	The metrics is pegged when sequenced policy decisions are collated into a single one, either due to an initial request failure followed by subsequent triggers (Update/ UDR, CHF Notify) or when subsequent requests also fail and then both Policy decisions are retransmitted during an reattempt after backoff notification.
Type	Counter
Dimensions	• source - The source for which N1N2MessageTransfer request is initiated. The sources are valid for: NCHF_SpendingLimitControl_Notify Npcf_UEPolicyControl_Update UDR_Policy_Data_Change_Notification Reattempt_Timer_Expiry_Notification
Example	-

Table 9-242 ocpm_late_arrival_rejection_total

Field	Details
Description	This metric is pegged whenever UE receives a request, and it is canceled because it is already stale.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-242 (Cont.) ocpm_late_arrival_rejection_total

Field	Details
Dimensions	• Operation Type Possible values: – CREATE – UPDATE – NOTIFY • Service Name Possible value: UE
Example	-

Table 9-243 occnp_late_processing_rejection_total

Field	Details
Description	This metric is pegged whenever UE receives a request and it got stale during processing.
Type	Counter
Dimensions	• Operation Type Possible values: – CREATE – UPDATE – NOTIFY • Service Name Possible value: UE • Stage Possible values: – PRE_PRE – POST_PRE – PRE_PDS – POST_PDS – PRE_Bulwark – POST_Bulwark – PRE_AMF – PRE_DB – POST_DB
Example	-

Table 9-244 occnp_ue_timer_registration_total

Field	Details
Description	This metric is pegged after sending registration request to timer service. Its state dimension tells whether the request was "SUCCESS" or "FAILURE".
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-244 (Cont.) occnp_ue_timer_registration_total

Field	Details
Dimensions	• **callbackServiceFqdn** - Service FQDN for callback Service. In this case it is the pcf-ue endpoint. • **timerName** - Unique identifier for timer. It can be either of the timer values: - UE_AMFDiscovery - UE_N1N2MessageSubscribe - UE_N1N2MessageTransfer - UE_N1N2TransferFailure • **state** - Tells the state of timer registration request. The possible values: **SUCCESS** - When timer is successfully registered in timer service. **FAILURE** - When timer registration request fails to register.
Example	-

Table 9-245 occnp_ue_timer_create_success_total

Field	Details
Description	This metric is pegged when timer is successfully created in timer service.
Type	Counter
Dimensions	• **timerName** - Unique identifier for timer.
Example	-

Table 9-246 occnp_ue_timer_create_failure_total

Field	Details
Description	This metric is pegged when timer creation fails in timer service.
Type	Counter
Dimensions	• **timerName** - Unique identifier for timer.
Example	-

Table 9-247 occnp_ue_timer_delete_success_total

Field	Details
Description	This metric is pegged when timer deletion request is success in timer service.
Type	Counter
Dimensions	• **timerName** - Unique identifier for timer.
Example	-

Table 9-248 occnp_ue_timer_delete_failure_total

Field	Details
Description	This metric is pegged when timer deletion fails in timer service.
Type	Counter
Dimensions	• **timerName** - Unique identifier for timer.
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-249 occnp_ue_nf_discovery_reattempt_request_total

Field	Details
Description	This metric on the request part is pegged only on reattempted request to NRF for AMF discovery.
Type	Counter
Dimensions	• **operationType** - It will be the operation being performed on resource/session. • **servicename3gpp** - The service name defined as per 3gpp specifications.
Example	-

Table 9-250 occnp_ue_nf_discovery_reattempt_response_total

Field	Details
Description	This metric on response part is pegged only on reattempted request to NRF for AMF discovery.
Type	Counter
Dimensions	• **operationType** - It will be the operation being performed on resource/session. • **servicename3gpp** - The service name defined as per 3gpp specifications. • **responseCode** - Response code received from NRF. • **cause** - Cause of the failure if any.
Example	-

Table 9-251 ue_rule_size_limit_exceeded

Field	Details
Description	This metric has been pegged when UPSI/URSP has been skipped from N1N2 message transfer due to URSP fragment size greater than configured, or N1 message size is greater than configured.
Type	Counter
Dimensions	Rule Name, Rule Type
Example	

Table 9-252 ue_rule_config_error_total

Field	Details
Description	This metric is incremented when an invalid URSP or UPSI rule is used during N1 transfer.
Type	Counter
Dimensions	ruleId, ruleType, ruleName
Example	ue_rule_config_error_total{ruleType="URSP", ruleId="5d99f63d-5f23-4565-8939-7133c68d437f", ruleName="ursp1"}

Table 9-253 ue_n1_transfer_t3501_expiry_total

Field	Details
Description	This metric is incremented when the T3501 timer expires.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-253 (Cont.) ue_n1_transfer_t3501_expiry_total

Field	Details
Dimensions	• fragIdx • servingPlmn
Example	ue_n1_transfer_t3501_expiry_total{application="pcf_ueservice",fragIdx="0",hostname="ocpcf-pcf-ueservice-864499b66b-smqz5",servingPlmn="311480",}1.0

Table 9-254 ue_n1_policy_rule_conflict_total

Field	Details
Description	This metric tracks UE Policy evaluations corresponding to a trigger which results in conflicting UE Policy action.
Type	Counter
Dimensions	Source Possible Values: • n1messagenotify_command_complete • n1messagenotify_command_reject • n1n2transfer_failure_notification • t3501_expiry • nchf_spendinglimitcontrol_notify • udr_policy_data_change_notification • npcf_uepolicycontrol_create • npcf_uepolicycontrol_update • npcf_uepolicycontrol_delete
Example	ue_n1_policy_rule_conflict_total{app_kubernetes_io_instance="v4", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="ue-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="25.2.100-beta.7.0.0", application="occnp", container="ue-service", endpoint="cnc-metrics", engVersion="25.2.100-beta.7", exported_application="pcf_ueservice", helm_sh_chart="ue-service-25.2.100-beta.7", hostname="v4-pcf-ueservice-9d9fff5-cdv6l", instance="10.233.93.187:9000", io_kompose_service="v4-pcf-ueservice", job="occne-infra/occne-nf-cnc-podmonitor", microservice="pcf_ueservice", mktgVersion="25.2.100-beta.7.0.0", namespace="vega-ns4", pod="v4-pcf-ueservice-9d9fff5-cdv6l", pod_template_hash="9d9fff5", source="n1messagenotify_command_complete", vendor="Oracle"} ue_n1_policy_rule_conflict_total{app_kubernetes_io_instance="sm", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="ue-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="25.2.100-beta.8.0.0", application="occnp", container="ue-service", endpoint="cnc-metrics", engVersion="25.2.100-beta.8", exported_application="pcf_ueservice", helm_sh_chart="ue-service-25.2.100-beta.8", hostname="sm-pcf-ueservice-6bc64f5798-lw48f", instance="10.233.124.254:9000", io_kompose_service="sm-pcf-ueservice", job="occne-infra/occne-nf-cnc-podmonitor", microservice="pcf_ueservice", mktgVersion="25.2.100-beta.8.0.0", namespace="sky3-ns8", pod="sm-pcf-ueservice-6bc64f5798-lw48f", pod_template_hash="6bc64f5798", source="npcf_uepolicycontrol_update", vendor="Oracle"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-255 occnp_ue_update_guami_change_during_retryafter_cancelled_total

Field	Details
Description	This metric is used to measure the number of updates received with change in GUAMI during the retry-after time period and "retryAfter" is cancelled for the N1N2Transfer to be sent to the new AMF. This metric provides the details of the AMF to which the N1N2Transfer is being sent.
Type	Counter
Dimensions	• amfId • application • hostname • mcc • mnc
Example	occnp_ue_update_guami_change_during_retryafter_cancelled_total{amfId="010081",application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",mcc="450",mnc="05"}

Table 9-256 occnp_ue_delete_during_retryafter_total

Field	Details
Description	This metric is used to measure the number of Delete requests received from AMF for the UEPolicyAssociation during the "retryAfter" time period and the session is deleted.
Type	Counter
Dimensions	• amfId • application • hostname • mcc • mnc
Example	occnp_ue_delete_during_retryafter_total{amfId="010041",application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",mcc="450",mnc="05"}

Table 9-257 occnp_ue_http_in_request_during_retryafter_total

Field	Details
Description	This metric is used to measure the number of requests (Update/Delete/UDR/CHF notification) received for the UEPolicyAssociation during the "retryAfter" time period.
Type	Counter
Dimensions	• application • hostname • source
Example	occnp_ue_http_in_request_during_retryafter_total{application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",source="nchf_spendinglimitcontrol_notify"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-258 occnp_n1n2transfer_error_with_retryafter_seconds

Field	Details
Description	This metric is used to measure the number of N1N2Transfer error responses received with "retryAfter" timer with a valid value in payload body.
Type	Counter
Dimensions	• amfId • application • hostname • mcc • mnc • response_code
Example	occnp_n1n2transfer_error_with_retryafter_seconds_bucket{amfId="0100C1",application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",mcc="450",mnc="05",response_code="504",le="600.0"} occnp_n1n2transfer_error_with_retryafter_seconds_bucket{amfId="0100C1",application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",mcc="450",mnc="05",response_code="504",le="+Inf"} occnp_n1n2transfer_error_with_retryafter_seconds_count{amfId="0100C1",application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",mcc="450",mnc="05",response_code="504"} occnp_n1n2transfer_error_with_retryafter_seconds_sum{amfId="0100C1",application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",mcc="450",mnc="05",response_code="504"}

Table 9-259 occnp_n1n2transfer_error_retryafter_invalid_total

Field	Details
Description	This metric is used to measure the number of N1N2Transfer error responses received with invalid "retryAfter" value (that is, greater than configured max (configuration is done in advance setting) in the payload body or less than or equal to 0).
Type	Counter
Dimensions	• amfId • application • hostname • mcc • mnc • response_code • retry_after_gt_config_max • retry_after_le_zero
Example	occnp_n1n2transfer_error_retryafter_invalid_total{amfId="010041",application="pcf_ueservice",hostname="adi-pcf-ueservice-84db8dc45f-j4pvb",mcc="450",mnc="05",response_code="504",retry_after_gt_config_max="false",retry_after_le_zero="true"}

Table 9-260 occnp_ue_update_guami_change_count

Field	Details
Description	This metric is used to measure the number of updates received with change in GUAMI.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-260 (Cont.) occnp_ue_update_guami_change_count

Field	Details
Type	Counter
Dimensions	• amfSetId • application • hostname • nfSetId • amfSetIdAndRegionId • guami
Example	-

Table 9-261 occnp_ue_update_resubscription_condition_change

Field	Details
Description	This metric is used to measure the number of updates received with change in GUAMI, which resulted in discovery and further subscription.
Type	Counter
Dimensions	• amfSetId • application • hostname • nfSetId • amfSetIdAndRegionId • guami
Example	-

For more information about Dimensions, see CNC Policy Metrics.

9.10 User Service Metrics

The following table describes the User Service (User/UDR/CHF) metrics and respective dimensions:

Table 9-262 ocpm_userservice_inbound_count_total

Field	Details
Description	Total number of inbound request.
Metric Type	Counter
Dimensions	• operation_type • service_resource

Examples:

- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="post",service_resource="udr-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="get",service_resource="chf-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="get",service_resource="udr-service",} 0.0 ; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="notify",service_resource="chf-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="delete",service_resource="user-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="get",service_resource="user-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="notify",service_resource="udr-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="delete",service_resource="udr-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="terminate",service_resource="chf-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="delete",service_resource="chf-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="patch",service_resource="udr-service",} 0.0 ; Type-Counter
- ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="put",service_resource="udr-service",} 0.0 ; Type-Counter

Table 9-263 ocpm_ar_setup_total

Field	Details
Description	Track number of registration request sent to alternate route service.
Metric Type	Counter
Dimensions	• anchorFqdn • application • scheme

Examples:

- ocpm_ar_setup_total{anchorFqdn="chfanchor.allsim.svc",application="pcf_userservice",scheme="http",} 1.0 ; Type-Counter

Table 9-264 ocpm_ar_request_total

Field	Details
Description	Tracks number of alternate routing attempts to producer or consumer on Initial, Subsequent, or Notification messages.
Metric Type	Counter
Dimensions	• application • Fqdn • scheme

Examples:

- ocpm_ar_request_total{application="pcf_userservice",fqdn="udmanchor.allsim.svc",scheme="http",} 1.0 ; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-265 ocpm_ar_response_total

Field	Details
Description	Tracks response on number of alternate routing attempts to producer or consumer on Initial, Subsequent, or Notification messages.
Metric Type	Counter
Dimensions	• application • Fqdn • scheme

Examples:

- ocpm_ar_response_total{application="pcf_userservice",fqdn="udmanchor.allsim.svc",responseCode="2xx",scheme="http",} 1.0 ; Type-Counter

Table 9-266 ocpm_ar_lookup_request_total

Field	Details
Description	Track number of time alternate route lookup was done for a given scheme+FQDN.
Metric Type	Counter
Dimensions	• anchorFqdn • application • scheme

Examples:

- ocpm_ar_lookup_request_total{anchorFqdn="udmanchor.allsim.svc",application="pcf_userservice",scheme="http",} 1.0 ; Type-Counter

Table 9-267 ocpm_ar_lookup_response_total

Field	Details
Description	Tracks response codes for request to "alternateRoute" service.
Metric Type	Counter
Dimensions	• anchorFqdn • application • responseCode • scheme

Examples:

- ocpm_ar_lookup_response_total{anchorFqdn="udmanchor.allsim.svc",application="pcf_userservice",responseCode="2xx",scheme="http",} 1.0 ; Type-Counter

Table 9-268 ocpm_udr_tracking_request_total

Field	Details
Description	This metric captures all the requests sent by UDR Connector on it's communication with UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-268 (Cont.) ocpm_udr_tracking_request_total

Field	Details
Metric Type	Counter
Dimensions	• HostName • application • operation_type • nf_instance_id • nf_name • servicename_3gpp • service_resource • service_version • service_subresource • binding_level • binding_id • discovery_level • discovery_id • discovery_parameter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-268 (Cont.) ocpm_udr_tracking_request_total

Field	Details
Examples	ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",binding_id="",binding_level="",discovery_id="",discovery_parameter="",hostname="my-cnpolicy-occnp-udr-connector-7ddfc965b9-s8nwq",nf_instance_id="fe7d992b-0541-4c7d-ab84-333334444434",nf_name="nf21stub.h3-ns10.svc",operation_type="get",service_resource="policy-data",service_subresource="um-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",binding_id="",binding_level="",discovery_id="",discovery_parameter="",hostname="titans-occnp-udr-connector-694f9795d8-gmdl4",nf_instance_id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf1stub.rigelns6.svc",operation_type="lookup_subscribe",service_resource="subscription-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",binding_id="",binding_level="",discovery_id="",discovery_parameter="",hostname="conv-occnp-udr-connector-797fb77675-dpmtz",nf_instance_id="fe7d992b-0541-4c7d-ab84-555556666655",nf_name="nf11stub.ch2-ns13.svc",operation_type="subscribe",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 3.0 ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",binding_id="",binding_level="nf-set",discovery_id="",discovery_parameter="",hostname="conv-occnp-udr-connector-797fb77675-dpmtz",nf_instance_id="fe7d992b-0541-4c7d-ab84-555553333333",nf_name="nf3stub.ch2-ns13.svc",operation_type="unsubscribe",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",binding_id="",binding_level="",discovery_id="",discovery_parameter="",hostname="conv-occnp-udr-connector-797fb77675-dpmtz",nf_instance_id="fe7d992b-0541-4c7d-ab84-555550000000",nf_name="nf3stub.ch2-ns13.svc",operation_type="get",service_resource="policy-data",service_subresource="ue-policy-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-268 (Cont.) ocpm_udr_tracking_request_total

Field	Details
	set",service_version="v1",servicename_3gpp="nudr-dr" ,} 2.0

Table 9-269 ocpm_chf_tracking_request_total

Field	Details
Description	Total number of CHF tracking requests.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • nf_name • servicename_3gpp • service_resource ["subscriptions"] • service_version ["v1,v1"] • binding_level • binding_id • discovery_level • discovery_id

Table 9-270 ocpm_udr_tracking_response_total

Field	Details
Description	This metric captures all the responses received by UDR-conn on it's communication with UDR.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • nf_name • servicename_3gpp= ["nudr-dr"] • service_resource ["policy-data"] • service_version ["v1,v2"] • service_subresource [am-data, sm-data, ue-policy-set, subs-to-notify] • response_code • DataSourceType • HostName • QueryType • RequestMapping • RequestMethod • application

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-270 (Cont.) ocpm_udr_tracking_response_total

Field	Details
Examples	ocpm_udr_tracking_response_total{HostName="", application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="subscribe",response_code="2xx",service_resource="policy-data",service_subresource="",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter ocpm_udr_tracking_response_total{HostName="", application="pcf_userservice",hostname="my-cnpolicy-occnp-udr-connector-7ddfc965b9-s8nwq",nf_instance_id="fe7d992b-0541-4c7d-ab84-333334444433",nf_name="nf2stub.h3-ns10.svc",operation_type="put",response_code="3xx",service_resource="policy-data",service_subresource="sm-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ocpm_udr_tracking_response_total{HostName="", application="pcf_userservice",hostname="titans-occnp-udr-connector-694f9795d8-gmdl4",nf_instance_id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf1stub.rigelns6.svc",operation_type="lookup_subscribe",response_code="2xx",service_resource="subscription-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 ocpm_udr_tracking_response_total{HostName="", application="pcf_userservice",hostname="conv-occnp-udr-connector-797fb77675-dpmtz",nf_instance _id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf2stub.ch2-ns13.svc",operation_type="subscribe",response_code="2xx",service_resource=" policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 3.0 ocpm_udr_tracking_response_total{HostName="", application="pcf_userservice",hostname="conv-occnp-udr-connector-797fb77675-dpmtz",nf_instance _id="fe7d992b-0541-4c7d-ab84-555553333333",nf_name="nf3stub.ch2-ns13.svc",operation_type="get",response_code="2xx",service_resource="policy -data",service_subresource="am-data",service_version="v1",servicename_3gpp="nudr-dr",} 2.0 ocpm_udr_tracking_response_total{HostName="", application="pcf_userservice",hostname="conv-occnp-udr-connector-797fb77675-dpmtz",nf_instance _id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf1stub.ch2-ns13.svc",operation_type="unsubscribe",response_code="2xx",service_resource ="policy-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-270 (Cont.) ocpm_udr_tracking_response_total

Field	Details
	data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 11.0

Table 9-271 ocpm_udr_tracking_request_timeout_total

Field	Details
Description	This metric captures all the requests sent by UDR Connector on it's communication with UDR which ends up with timeout.
Metric Type	Counter
Dimensions	• Hostname • application • nf_instance_id • nf_name • operation_type • service_resource • service_subresource • service_version • servicename_3gpp
Examples	ocpm_udr_tracking_request_timeout_total{HostName="",application="pcf_userservice",hostname="conv-occnp-udr-connector-66c6f47c4f-45tjf",nf_instance_id="fe7d992b-0541-4c7d-ab84-555553333333",nf_name="nf3stub.ch2-ns13.svc",operation_type="lookup_subscribe",service_resource="subscription-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} ocpm_udr_tracking_request_timeout_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="patch",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 0.0; Type-Counter

Table 9-272 ocpm_chf_tracking_response_total

Field	Details
Description	Total number of CHF tracking responses.
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-272 (Cont.) ocpm_chf_tracking_response_total

Field	Details
Dimensions	• operation_type • nf_instance_id • nf_name • servicename_3gpp= ["nchf-spendinglimitcontrol"] • service_resource ["subscriptions"] • service_version ["v1"] • response_code

Table 9-273 ocpm_chf_tracking_request_timeout_total

Field	Details
Description	Total number of CHF request timeouts.
Metric Type	-
Dimensions	• Hostname • application • nf_instance_id • nf_name • operation_type • service_resource • service_subresource • service_version • servicename_3gpp

Table 9-274 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Metric Type	Gauge
Dimensions	• Service Name • Pod Name

Table 9-275 occnp_policy_userservice_overall_processing_time_seconds

Field	Details
Description	User service overall processing time. **Note**: Default name used when there is no custom name available is data_repository_invocations.
Type	Summary

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-275 (Cont.) occnp_policy_userservice_overall_processing_time_seconds

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Example	-

Table 9-276 occnp_policy_userservice_overall_processing_time_seconds_count

Field	Details
Description	User service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-277 occnp_policy_userservice_overall_processing_time_seconds_max

Field	Details
Description	User service overall processing time.
Type	Gauge
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-278 occnp_policy_userservice_overall_processing_time_seconds_sum

Field	Details
Description	User service overall processing time.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-278 (Cont.) occnp_policy_userservice_overall_processing_time_seconds_sum

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-279 occnp_udr_nf_profile_cookie_enabled_total

Field	Details
Description	This metric is incremented when cached NF profile is used and the feature is enabled.
Metric Type	Counter
Dimensions	• HostName • application • hostname • nf_name • operation_type • service_resource • service_subresource • service_version • servicename_3gpp
Example	occnp_udr_nf_profile_cookie_enabled_total{HostName="",application="pcf_userservice",hostname="pcf-occnp-udr-connector-5dc478c84c-78k9p",nf_instance_id="fe7d992b-0541-4c7d-ab84-555550000000",nf_name="nf1stub.s-galeleo.svc",operation_type="GET",service_resource="policy-data",service_subresource="ue-policy-set",service_version="v1",servicename_3gpp="nudr-dr",} 3.0

Examples:

- occnp_udr_nf_profile_cookie_enabled_total{HostName="",application="pcf_userservice",hostname="pcf-occnp-udr-connector-5dc478c84c-78k9p",nf_instance_id="fe7d992b-0541-4c7d-

Copyright © 2019, 2026, Oracle and/or its affiliates.

ab84-555550000000",nf_name="nf1stub.s-galeleo.svc",operation_type="GET",service_resource="policy-data",service_subresource="ue-policy-set",service_version="v1",servicename_3gpp="nudr-dr",} 3.0

Table 9-280 occnp_udr_use_related_resource

Field	Details
Description	This metric is incremented when a related resource is used and feature is enabled.
Metric Type	Counter
Dimensions	• HostName • application • hostname • nf_name • operation_type • service_resource • service_subresource • service_version • servicename_3gpp
Example	occnp_udr_use_related_resource_total{HostName="",application="pcf_userservice",hostname="pcf-occnp-udr-connector-5dc478c84c-78k9p",nf_instance_id="fe7d992b-0541-4c7d-ab84-555550000000",nf_name="nf1stub.s-galeleo.svc",operation_type="GET",service_resource="policy-data",service_subresource="ue-policy-set",service_version="v1",servicename_3gpp="NUDR_DR",} 1.0

Table 9-281 error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter
Dimensions	• application • applicationException • wrapped_exception
Example	occnp_error_handler_in_total{application="pcf_userservice",application_exception="JavaException",status="502",wrapped_exception="ServiceException",} 4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-282 error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter
Dimensions	• application • applicationException • error_type • operation • origin • rule_name • source_interface • target_interface • wrapped_exception
Example	occnp_error_handler_exec_total{application="pcf_userservice",application_exception="JavaException",error_type="INTERNAL",operation="NOTIFY",origin="JAVA",rule_name="REJECT_WITH_ENHANCED_DETAIL",source_interface="UDR",status="502",target_interface="POLICY",wrapped_exception="ServiceException",} 4.0

Table 9-283 error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter
Dimensions	• application • applicationException • error_resolved • wrapped_exception
Example	occnp_error_handler_out_total{application="pcf_userservice",application_exception="JavaException",error_resolved="true",status="400",wrapped_exception="ServiceException",} 4.0

Table 9-284 occnp_late_arrival_rejection_total

Field	Details
Description	This metric is pegged whenever User Service receives a request, and it is canceled because it is already stale.
Type	Counter
Dimensions	• Operation Type Accepts values such as GET, POST, and DELETE • application Accepted values such as UDR-connector and CHF-connector
Example	-

Table 9-285 occnp_late_processing_rejection_total

Field	Details
Description	This metric is pegged whenever User Service receives a request, and it is canceled because it has gone stale while processing it.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-285 (Cont.) occnp_late_processing_rejection_total

Field	Details
Type	Counter
Dimensions	• Operation Type Accepts values such as LOOKUP, UPDATE, SUBSCRIBE, UNSUBSCRIBE, LOOKUPSUBSCRIBE, GET, PUT, POST, PATCH, and DELETE • application Accepted values such as UDR-connector and CHF-connector • Stage Accepts the following values: – PRE_PROCESS("Before processing request") – PRE_UDR("Before sending to external UDR") – POST_UDR("After getting response from external UDR") – PRE_CHF("Before sending to external CHF") – POST_CHF("After getting response from external CHF")
Example	-

Table 9-286 occnp_immrep_request_total

Field	Details
Description	This metric is incremented in the following scenarios related to immediate reporting and fallback procedures with the UDR: • Scenario 1: When a discovered UDR profile supports immediate reporting, and a POST request is sent to the UDR with the immRep parameter set to true. • Scenario 2: When a discovered UDR profile supports immediate reporting, and a POST request is sent with immRep set to true, but subscriber data is not obtained. In this case, if fallback is configured, PCF triggers a GET towards UDR and this will also peg the metric. • Scenario 3: When the immediate report feature is enabled and a subscription is successfully created, but subscriber data is not obtained. The fallback logic initiates a GET procedure, which ultimately fails, leading to an unsubscribe request being sent to the UDR to terminate the previously created subscription. This unsubscribe request also pegs this metric.
Type	Counter
Dimensions	• application • container • endpoint • exported_application • hostname • instance • io_kompose_service • job • microservice • namespace • nf_name • operation_type • pod • pod_template_hash • service_subresource • vendor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-286 (Cont.) occnp_immrep_request_total

Field	Details
Example	occnp_immrep_request_total{app_kubernetes_io_instance="ocpcf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="25.2.100-ocngf-pre-dev-prodigies.0.0", application="occnp", container="user-service", endpoint="cnc-metrics", engVersion="25.2.100-ocngf-pre-dev-prodigies", exported_application="pcf_userservice", helm_sh_chart="user-service-25.2.100-ocngf-pre-dev-prodigies", hostname="ocpcf-occnp-udr-connector-86c5786fff-dqzfh", instance="10.233.101.111:9000", io_kompose_service="ocpcf-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="25.2.100-ocngf-pre-dev-prodigies.0.0", namespace="hi-ns01", nf_name="10.148.211.41", operation_type="post", pod="ocpcf-occnp-udr-connector-86c5786fff-dqzfh", pod_template_hash="86c5786fff", service_subresource="am-data", vendor="Oracle"}

Table 9-287 occnp_immrep_response_total

Field	Details
Description	This metric shall be incremented after receiving UDR response for immediate Report. **Note**: This metric will only be pegged if the discovered UDR has immediate reporting capability.
Type	Counter
Dimensions	• application • container • endpoint • exported_application • hostname • imm_reports_present • immediate_report_pcc • instance • io_kompose_service • job • microservice • namespace • operation_type • pod • pod_template_hash • response_code • service_subresource • vendor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-287 (Cont.) occnp_immrep_response_total

Field	Details
Example	occnp_immrep_response_total{app_kubernetes_io_instance="ocpcf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="25.2.100-ocngf-pre-dev-prodigies.0.0", application="occnp", container="user-service", endpoint="cnc-metrics", engVersion="25.2.100-ocngf-pre-dev-prodigies", exported_application="pcf_userservice", helm_sh_chart="user-service-25.2.100-ocngf-pre-dev-prodigies", hostname="ocpcf-occnp-udr-connector-86c5786fff-dqzfh", imm_reports_present="true", immediate_report_pcc="true", instance="10.233.101.111:9000", io_kompose_service="ocpcf-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="25.2.100-ocngf-pre-dev-prodigies.0.0", namespace="hi-ns01", nf_name="10.148.211.41", operation_type="post", pod="ocpcf-occnp-udr-connector-86c5786fff-dqzfh", pod_template_hash="86c5786fff", response_code="2xx", service_subresource="am-data", vendor="Oracle"}

Table 9-288 occnp_immrep_skipped_total

Field	Details
Description	This metric is incremented when PCF from a prior transaction with the same UDR for the same subscriber finds out that the Immediate Report feature is not supported by the UDR and hence skips the feature during a subsequent session creation. This functionality is dependent on discovery optimization feature. It can be enabled by setting *UDR_GET_USE_RELATED_RESOURCE* flag as true. For more information on this flag, see PCF User Connector.
Type	Counter
Dimensions	• application • container • endpoint • exported_application • hostname • instance • io_kompose_service • job • microservice • namespace • operation_type • pod • pod_template_hash • service_subresource • vendor

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-288 (Cont.) occnp_immrep_skipped_total

Field	Details
Example	occnp_immrep_skipped_total{app_kubernetes_io_instance="ocpcf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="25.2.100-ocngf-pre-dev-prodigies.0.0", application="occnp", container="user-service", endpoint="cnc-metrics", engVersion="25.2.100-ocngf-pre-dev-prodigies", exported_application="pcf_userservice", helm_sh_chart="user-service-25.2.100-ocngf-pre-dev-prodigies", hostname="ocpcf-occnp-udr-connector-86c5786fff-dqzfh", instance="10.233.101.111:9000", io_kompose_service="ocpcf-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="25.2.100-ocngf-pre-dev-prodigies.0.0", namespace="hi-ns01", nf_name="10.148.211.41", pod="ocpcf-occnp-udr-connector-86c5786fff-dqzfh", pod_template_hash="86c5786fff", service_subresource="ue-policy-set", vendor="Oracle"}

For more information about Dimensions, see CNC Policy Metrics.

9.11 Diameter Connector Service Metrics

The following table describes the Diameter Connector Service metrics and respective dimensions:

Table 9-289 ocpm_ingress_request_total

Field	Details
Description	Total number of ingress requests received.
Metric Type	Counter
Dimensions	• operation_type • dnn • nf_instance_id • servicename_3gpp

Examples:

- ocpm_ingress_request_total{apn="",nf_instance_id="AF.xxx.com",operation_type="create", servicename_3gpp="rx",} 5.0 ; Type-Counter

Table 9-290 ocpm_ingress_response_total

Field	Details
Description	Total number of ingress responses.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • dnn • servicename_3gpp • response_code

Examples:

Copyright © 2019, 2026, Oracle and/or its affiliates.

- ocpm_ingress_response_total{apn="",nf_instance_id="ocpcf",operation_type="create",response_code="2xxx",servicename_3gpp="rx",} 2.0 ; Type-Counter

Table 9-291 ocpm_egress_request_total

Field	Details
Description	Total number of egress requests received.
Metric Type	Counter
Dimensions	• operation_type • dnn • nf_instance_id • servicename_3gpp

Examples:

- ocpm_egress_request_total{nf_instance_id="AF.xxx.com",operation_type="update_notify",servicename_3gpp="rx",} 1.0 ; Type-Counter

Table 9-292 ocpm_egress_response_total

Field	Details
Description	Total number of egress responses.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • dnn • servicename_3gpp • response_code

Example:

- ocpm_egress_response_total{latency="3",nf_instance_id="AF.xxx.com",operation_type="update_notify",response_code="2xxx",servicename_3gpp="rx",} 1.0 ; Type-Counter

Table 9-293 occnp_diam_pending_requests

Field	Details
Description	Track the total pending Diameter messages
Type	Gauge
Dimension	• namespace • pod
Example	-

Table 9-294 occnp_http_pending_requests

Field	Details
Description	Track the total pending HTTP messages.
Type	Gauge
Dimension	• namespace • pod
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-295 ocpm_egress_response_total

Field	Details
Description	Total number of egress responses.
Metric Type	Counter
Dimensions	• operation_type • nf_instance_id • dnn • servicename_3gpp • response_code

Table 9-296 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Metric Type	Gauge
Dimensions	• Service Name • Pod Name

Table 9-297 occnp_diam_connector_overall_processing_time_seconds

Field	Details
Description	Diameter Connector service overall processing time.
Type	Summary
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-298 occnp_diam_connector_overall_processing_time_seconds_max

Field	Details
Description	Diameter Connector service overall processing time. **Note**: Default name used when there is no custom name available is data_repository_invocations.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-298 (Cont.) occnp_diam_connector_overall_processing_time_seconds_max

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Example	• occnp_diam_connector_overall_processing_time_seconds_max{error="none",exception="none",method="POST",outcome="SERVER_ERROR", status="500",uri="/smservicenotify/tdf/createsession",} 0.0 • occnp_diam_connector_overall_processing_time_seconds_max{error="none",exception="none",method="POST",outcome="CLIENT_ERROR", status="400",uri="/smservicenotify/tdf/createsession" • occnp_diam_connector_overall_processing_time_seconds_max{error="none",exception="none",method="POST",outcome="SUCCESS", status="200",uri="/smservicenotify/tdf/createsession",} 0.0

Table 9-299 occnp_diam_connector_overall_processing_time_seconds_count

Field	Details
Description	Diameter Connector service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Examples	• occnp_diam_connector_overall_processing_time_seconds_count{error="none",exception="none",method="POST",outcome="SERVER_ERROR",status="500",uri="/smservicenotify/tdf/createsession",} 2.0 • occnp_diam_connector_overall_processing_time_seconds_count{error="none",exception="none",method="POST",outcome="SUCCESS",status="200",uri="/smservicenotify/tdf/createsession",} 2.0

Table 9-300 occnp_diam_connector_overall_processing_time_seconds_sum

Field	Details
Description	Diameter Connector service overall processing time.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-300 (Cont.) occnp_diam_connector_overall_processing_time_seconds_sum

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Examples	• occnp_diam_connector_overall_processing_time_seconds_sum{error="none",exception="none",method="POST", outcome="SERVER_ERROR",status="500",uri="/smservicenotify/tdf/createsession",} 0.055592208 • occnp_diam_connector_overall_processing_time_seconds_sum{error="none",exception="none",method="POST", outcome="SUCCESS",status="200",uri="/smservicenotify/tdf/createsession",} 2.993459709

Table 9-301 occnp_stale_diam_request_cleanup_total

Field	Details
Description	This metric is pegged whenever Diameter Connector receives a Diameter request, and it is canceled either because it is already stale (late arrival request), or it has gone stale while processing it (late processing request).
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-301 (Cont.) occnp_stale_diam_request_cleanup_total

Field	Details
Dimensions	• App Type : Rx, Gx, Sy • Message Type : AAR, RAR, STR • Destination Host • Destination Realm • Cause • Stage The sage dimension indicates at which stage the request became stale. The following are the possible values for Stage dimension for late arrival requests: – PRE_AAR_REQUEST: The AAR request arrived at Diameter Connector is already stale, and no further processing happened. – PRE_RAR_REQUEST: The request arrived from SM Service for notification is already stale and no further processing happened. – PRE_SLR_REQUEST: The request arrived stale from PDS for OCS Fetch, no further processing happened. – PRE_STR_REQUEST: The request arrived stale from PDS for termination, no further processing happened. – PRE_ASR_REQUEST: The request arrived stale from SM Service for termination, no further processing happened. – PRE_SNR_REQUEST: The request arrived stale from SM Service for termination, no further processing happened. The following are the possible values for Stage dimension for late processing requests: – PRE_SM_REQUEST: The request went stale before contacting SM Service. – POST_SM_REQUEST: The request went stale after receiving response from SM Service. – PRE_DIAM_GW_REQUEST: Before sending any request towards Diameter Gateway. The following are the possible values for Stage dimensions for TDF stale session: – PRE_TSR_REQUEST : TSR request late arrived or staled while processing. – PRE_RAR_REQUEST: RAR request late arrived or staled while processing – PRE_RAR_TERMINATE_REQUEST : RAR Terminate request late arrived or staled while processing. – PRE_SD_CCR_UPDATE_REQUEST : CCR-U request late arrived or staled while processing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-301 (Cont.) occnp_stale_diam_request_cleanup_total

Field	Details
	– PRE_SD_CCR_TERMINATE_REQUEST : CCR-T request late arrived or staled while processing. – PRE_SM_REQUEST: Request got staled just before sending request to SM. – POST_SM_REQUEST : Request got staled just after getting response from SM. – PRE_DIAM_GW_REQUEST : Request got staled just before sending request to Diameter Gateway.

Table 9-302 occnp_stale_http_request_cleanup_total

Field	Details
Description	This metric is pegged whenever Diameter Connector receives a HTTP request, and it is canceled either because it is already stale (late arrival request), or it has gone stale while processing it (late processing request).
Metric Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-302 (Cont.) occnp_stale_http_request_cleanup_total

Field	Details
Dimensions	• Service Resource • Operation Type • Stage The sage dimension indicates at which stage the request became stale. The following are the possible values for Stage dimension for late arrival requests: – PRE_AAR_REQUEST: The AAR request arrived at Diameter Connector is already stale, and no further processing happened. – PRE_RAR_REQUEST: The request arrived from SM Service for notification is already stale and no further processing happened. – PRE_SLR_REQUEST: The request arrived stale from PDS for OCS Fetch, no further processing happened. – PRE_STR_REQUEST: The request arrived stale from PDS for termination, no further processing happened. – PRE_ASR_REQUEST: The request arrived stale from SM Service for termination, no further processing happened. – PRE_SNR_REQUEST: The request arrived stale from SM Service for termination, no further processing happened. The following are the possible values for Stage dimension for late processing requests: – PRE_SM_REQUEST: The request went stale before contacting SM Service. – POST_SM_REQUEST: The request went stale after receiving response from SM Service. – PRE_DIAM_GW_REQUEST: Before sending any request towards Diameter Gateway. The following are the possible values for Stage dimensions for TDF stale session: – PRE_TSR_REQUEST : TSR request late arrived or staled while processing. – PRE_RAR_REQUEST: RAR request late arrived or staled while processing – PRE_RAR_TERMINATE_REQUEST : RAR Terminate request late arrived or staled while processing. – PRE_SD_CCR_UPDATE_REQUEST : CCR-U request late arrived or staled while processing. – PRE_SD_CCR_TERMINATE_REQUEST : CCR-T request late arrived or staled while processing.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-302 (Cont.) occnp_stale_http_request_cleanup_total

Field	Details
	– PRE_SM_REQUEST: Request got staled just before sending request to SM. – POST_SM_REQUEST : Request got staled just after getting response from SM. – PRE_DIAM_GW_REQUEST : Request got staled just before sending request to Diameter Gateway.

Table 9-303 diam_avp_dropped

Field	Details
Description	This metric is incremented when the value of `ratTypeNRRedCapEnabled` parameter in Diameter Connector API is `false` or the **Redcap Support For Rx Interface** field is disabled in CNC Console. The metric is incremented only when the RATType received in SM CREATE or SM UPDATE request for Rx sessions has NR_REDCAP value.
Metric Type	Counter
Dimensions	• Message Type Example values: AAA, RAR • AVP Name • AVP Value • Servicename_3gpp
Example	• occnp_diam_avp_dropped_total{avp_name="RAT-Type",avp_value="NR_REDCAP",msg_type="AAA",servicename_3gpp="rx",} 1.0 • occnp_diam_avp_dropped_total{avp_name="RAT-Type",avp_value="NR_REDCAP",msg_type="RAR",servicename_3gpp="rx",} 1.0

For more information about Dimensions, see CNC Policy Metrics.

9.12 Diameter Gateway Metrics

The following table describes the Diameter Gateway metrics and respective dimensions:

Table 9-304 occnp_diam_conn_network

Field	Details
Description	Tracks active diameter connections with network peers.
Type	Gauge
Dimension	• direction • peerHost • peerRealm

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-304 (Cont.) occnp_diam_conn_network

Field	Details
Example	-

Table 9-305 occnp_diam_conn_app_network

Field	Details
Description	Tracks active diameter connections with network peers that support given application ID.
Type	Gauge
Dimension	• appId • applicationName • peerHost • peerRealm
Examples	-

Example:

Table 9-306 occnp_diam_request_network_total

Field	Details
Description	Tracks total number of request messages of given command code to or from network
Type	Counter
Dimension	• appId • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • retry • retryReason • immediatePeerHost • immediatePeerRealm

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-306 (Cont.) occnp_diam_request_network_total

Field	Details
Example	• occnp_diam_request_network_total{appId="16777217",cmdCode="308",destHost="",destRealm="xxxx.com",direction="out",msgType="SNR",origHost="pcrf-core",origRealm="xxxx.com",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 2.0 ; Type-Counter • occnp_diam_request_network_total{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",destRealm="telecom.com",direction="out",msgType="TSR",origHost="oc-diam-connector",origRealm="oacle.com",retry="false",retryReason="",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 1.0 • occnp_diam_request_network_total{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",destRealm="telecom.com",direction="out",msgType="RAR",origHost="oc-diam-connector",origRealm="oacle.com",retry="false",retryReason="",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 2.0 • occnp_diam_request_network_total{appId="16777303",cmdCode="272",destHost="oc-diam-connector",destRealm="oacle.com",direction="in",msgType="CCR",origHost="tdf.telecom.com",origRealm="oacle.com",retry="false",retryReason="",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 1.0

Table 9-307 occnp_diam_response_network_total

Field	Details
Description	Tracks total number of answer messages of given command code to or from network.
Type	Counter
Dimension	• appId • cmdCode • reqDestHost • reqDestRealm • direction • msgType • reqOrigHost • reqOrigRealm • responseCode • immediatePeerHost • immediatePeerRealm

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-307 (Cont.) occnp_diam_response_network_total

Field	Details
Example	• occnp_diam_response_network_total{appId="16777217",cmdCode="308",reqDestHost="udr.xxxx.com",reqDestRealm="xxxx.com",direction="in",msgType="SNA",reqOrigHost="pcrf-core",reqOrigRealm="xxxx.com",responseCode="2001",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 2.0 ; Type-Counter • occnp_diam_response_network_total{appId="16777303",cmdCode="8388637",direction="in",msgType="TSA",reqDestHost="tdf.telecom.com",reqDestRealm="oacle.com",reqOrigHost="",reqOrigRealm="",responseCode="2001",retry="false",retryReason="",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 1.0 • occnp_diam_response_network_total{appId="16777303",cmdCode="258",direction="in",msgType="RAA",reqDestHost="tdf.telecom.com",reqDestRealm="oacle.com",reqOrigHost="",reqOrigRealm="",responseCode="2001",retry="false",retryReason="",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 2.0 • occnp_diam_response_network_total{appId="16777303",cmdCode="272",direction="out",msgType="CCA",reqDestHost="oc-diam-connector",reqDestRealm="oacle.com",reqOrigHost="",reqOrigRealm="",responseCode="2001",retry="false",retryReason="",immediatePeerHost="pgw.oracle.com",immediatePeerRealm="oracle.com"} 1.0

Table 9-308 occnp_diam_conn_local

Field	Details
Description	Tracks active diameter connections with local services.
Type	Gauge
Dimension	• direction • peerHost • peerRealm
Example	-

Table 9-309 occnp_diam_conn_app_local

Field	Details
Description	Tracks active diameter connections with local services that support given application id. Increment this metric for each application Id supported over connection, such as intersection of application ID in CER and CEA.
Type	Gauge
Dimension	• appId • appType • applicationName • peerHost • peerRealm
Example	

Table 9-310 occnp_diam_request_local_total

Field	Details
Description	Tracks total number of request messages of given command code to or from local service

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-310 (Cont.) occnp_diam_request_local_total

Field	Details
Type	Counter
Dimension	• appId • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqDestHost • retry • retryReason
Examples	• occnp_diam_request_local_total{appId="16777303",appType="",cmdCode="8388637",destHost="pcrf-core",destRealm="xxxx.com",direction="out",msgType="TSR",origHost="local-pcrf",origRealm=local.com",reqDestHost="tdf.xxxx.com",reqDestRealm="tdf.xxxx.com",reqOrigHost="pcrf-core",reqOrigRealm="xxxx.com",} 1.0 1658786894876 • occnp_diam_request_local_total{appId="16777217",cmdCode="308",destHost="",destRealm="xxxx.com",direction="in",msgType="SNR",origHost="pcrf-core",origRealm="xxxx.com",} 2.0 ; Type-Counter • occnp_diam_request_local_total{appId="16777217",cmdCode="306",destHost="",destRealm="xxxx.com",direction="in",msgType="UDR",origHost="pcrf-core",origRealm="xxxx.com",} 5.0 ; Type-Counter

Table 9-311 occnp_diam_response_local_total

Field	Details
Description	Tracks total number of answer messages of given command code to or from local service.
Type	Counter
Dimension	• appId • cmdCode • reqDestHost • reqDestRealm • direction • msgType • reqOrigHost • reqOrigRealm • responseCode
Examples	• occnp_diam_response_local_total{appId="16777217",cmdCode="308",reqDestHost="udr.xxxx.com",reqDestRealm="xxxx.com",direction="out",msgType="SNA",reqOrigHost="pcrf-core",rqOrigRealm="xxxx.com",responseCode="2001",} 2.0 ; Type-Counter • occnp_diam_response_local_total{appId="16777217",cmdCode="306",reqDestHost="udr.xxxx.com",reqDestRealm="xxxx.com",direction="out",msgType="UDA",reqOrigHost="pcrf-core",reqOrigRealm="xxxx.com",responseCode="2001",} 3.0 ; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-312 occnp_diam_request_inter_total

Field	Details
Description	Tracks total number of request messages of given command code to or from host services
Type	Counter
Dimension	• appId • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • retry • retryReason

Table 9-313 occnp_http_out_conn_request_total

Field	Details
Description	Total number of http connection requests.
Type	Counter
Dimension	• operationType • serviceResource • serviceVersion • servicename3gpp
Example	occnp_http_out_conn_request_total{operationType="read",serviceResource="Binding",service_version="v1",servicename3gpp="DiameterGateway",} 1.0 ; Type-Counter

Table 9-314 occnp_http_out_conn_response_total

Field	Details
Description	Total number of http connection responses.
Type	Counter
Dimension	• latency • operationType • serviceResource • serviceVersion • servicename3gpp
Example	occnp_http_out_conn_response_total{latency="9",operationType="read",responseCode="2xx",serviceResource="Binding",serviceVersion="v1",servicename3gpp="DiameterGateway",} 1.0 ; Type-Counter

Table 9-315 diam_overload_msg_reject_total

Field	Details
Description	Total number of messages rejected due to overload control.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-315 (Cont.) diam_overload_msg_reject_total

Field	Details
Dimension	• priority • response_code • destHost • destRealm • origHost • origRealm • appId • cmdCode • msgType

Table 9-316 diam_controlled_shutdown_message_reject_total

Field	Details
Description	Indicates failure count because of forced shutdown feature.
Type	Counter
Dimension	• operationalState • responseCode • destHost • destRealm • origHost • origRealm • appId • cmdCode • msgType • direction
Example	diam_controlled_shutdown_message_reject_total{msgType="Gx_CCR_I",appId="16777238",cmdCode="272",destHost="",destRealm="xxxx.com",operationalState="PARTIAL_SHUTDOWN",origHost="pgw.xxxx.com",origRealm="test.example.com",responseCode="5012",} 1.0

Table 9-317 occnp_diam_overload_message_reject_total

Field	Details
Description	Indicates the number of messages rejected due to overload.
Type	Counter
Dimension	• priority • response_code • destHost • destRealm • origHost • origRealm • appId • cmdCode • msgType • loadLevel

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-317 (Cont.) occnp_diam_overload_message_reject_total

Field	Details
Example	occnp_diam_overload_message_reject_total{appId="16777236",cmdCode="265",destHost="",destRealm="xxxx.com",msgType="request",origHost="diamcliaf.xxxx.com",origRealm="test.example.com",priority="12",responseCode="3004",} 1.0

Table 9-318 occnp_diam_congestion_message_reject_total

Field	Details
Description	Indicates the number of messages rejected due to congestion.
Type	Counter
Dimension	• appId • cmdCode • destHost • destRealm • msgType • origHost • origRealm • responseCode • direction • priority • drmp • ocMsgPriority • congestion_level
Examples	• occnp_diam_congestion_message_reject_total{appId="16777238", cmdCode="272", congestion_level="2",destHost="", destRealm="xxxx.com", drmp="10", ocMessagePriority="20", origHost="pgw1.ora.com", origRealm="ora.com", msgType="request", priority="20", responseCode="3004"} 50.0 • occnp_diam_congestion_message_reject_total{appId="16777238",cmdCode="272",destHost="pcrf-core",destRealm="xxxx.com",msgType="request",origHost="diamclipgw.xxxx.com",origRealm="xxxx.com",priority="11",responseCode="3004",} 38.0; Type-Counter • occnp_diam_congestion_message_reject_total{appId="16777238",cmdCode="272",destHost="pcrf-core",destRealm="xxxx.com",msgType="request",origHost="diamclipgw.xxxx.com",origRealm="xxxx.com",priority="10",responseCode="3004",} 61.0; Type-Counter • occnp_diam_congestion_message_reject_total{appId="16777238",cmdCode="272",destHost="pcrf-core",destRealm="xxxx.com",msgType="request",origHost="diamclipgw.xxxx.com",origRealm="xxxx.com",priority="11",responseCode="3002",} 8.0 Type-Counter

Table 9-319 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimension	• Service Name • Pod Name

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-320 occnp_pod_resource_congestion_state

Field	Details
Description	Indicates the pod congestion state.
Type	Gauge
Dimension	type
Examples	• occnp_pod_congestion_state 1.0; Type-Gauge • occnp_pod_resource_congestion_state{type="memory",} 1.0; Type-Gauge • occnp_pod_resource_congestion_state{type="cpu",} 0.0; Type-Gauge • occnp_pod_resource_congestion_state{type="queue",} 0.0; Type-Gauge • occnp_pod_resource_stress{type="memory",} 41.0; Type-Gauge • occnp_pod_resource_stress{type="cpu",} 0.0; Type-Gauge • occnp_pod_resource_stress{type="queue",} 0.0; Type-Gauge

Table 9-321 occnp_diameter_outstanding_msg_count

Field	Details
Description	Provides an instantaneous number of outstanding diameter messages in the queue.
Type	Gauge
Dimension	NA
Examples	occnp_diameter_outstanding_msg_count 10.0

Table 9-322 occnp_diam_response_latency_seconds_count

Field	Details
Description	Tracks latency of all outgoing requests from Diameter Gateway. This provides information on latency time for any calls made by Diameter Gateway towards any network peers or internal back end services.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost
Examples	• occnp_diam_response_latency_seconds_count{appId="16777236",cmdCode="265",destHost="pcrf-core",msgType="AAA-I",origHost="af.xxxx.com",} 5.0 • occnp_diam_response_latency_seconds_count{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",msgType="TSA",origHost="oc-diam-connector",} 1.0 • occnp_diam_response_latency_seconds_count{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Update",origHost="oc-diam-connector",} 1.0 • occnp_diam_response_latency_seconds_count{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Terminate",origHost="oc-diam-connector",} 1.0 • occnp_diam_response_latency_seconds_count{appId="16777303",cmdCode="272",destHost="oc-diam-connector",msgType="CCA-T",origHost="tdf.telecom.com",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-323 occnp_diam_response_latency_seconds_bucket

Field	Details
Description	Tracks latency of all outgoing requests from Diameter Gateway. This provides information on latency time for any calls made by Diameter Gateway towards any network peers or internal back end services.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost • le
Examples	• occnp_diam_response_latency_seconds_bucket{appId="0",cmdCode="280",destHost="pgw.xxxx.com",msgType="",origHost="oc-diam-gateway-client",le="0.002",} 18.0 • occnp_diam_response_latency_seconds_bucket{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",msgType="TSA",origHost="oc-diam-connector",le="0.001",} 0.0 • occnp_diam_response_latency_seconds_bucket{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Update",origHost="oc-diam-connector",le="0.001",} 0.0 • occnp_diam_response_latency_seconds_bucket{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Terminate",origHost="oc-diam-connector",le="0.001",} 0.0 • occnp_diam_response_latency_seconds_bucket{appId="16777303",cmdCode="272",destHost="oc-diam-connector",msgType="CCA-T",origHost="tdf.telecom.com",le="0.001",} 0.0

Table 9-324 occnp_diam_response_latency_seconds_sum

Field	Details
Description	Tracks latency of all incoming requests towards Diameter Gateway. This provides an overall time tracking latency for any request towards Diameter Gateway.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-324 (Cont.) occnp_diam_response_latency_seconds_sum

Field	Details
Examples	• occnp_diam_response_latency_seconds_sum{appId="16777236",cmdCode="265",destHost="pcrf-core",msgType="AAA-I",origHost="af.xxxx.com",} 1.662 • occnp_diam_response_latency_seconds_sum{appId="16777303",cmdCode="258",destHost="tdf1.oacle.com",msgType="RAA-Update",origHost="ocpcf",} 0.013 • occnp_diam_response_latency_seconds_sum{appId="16777236",cmdCode="265",destHost="pcrf-core",msgType="AAA-I",origHost="af.xxxx.com",} 1.662 • occnp_diam_response_latency_seconds_sum{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",msgType="TSA",origHost="oc-diam-connector",} 0.004 • occnp_diam_response_latency_seconds_sum{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Update",origHost="oc-diam-connector",} 0.004 • occnp_diam_response_latency_seconds_sum{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Terminate",origHost="oc-diam-connector",} 0.004 • occnp_diam_response_latency_seconds_sum{appId="16777303",cmdCode="272",destHost="oc-diam-connector",msgType="CCA-T",origHost="tdf.telecom.com",} 0.475

Table 9-325 occnp_diam_response_latency_seconds_max

Field	Details
Description	Tracks latency of all incoming requests towards Diameter Gateway. This provides an overall time tracking latency for any request towards Diameter Gateway.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost
Examples	• occnp_diam_response_latency_seconds_max{appId="16777238",cmdCode="272",destHost="pcrf-core",msgType="CCA-T",origHost="pgw.xxxx.com",} 0.312 • occnp_diam_response_latency_seconds_max{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Update",origHost="oc-diam-connector",} 0.0 • occnp_diam_response_latency_seconds_max{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",msgType="TSA",origHost="oc-diam-connector",} 0.0 • occnp_diam_response_latency_seconds_max{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Terminate",origHost="oc-diam-connector",} 0.0 • occnp_diam_response_latency_seconds_max{appId="16777303",cmdCode="272",destHost="oc-diam-connector",msgType="CCA-T",origHost="tdf.telecom.com",} 0.0

Table 9-326 occnp_diam_service_overall_processing_time_seconds_sum

Field	Details
Description	Tracks latency of all incoming requests towards Diameter Gateway. This provides an overall time tracking latency for any request towards Diameter Gateway.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-326 (Cont.) occnp_diam_service_overall_processing_time_seconds_sum

Field	Details
Examples	• occnp_diam_service_overall_processing_time_seconds_sum{appId="16777303", cmdCode="8388637",destHost="tdf1.oacle.com",msgType="TSA",origHost="ocpcf",} 0.607 • occnp_diam_service_overall_processing_time_seconds_sum{appId="16777303"cmdCode="258",destHost="tdf1.oacle.com",msgType="RAA-Terminate",origHost="ocpcf",} 0.04 • occnp_diam_service_overall_processing_time_seconds_sum{appId="16777303",cmdCode="272",destHost="oc-diam-connector",msgType="CCA-T",origHost="tdf.telecom.com",} 0.479

Table 9-327 occnp_diam_service_overall_processing_time_seconds_max

Field	Details
Description	Tracks latency of all incoming requests towards Diameter Gateway. This provides an overall time tracking latency for any request towards Diameter Gateway.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost
Examples	• occnp_diam_service_overall_processing_time_seconds_max{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",msgType="TSA",origHost="oc-diam-connector",} 0.0 • occnp_diam_service_overall_processing_time_seconds_max{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Update",origHost="oc-diam-connector",} 0.0 • occnp_diam_service_overall_processing_time_seconds_max{appId="16777303",cmdCode="258",destHost="tdf.telecom.com",msgType="RAA-Terminate",origHost="oc-diam-connector",} 0.0 • occnp_diam_service_overall_processing_time_seconds_max{appId="16777303",cmdCode="272",destHost="oc-diam-connector",msgType="CCA-T",origHost="tdf.telecom.com",} 0.0

Table 9-328 occnp_diam_service_overall_processing_time_seconds_bucket

Field	Details
Description	Tracks latency of all incoming requests towards Diameter Gateway. This provides an overall time tracking latency for any request towards Diameter Gateway.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost • le
Examples	• occnp_diam_service_overall_processing_time_seconds_bucket{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",msgType="TSA",origHost="oc-diam-connector",le="0.002",} 0.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-329 occnp_diam_service_overall_processing_time_seconds_count

Field	Details
Description	Tracks latency of all incoming requests towards Diameter Gateway. This provides an overall time tracking latency for any request towards Diameter Gateway.
Type	Histogram
Dimension	• appId • cmdCode • msgType • origHost • destHost
Examples	• occnp_diam_service_overall_processing_time_seconds_count{appId="16777303",cmdCode="8388637",destHost="tdf.telecom.com",msgType="TSA",origHost="oc-diam-connector",} 0.0

Table 9-330 occnp_diam_pending_requests

Field	Details
Description	This tracks the total pending diameter requests.
Type	Gauge
Dimension	• namespace • pod
Examples	occnp_diam_pending_requests 1.0

Table 9-331 occnp_congestion_DiamMsgBuffer_queue_msg_count

Field	Details
Description	This tracks the congestion control DiamMsgBuffer queue message count.
Type	Gauge
Dimension	• namespace • pod
Examples	occnp_congestion_DiamMsgBuffer_queue_msg_count 1.0

Table 9-332 occnp_congestion_diam_pending_request_end_to_end_id_map_size

Field	Details
Description	This tracks the congestion control diameter pending requests end to end id map size.
Type	Gauge
Dimension	• namespace • pod • diameterPendingRequestsEndToEndIdMap
Examples	occnp_congestion_diam_pending_request_end_to_end_id_map_size 1.0

Table 9-333 occnp_congestion_diam_pending_request_active_counter

Field	Details
Description	This tracks the current active counter for calculating pending diameter requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-333 (Cont.) occnp_congestion_diam_pending_request_active_counter

Field	Details
Type	Gauge
Dimension	• namespace • pod
Examples	occnp_congestion_diam_pending_request_active_counter 1.0

Table 9-334 occnp_ocnf_service_cookie_total

Field	Details
Description	The metrics with direction "IN" is pegged only when `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key for Diameter Gateway is enabled and custom AVP is received from Diameter Gateway for BSF. In this case, source is `External Peer`. Also, the metrics with direction "IN" is pegged when `ENABLE_N7_SESSION_LOOKUP_COOKIE` Advanced Settings key for Diameter Gateway is enabled and is incremented after Diameter Gateway receives ocnf-service-cookie from Network Peer or after Diameter Gateway receives ocnf-service-cookie from Binding service. The metrics with direction "OUT" is pegged only when OCNF-Service-Cookie customAVP is present while sending the request to destination peer.
Type	Counter
Dimension	• direction • source
Examples	occnp_ocnf_service_cookie_total{direction="in",source="Binding"} 1.0 occnp_ocnf_service_cookie_total{direction="in",source="network_peer"} 1.0 occnp_ocnf_service_cookie_total{direction="out",source=""} 2.0

Table 9-335 occnp_context_owner_source_total

Field	Details
Description	This metric determines how the context owner is identified, if it is from custom AVP or by querying Binding service. When queried from Binding service, context_owner can be SM service. When context_owner_source is "ocnf-service-cookie", context_owner is SM service.
Type	Counter
Dimension	• direction • source
Examples	occnp_context_owner_source_total {context_owner="PCF-SM",source="Binding"} 4.0 occnp_context_owner_source_total {context_owner="PCRF-CORE",source="Binding"} 4.0 occnp_context_owner_source_total {context_owner="PCF-SM",source="ocnf-service-cookie"} 1.0

Table 9-336 diam_repaving_disconnections_total

Field	Details
Description	This metric counts the total number of connections terminated by the "force disconnect" mechanism.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-336 (Cont.) diam_repaving_disconnections_total

Field	Details
Type	Counter
Dimension	• peer_realm • peer_host
Example	diam_repaving_disconnections_total{origHost="pgw.oracle.com",origRealm="oracle.com"} 1.0

For more information about Dimensions, seeCNC Policy Metrics.

9.13 Policy DS Metrics

The following table describes the Policy DS Service metrics and respective dimensions:

Table 9-337 client_request_total

Field	Details
Description	Total number of client requests.
Type	Counter
Dimension	• operation • task
Example	client_request_total{application="policyds",operation="SEARCH",workflow="LDAP",} 1.0 ; Type-Counter

Table 9-338 client_response_total

Field	Details
Description	Total number of responses from the client.
Type	Counter
Dimension	• operation • task • response
Example	client_response_total{application="policyds",operation="SEARCH",response="200",workflow="LDAP",} 1.0 ; Type-Counter

Table 9-339 server_request_total

Field	Details
Description	Metric that increments its value each time a request is being sent from PDS to another service. For example: For communication with CHF task dimension is "CHF".
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-339 (Cont.) server_request_total

Field	Details
Dimension	• exported_application • hostname • method • task • vendorId
Examples	• server_request_total{exported_application="policyds",method="SEARCH",task="UDR",} 1.0 ; Type-Counter • server_request_total{exported_application="policyds",method="GET",task="LDAP",} 1.0 ; Type-Counter • server_request_total{exported_application="policyds",method="INSERT",task="PRE",} 1.0 ;Type-Counter • server_request_total{application="policyds",method="NOTIFY",task="PCF_AM",vendorId="Oracle",} 1.0 • server_response_total{application="policyds",method="NOTIFY",response="204",task="PCF_AM",vendorId="Oracle",} 1.0 • server_request_total{application="policyds",method="JSON_PATCH",task="SSV",vendorId="Oracle"} 6.0

Table 9-340 occnp_http_in_conn_processing_latency_seconds_bucket

Field	Details
Description	This metric is used to measure the overall response time for request received from downstream components to Binding service database.
Type	Histogram
Dimensions	• sourceUri • sourceOperationType • uri • operationType • priority • responseCode • responseCause • duration
Example	-

Table 9-341 occnp_http_out_conn_processing_latency_seconds_bucket

Field	Details
Description	This metric is used to measure the overall response time for request towards upstream components to Binding service database.
Type	Histogram
Dimensions	• sourceUri • sourceOperationType • uri • operationType • priority • responseCode • responseCause • duration

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-341 (Cont.) occnp_http_out_conn_processing_latency_seconds_bucket

Field	Details
Example	-

Table 9-342 server_response_total

Field	Details
Description	Metric that increments its value each time a response is being received from a request that PDS sent to another service. For example: For communication with CHF task dimension is "CHF". Response dimension specifies the response of the request (200, 500, 400, etc)
Type	Counter
Dimension	• exported_application • hostname • method • response • task • vendorId
Example	• server_response_total{exported_application="policyds",method="POST",response="200",} 1.0 ; Type-Counter • server_response_total{application="policyds",method="JSON_PATCH",response="204",task="SSV",vendorId="Oracle"} 6.0

Table 9-343 revalidation_request_total

Field	Details
Description	This metric is incremented when the revalidation is required for a datasource. It is also incremented when revalidation for a subscription failed with 404 but reattempt is done for the request.
Type	Counter
Dimension	• application • hostname • task • method • revalidation_status • vendorId
Examples	• revalidation_request_total{application="policyds",hostname="plcy-ocpm-policyds-567d754bbd-7cwrt",method="INSERT",revalidation_status="REVALIDATION",task="UDR_SUBS",vendorId="Oracle",} 9.0 • revalidation_request_total{application="policyds",hostname="plcy-ocpm-policyds-567d754bbd-7cwrt",method="SEARCH",revalidation_status="REVALIDATION",task="CHF",vendorId="Oracle",} 11.0 • revalidation_request_total{application="policyds",hostname="plcy-ocpm-policyds-567d754bbd-7cwrt",method="SEARCH",revalidation_status="REVALIDATION_REATTEMPT",task="CHF",vendorId="Oracle",} 4.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-344 revalidation_response_total

Field	Details
Description	This metric is incremented when any of the following responses are received for revalidation request: • When CHF or UDR query is successful returning 200 OK and revalidation required is also true. • CHF revalidation failed with an error other than 404 but reattempt is not required, thereby resulting in data removal. • CHF query is unsuccessful returning 404, and revalidation failed but reattempt is not to be done, thereby resulting in data removal. • UDR subscription query revalidation reattempt failed, so subscription information is removed for UDR datasource. • Revalidation request for UDR GET failed. **Note**: You can identify the exact cause with the `revalidation_status` dimension of the metric.
Type	Counter
Dimension	• application • hostname • task • method • revalidation_status • vendorId
Examples	• revalidation_response_total{application="policyds",hostname="plcy-ocpm-policyds-567d754bbd-7cwrt",method="SEARCH",revalidation_status="REVALIDATION_SUCCESS",task="CHF",vendorId="Oracle",} 9.0 • revalidation_response_total{application="policyds",hostname="plcy-ocpm-policyds-567d754bbd-7cwrt",method="INSERT",revalidation_status="REVALIDATION_REATTEMPT_DELETE_SUBSCRIPTION",task="UDR_SUBS",vendorId="Oracle",} 1.0 • revalidation_response_total{application="policyds",hostname="plcy-ocpm-policyds-567d754bbd-7cwrt",method="SEARCH",revalidation_status="REVALIDATION_REATTEMPT_DELETE_ENTITY",task="UDR",vendorId="Oracle",} 2.0

Table 9-345 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimension	• Service Name • Pod Name

Table 9-346 occnp_error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter
Dimension	• application • application_exception • wrapped_exception

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-346 (Cont.) occnp_error_handler_in_total

Field	Details
Example	occnp_error_handler_in_total{application="policyds",application_exception="HttpException",wrapped_exception="TimeoutException",} 1.0

Table 9-347 occnp_error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter
Dimension	• application • application_exception • error_type • operation • origin • rule_name • source_interface • target • wrapped_exception
Example	occnp_error_handler_exec_total{application="policyds",application_exception="HttpException",error_type="INTERNAL",operation="LOOKUP",origin="HTTP",rule_name="HTTP_REQUEST",source_interface="POLICY",status="502",target_interface="BSF",wrapped_exception="BadGateway",} 1.0

Table 9-348 occnp_error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter
Dimension	• application • application_exception • error_resolved • wrapped_exception
Example	occnp_error_handler_out_total{application="policyds",application_exception="HttpException",error_resolved="true",wrapped_exception="ServiceUnavailable",} 1.0

Table 9-349 occnp_policyds_overall_processing_time_seconds

Field	Details
Description	Policy DS service overall processing time. **Note**: Default name used when there is no custom name available is data_repository_invocations.
Type	Summary

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-349 (Cont.) occnp_policyds_overall_processing_time_seconds

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-350 occnp_policyds_overall_processing_time_seconds_max

Field	Details
Description	Diameter Connector service overall processing time.
Type	Gauge
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-351 occnp_policyds_overall_processing_time_seconds_count

Field	Details
Description	Diameter Connector service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Table 9-352 occnp_policyds_overall_processing_time_seconds_sum

Field	Details
Description	Diameter Connector service overall processing time.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-352 (Cont.) occnp_policyds_overall_processing_time_seconds_sum

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Examples	error_handler_out_total{application="policyds",application_exception="HttpException",error_resolved="true",wrapped_exception="BadRequest",} 1.0

Table 9-353 occnp_nf_cookie_forwarded_total

Field	Details
Description	This metric is incremented every time a NF profile cookie is forwarded from PDS.
Type	Counter
Dimension	• application • task • vendorId
Example	occnp_nf_cookie_forwarded_total{application="policyds,"task="UDR",vendorId="Oracle"} 1.0 ;

Table 9-354 occnp_nf_cookie_recieved_total

Field	Details
Description	This metric is incremented every time a NF profile cookie is received from PDS.
Type	Counter
Dimension	• application • task • vendorId
Example	occnp_nf_cookie_recieved_total{application="policyds,task="UDR",vendorId="Oracle"} 1.0 ;

Table 9-355 data_repository_invocations_seconds_max

Field	Details
Description	This metric is used to track the maximum execution time of Data repository invocations. It is a useful metric for monitoring the performance of data repositories and identifying slow-running queries.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-355 (Cont.) data_repository_invocations_seconds_max

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_max{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-356 data_repository_invocations_seconds_sum

Field	Details
Description	The seconds_sum metric for Data repository invocations is a measure of the total time spent executing repository methods.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-356 (Cont.) data_repository_invocations_seconds_sum

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_sum{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.84.88:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nshv9", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-357 data_repository_invocations_seconds_count

Field	Details
Description	This metric measures the total time spent in Data JPA repository invocations. It is a counter metric, which means that it increments each time a repository method is invoked. The metric is reported in seconds.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-357 (Cont.) data_repository_invocations_seconds_count

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • service • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_count{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="findAll", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditRegistrationsRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-358 create_context_on_failure_response

Field	Details
Description	This metrics increments on receiving failure response from its respective data source and that has createContextOnFailure set to true in the request.
Metric Type	Counter
Dimensions	• task • method • sourceType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-358 (Cont.) create_context_on_failure_response

Field	Details
Example	-

Table 9-359 occnp_db_processing_latency_seconds_count

Field	Details
Description	This metric is used to measure the overall response time for requested DB operations.
Type	Histogram
Dimension	• application • hostname • inOperationType • inUri • method • primary_key_combination • responseCause • responseCode • sourceOperationType • sourceUri • tableName • type_of_search • search_key_type • migration_enabled • mode • prev_mode • response_content
Example	occnp_db_processing_latency_seconds_count{application="policyds",inOperationType="SEARCH", inUri="/pds/v2/user-data",method="findSubscriberDataByProfileId", primary_key_combination="NA", responseCause="", responseCode="success", sourceOperationType="", sourceUri="", tableName="pdssubscriber", type_of_search="MULTI_UE_ID_SEARCH",} 2.0 occnp_db_processing_latency_seconds_count{application="policyds",inOperationType="SEARCH", inUri="/pds/v2/user-data", method="deleteSubscribers", primary_key_combination="NA", responseCause="", responseCode="success", sourceOperationType="", sourceUri="", tableName="pdssubscriber", type_of_search="MULTI_UE_ID_SEARCH",} 2.0

Table 9-360 pds_location_info_db_search_total

Field	Details
Description	This metric is used to monitor the DB queries using the primary key lookup. The metrics also monitors the queries, doing DB lookup using a index column in case of primary key lookup failure.
Type	Counter
Dimension	• application • cause • hostname • method • primary_key_ds • search_method • types_array • workflow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-360 (Cont.) pds_location_info_db_search_total

Field	Details
Example	• pds_location_info_db_search_total{application="policyds",cause="SUCCESS",hostname="cnpolicy-ocpm-policyds-6dcd4c45d7-92krq",method="DELETE",primary_key_ds="[1, 2, 7]",search_method="findPdsSubscriberDataByPDSUserIdList",types_array="[2]",workflow="SUBSCRIBER-DELETE",} 1.0 • pds_location_info_db_search_total{application="policyds",cause="SUCCESS",hostname="cnpolicy-ocpm-policyds-6dcd4c45d7-92krq",method="SEARCH",primary_key_ds="NA",search_method="findPdsSubscriberDataByPDSUserIdList",types_array="NA",workflow="PCF-AM-SEARCH",} 2.0 • pds_location_info_db_search_total{application="policyds",cause="PRIMARY_KEY_NOT_EXIST",hostname="cnpolicy-ocpm-policyds-6dcd4c45d7-92krq",method="SEARCH",primary_key_ds="NA",search_method="findPdsSubscriberDataByProfileId",types_array="NA",workflow="REQUEST-PC",} 2.0 • pds_location_info_db_search_total{application="policyds",cause="CREATE",hostname="cnpolicy-ocpm-policyds-6dcd4c45d7-92krq",method="SEARCH",primary_key_ds="NA",search_method="findPdsSubscriberDataByProfileId",types_array="NA",workflow="PCF-AM-SEARCH",} 4.0 • pds_location_info_db_search_total{application="policyds",cause="DATA_MISMATCH",hostname="cnpolicy-ocpm-policyds-6dcd4c45d7-92krq",method="DELETE",primary_key_ds="[2, 7]",search_method="findPdsSubscriberDataByProfileId",types_array="[1, 2, 7]",workflow="SUBSCRIBER-DELETE",} 1.0 • pds_location_info_db_search_total{application="policyds",cause="HEADER_MISSING",hostname="cnpolicy-ocpm-policyds-6dcd4c45d7-92krq",method="DELETE",primary_key_ds="NA",search_method="findPdsSubscriberDataByProfileId",types_array="NA",workflow="SUBSCRIBER-DELETE",} 1.0 • pds_location_info_db_search_total{application="policyds",cause="NO_DATA",hostname="cnpolicy-ocpm-policyds-6dcd4c45d7-92krq",method="DELETE",primary_key_ds="[1, 2, 7]",search_method="findPdsSubscriberDataByProfileId",types_array="[1, 2, 7]",workflow="SUBSCRIBER-DELETE",} 1.0

Table 9-361 task_count_total

Field	Details
Description	This metric is used to monitor the number of times the tasks were executed for a specific workflow.
Type	Counter
Dimension	• application • method • task • workflow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-361 (Cont.) task_count_total

Field	Details
Example	• task_count_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.dbtask.DBFlowTask",workflow="PCF-SM-SEARCH",} 1.0 • task_count_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.httpTask.CHFConnectorFlowTask",workflow="REQUEST-PC",} 1.0 • task_count_total{application="policyds",method="INSERT",task="ocpm.uds.policyds.workflow.flowtask.dbtask.DBFlowTask",workflow="PCF-SM-SEARCH",} 1.0 • task_count_total{application="policyds",method="INSERT",task="ocpm.uds.policyds.workflow.flowtask.dbtask.PolicyCounterFlowTask",workflow="REQUEST-PC",} 1.0 • task_count_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.dbtask.PolicyCounterFlowTask",workflow="REQUEST-PC",} 1.0 • task_count_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.dbtask.AuditDBFlowTask",workflow="AUDIT-SUBSCRIBER-CLEANUP",} 1.0 • task_count_total{application="policyds",method="DELETE",task="ocpm.uds.policyds.workflow.flowtask.httpTask.CHFConnectorFlowTask",workflow="CONTEXT_CLEANUP",} 1.0 • task_count_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.httpTask.ContextVerifyFlowTask",workflow="AUDIT-SUBSCRIBER-CLEANUP",} 1.0 • task_count_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.httpTask.UDRServiceFlowTask",workflow="PCF-SM-SEARCH",} 1.0 • task_count_total{application="policyds",method="DELETE",task="ocpm.uds.policyds.workflow.flowtask.dbtask.ContextCleanupTask",workflow="CONTEXT_CLEANUP",} 1.0

Table 9-362 task_processing_latency_sum_total

Field	Details
Description	This metric is used to monitor the total time spent on executing a task for a given workflow.
Type	Gauge
Dimension	• application • method • task • workflow

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-362 (Cont.) task_processing_latency_sum_total

Field	Details
Example	• task_processing_latency_sum_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.dbtask.DBFlowTask",workflow="PCF-SM-SEARCH",} 25.0 • task_processing_latency_sum_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.httpTask.CHFConnectorFlowTask",workflow="REQUEST-PC",} 1.0 • task_processing_latency_sum_total{application="policyds",method="INSERT",task="ocpm.uds.policyds.workflow.flowtask.dbtask.DBFlowTask",workflow="PCF-SM-SEARCH",} 94.0 • task_processing_latency_sum_total{application="policyds",method="INSERT",task="ocpm.uds.policyds.workflow.flowtask.dbtask.PolicyCounterFlowTask",workflow="REQUEST-PC",} 41.0 • task_processing_latency_sum_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.dbtask.PolicyCounterFlowTask",workflow="REQUEST-PC",} 0.0 • task_processing_latency_sum_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.dbtask.AuditDBFlowTask",workflow="AUDIT-SUBSCRIBER-CLEANUP",} 14.0 • task_processing_latency_sum_total{application="policyds",method="DELETE",task="ocpm.uds.policyds.workflow.flowtask.httpTask.CHFConnectorFlowTask",workflow="CONTEXT_CLEANUP",} 5.0 • task_processing_latency_sum_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.httpTask.ContextVerifyFlowTask",workflow="AUDIT-SUBSCRIBER-CLEANUP",} 131.0 • task_processing_latency_sum_total{application="policyds",method="SEARCH",task="ocpm.uds.policyds.workflow.flowtask.httpTask.UDRServiceFlowTask",workflow="PCF-SM-SEARCH",} 7.0 • task_processing_latency_sum_total{application="policyds",method="DELETE",task="ocpm.uds.policyds.workflow.flowtask.dbtask.ContextCleanupTask",workflow="CONTEXT_CLEANUP",} 96.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-363 occnp_policy_data_subscription_expiry_status_total

Field	Details
Description	This metric is used to monitor the status of the UDR data subscription.
Type	Counter
Dimension	• application • hostname • sourceType • expiryStatus • contextOwner
Example	{application="policyds",contextOwner="PCF_SM",expiryStatus="PRE_EXPIRY",hostname="policy-ocpm-policyds-748fbc8d55-gcm4c",sourceType="operatorSpecificData"} 3.0

Table 9-364 occnp_policy_data_resubscription_request_total

Field	Details
Description	This metric is used to monitor the resubscription request sent from PDS.
Type	Counter
Dimension	• application • hostname • sourceType • expiryStatus • action
Example	{action="RESUBSCRIBE",application="policyds",expiryStatus="PRE_EXPIRY",hostname="policy-ocpm-policyds-748fbc8d55-gcm4c",sourceType="OperatorSpecificData"} 3.0

Table 9-365 occnp_policy_data_resubscription_response_total

Field	Details
Description	This metric is used to monitor the resubscription response[success/failure] received at PDS.
Type	Counter
Dimension	• application • hostname • sourceType • expiryStatus • action • response
Example	{action="DELETE",application="policyds",expiryStatus="PRE_EXPIRY",hostname="policy-ocpm-policyds-748fbc8d55-gcm4c",response="404",sourceType="OperatorSpecificData"} 2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-366 occnp_audit_notifications_total

Field	Details
Description	This metric is used to retrieve the total number of audit requests received by PDS.
Type	Counter
Dimension	• application • contextOwner • method • workflow
Example	occnp_audit_notifications_total{application="policyds",contextOwner="AUDIT", method="NOTIFY",workflow="AUDIT-SUBSCRIBER-CLEANUP"} 71.0

For more information about Dimensions, see CNC Policy Metrics.

9.14 LDAP Gateway

The following table describes the LDAP Gateway Service metrics and respective dimensions:

Table 9-367 ldap_request_total

Field	Details
Description	Indicates the total number of LDAP requests.
Type	Counter
Dimension	• code • ReqType • hostname • application
Example	ldap_request_total{ReqType="GET",application="ldapgateway",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",} 10.0 ; Type-Counter

Table 9-368 ldap_response_total

Field	Details
Description	Indicates the total number of LDAP responses.
Type	Counter
Dimension	• ReqType • Code • application • hostname
Examples	• ldap_response_total{Code="5xx",ReqType="GET",application="ldapgateway",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",} 1.0 ; Type-Counter • ldap_response_total{Code="2xx",ReqType="GET",application="ldapgateway",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",} 2.0 ; Type-Counter • ldap_response_total{Code="4xx",ReqType="GET",application="ldapgateway",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",} 7.0 ; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-369 occnp_ldap_search_request_total

Field	Details
Description	Indicates the total number of LDAP search requests.
Type	Counter
Dimension	• application • destination_host • hostname • retry
Example	• occnp_ldap_search_request_total{application="ldapgateway",destination_host="10.233.91.248",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",retry="true",} 2.0 ; Type-Counter • occnp_ldap_search_request_total{application="ldapgateway",destination_host="10.233.91.190",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",retry="false",} 1.0 ; Type-Counter

Table 9-370 occnp_ldap_search_response_total

Field	Details
Description	Indicates the total number of LDAP search responses.
Type	Counter
Dimension	• application • destination_host • hostname • result_code • retry
Example	• occnp_ldap_search_response_total{application="ldapgateway",destination_host="10.233.91.187",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",result_code="32",retry="false",} 1.0 ; Type-Counter • occnp_ldap_search_response_total{application="ldapgateway",destination_host="10.233.73.139",hostname="policy-ocpm-ldap-gateway-794f856db6-2w8gr",result_code="32",retry="true",} 2.0 ; Type-Counter

Table 9-371 occnp_ldap_conn_total

Field	Details
Description	This metric is used to monitor and track the number of active connections between the LDAP Gateway and its configured LDAP servers. It provides greater visibility into the connectivity status and helps in identifying issues related to LDAP server availability.
Type	Gauge
Dimension	• peer
Example	• occnp_ldap_conn_total{peer="10.233.12.145:8080"}

Table 9-372 http_server_requests_seconds_count

Field	Details
Description	Number of http request received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-372 (Cont.) http_server_requests_seconds_count

Field	Details
Dimension	• method • outcome • status • uri • error • exception
Example	http_server_requests_seconds_count{exception="None",method="GET",outcome="SUCCESS",status="200",uri="/pcrfSessionData",} 2.0

Table 9-373 http_server_requests_seconds_max

Field	Details
Description	Maximum number of http requests received.
Type	Counter
Dimension	• method • outcome • status • uri • error • exception
Example	http_server_requests_seconds_max{exception="None",method="GET",outcome="SUCCESS",status="200",uri="/pcrfSessionData",} 0.0

For more information about Dimensions, see CNC Policy Metrics.

9.15 Binding Service Metrics

The following table describes the Binding Service metrics and respective dimensions:

Table 9-374 ocpm_binding_inbound_request_total

Field	Details
Description	Total number of inbound requests.
Type	Counter
Dimension	• operation_type • servicename_3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-374 (Cont.) ocpm_binding_inbound_request_total

Field	Details
Examples	• ocpm_binding_inbound_request_total{operation_type="read",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com",servicename_3gpp="binding.1.0",} 5.0 ; Type-Counter • ocpm_binding_inbound_request_total{operation_type="delete",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com",servicename_3gpp="binding.1.0",} 10.0 ; Type-Counter • ocpm_binding_inbound_request_total{operation_type="write",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com",servicename_3gpp="binding.1.0",} 91.0 ; Type-Counter

Table 9-375 ocpm_egress_request_total

Field	Details
Description	Total number of egress requests.
Type	Counter
Dimension	• operation_type • servicename_3gpp • nf_instance_id • nf_name • egress_service
Example	-

Table 9-376 ocpm_egress_response_total

Field	Details
Description	Total number of egress responses.
Type	Counter
Dimension	• servicename_3gpp • response_code • nf_instance_id • nf_name • egress_service • latency • DNN • snssai • PCF FQDN
Example	-

Table 9-377 ocpm_binding_inbound_response_total

Field	Details
Description	Total number of inbound responses.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-377 (Cont.) ocpm_binding_inbound_response_total

Field	Details
Dimension	• operation • task • response_code
Examples	• ocpm_binding_inbound_response_total{operation_type="delete",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com",response_code="2xx",servicename_3gpp="binding.1.0",} 10.0 ; Type-Counter • ocpm_binding_inbound_response_total{operation_type="write",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com"response_code="2xx",servicename_3gpp="binding.1.0",} 91.0 ; Type-Counter • ocpm_binding_inbound_response_total{operation_type="read",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com"response_code="4xx",servicename_3gpp="binding.1.0",} 1.0 ; Type-Counter • ocpm_binding_inbound_response_total{operation_type="read",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com"response_code="5xx",servicename_3gpp="binding.1.0",} 1.0 ; Type-Counter

Table 9-378 occnp_binding_query_request_count

Field	Details
Description	This metric tracks the total number of Audit Notify requests received from BSF.
Type	Counter
Dimension	• operation • servicename_3gpp
Example	occnp_binding_query_request_count_total{ingress_service="",operation_type="AuditNotify",servicename_3gpp="binding",} 1.0

Table 9-379 occnp_binding_query_response_count

Field	Details
Description	This metric tracks the total number of successful responses sent to BSF for Audit Notify requests.
Type	Counter
Dimension	• operation • servicename_3gpp • response_code
Example	occnp_binding_query_response_count_total{ingress_service="",operation_type="AuditNotify",response_code="2xx",servicename_3gpp="binding",} 1.0

Table 9-380 occnp_audit_notif_request_count_total

Field	Details
Description	The total number of audit notification requests received by binding service.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-380 (Cont.) occnp_audit_notif_request_count_total

Field	Details
Dimension	• servicename_3gpp • nfInstanceId
Example	occnp_audit_notif_request_count_total{nfInstanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",servicename_3gpp="binding",} 1.0 ; Type-Counter

Table 9-381 occnp_audit_notif_response_count_total

Field	Details
Description	The total number of responses sent by binding service for audit notifications.
Type	Counter
Dimension	• servicename_3gpp • nfInstanceId • response_code
Example	occnp_audit_notif_response_count_total{nfInstanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",response_code="2xx",servicename_3gpp="binding",} 1.0 ; Type-Counter

Table 9-382 occnp_stale_session_cleanup_count_total

Field	Details
Description	Total number of records deleted from the binding database by the stale session clean up process.
Type	Counter
Dimension	• servicename_3gpp • sessionType
Example	occnp_stale_session_cleanup_count_total{servicename_3gpp="binding",sessionType="dependentcontextbinding",} 1.0 ; Type-Counter

Table 9-383 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimension	• Service Name • Pod Name
Example	-

Table 9-384 occnp_binding_service_overall_processing_time_seconds

Field	Details
Description	Binding service overall processing time.
Type	Summary

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-384 (Cont.) occnp_binding_service_overall_processing_time_seconds

Field	Details
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Example	-

Table 9-385 occnp_binding_service_overall_processing_time_seconds_max

Field	Details
Description	Binding service overall processing time.
Type	Gauge
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Examples	• occnp_binding_service_overall_processing_time_seconds_max{error="none", exception="none", method="POST", outcome="SUCCESS", status="201", uri="/binding/v1/contextBinding/context-owner/{contextOwner}",} 2.595594434 • occnp_binding_service_overall_processing_time_seconds_max{error="none", exception="none", method="DELETE", outcome="SUCCESS", status="204", uri="/binding/v1/contextBinding/contextId/{contextId}",} 0.276239293 • occnp_binding_service_overall_processing_time_seconds_max{error="ContextBindingNotFound", exception="ContextBindingNotFound", method="DELETE", outcome="CLIENT_ERROR", status="404", uri="/binding/v1/contextBinding/cleanup",} 0.115288423

Table 9-386 occnp_binding_service_overall_processing_time_seconds_count

Field	Details
Description	Binding service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-386 (Cont.) occnp_binding_service_overall_processing_time_seconds_count

Field	Details
Examples	• occnp_binding_service_overall_processing_time_seconds_count{error="none", exception="none", method="POST", outcome="SUCCESS", status="201", uri="/binding/v1/contextBinding/context-owner/{contextOwner}",} 3.0 • occnp_binding_service_overall_processing_time_seconds_count{error="none", exception="none", method="DELETE", outcome="SUCCESS", status="204", uri="/binding/v1/contextBinding/contextId/{contextId}",} 3.0 • occnp_binding_service_overall_processing_time_seconds_count{error="ContextBindingNotFound", exception="ContextBindingNotFound",method="DELETE",outcome="CLIENT_ERROR", status="404",uri="/binding/v1/contextBinding/cleanup",} 6.0

Table 9-387 occnp_binding_service_overall_processing_time_seconds_sum

Field	Details
Description	Binding service overall processing time.
Type	Counter
Dimension	• application • error • exception • hostname • method • outcome • status • uri
Examples	• occnp_binding_service_overall_processing_time_seconds_sum{error="none",exception="none",method="POST", outcome="SUCCESS", status="201", uri="/binding/v1/contextBinding/context-owner/{contextOwner}",} 5.861114721 • occnp_binding_service_overall_processing_time_seconds_sum{error="none", exception="none",method="DELETE",outcome="SUCCESS",status="204",uri="/binding/v1/contextBinding/contextId/{contextId}",} 0.349598291 • occnp_binding_service_overall_processing_time_seconds_sum{error="ContextBindingNotFound",exception="ContextBindingNotFound", method="DELETE",outcome="CLIENT_ERROR",status="404", uri="/binding/v1/contextBinding/cleanup",} 0.203103476

Table 9-388 occnp_bindingservice_db_operation_time_seconds_count

Field	Details
Description	Binding service overall database processing time.
Type	Gauge
Dimension	• exception • method • repository • state
Examples	• occnp_bindingservice_db_operation_time_seconds_count{exception="None",method="findByTopicInfo",repository="ConfigurationItemRepository",state="SUCCESS",} 7721880.0 • occnp_bindingservice_db_operation_time_seconds_count{exception="None",method="findByName",repository="TopicInfoRepository",state="SUCCESS",} 8190322.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-389 occnp_bindingservice_db_operation_time_seconds_sum

Field	Details
Description	Binding service overall database processing time.
Type	Gauge
Dimension	• exception • method • repository • state
Examples	• occnp_bindingservice_db_operation_time_seconds_sum{exception="None",method="findByTopicInfo",repository="ConfigurationItemRepository",state="SUCCESS",} 4713.01 • occnp_bindingservice_db_operation_time_seconds_sum{exception="None",method="findByName",repository="TopicInfoRepository",state="SUCCESS",} 6328.74490

Table 9-390 occnp_bindingservice_db_operation_time_seconds_max

Field	Details
Description	Binding service overall database processing time.
Type	Gauge
Dimension	• exception • method • repository • state

Table 9-391 ocpm_egress_request_timeout_total

Field	Details
Description	Binding service overall database processing time.
Type	Gauge
Dimension	• exception • method • repository • state
Examples	• ocpm_egress_request_timeout_total{Host_Name="",application="pcf_bindingservice",egress_service="BSF",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com",operation_type="write",service_resource="pcfBindings",service_version="V1",servicename_3gpp="binding",} 1.0 • ocpm_egress_request_timeout_total{Host_Name="",application="pcf_bindingservice",egress_service="BSF",nfInstanceId="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="bsf.xxxx.com",operation_type="delete",service_resource="pcfBindings",service_version="V1",servicename_3gpp="binding",} 1.0

Table 9-392 occnp_stale_session_cleanup_internal_queue_size

Field	Details
Description	Binding session stale internal queue size.
Type	Gauge
Dimension	servicename_3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-392 (Cont.) occnp_stale_session_cleanup_internal_queue_size

Field	Details
Example	occnp_stale_session_cleanup_internal_queue_size{servicename_3gpp="binding",} 2.0; Type-Gauge

Table 9-393 occnp_audit_delete_record_count_total

Field	Details
Description	This metric is used to monitor records deleted in binding by Audit Service.
Type	Counter
Dimension	• max_ttl_reached (true/false) • nfInstanceId • sessionType (contextbinding/ dependentContextBinding) • servicename_3gpp
Examples	occnp_audit_delete_record_count{max_ttl_reached="true",nfInstanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",servicename_3gpp="binding",sessionType="contextbinding",}2.0

Table 9-394 occnp_error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter
Dimensions	• application • applicationException • wrapped_exception
Example	occnp_error_handler_in_total{application_exception="JavaException",status="500",wrapped_exception="ServiceException",} 1.0

Table 9-395 occnp_error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter
Dimensions	• application • applicationException • error_type • operation • origin • rule_name • source_interface • target_interface • wrapped_exception
Example	occnp_error_handler_exec_total{application_exception="JavaException",error_type="INTERNAL",operation="AUDIT",origin="JAVA",rule_name="REJECT_WITH_ENHANCED_DETAIL",source_interface="BSF",status="404",target_interface="POLICY",wrapped_exception="ServiceException",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-396 occnp_error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter
Dimensions	• application • applicationException • error_resolved • wrapped_exception
Example	occnp_error_handler_out_total{application_exception="JavaException",error_resolved="true",status="404",wrapped_exception="ServiceException",} 1.0

Table 9-397 occnp_late_arrival_rejection_total

Field	Details
Description	This metric is pegged whenever Binding service receives a request and it gets rejected at the moment that the request is received (before doing any time consuming operations) because it is already stale.
Type	Counter
Dimensions	• cause Example value: `TIMED_OUT_REQUEST` • servicename_3gpp Example value: `binding` • operation_type Example values: – `CREATE` – `UPDATE` – `LOOKUP`
Example	-

Table 9-398 occnp_late_processing_rejection_total

Field	Details
Description	This metric is pegged whenever Binding service receives a request and it gets rejected after doing time consuming operation (DB operations or requests to BSF) because it is already stale.
Type	Counter
Dimensions	• cause Example value: `TIMED_OUT_REQUEST` • servicename_3gpp Example value: `binding` • operation_type Example values: – `CREATE` – `UPDATE` – `LOOKUP` • stage Example values: – PRE_BSF – POST_BSF
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-399 occnp_session_binding_revalidation_request_total

Field	Details
Description	During revalidation, when Policy performs audit check of the binding association returns and sends POST request to BSF, Policy increments metrics with details of DNN, snssai, PCF FQDN.
Type	Counter
Dimensions	• DNN • snssai • PCF FQDN
Example	-

Table 9-400 occnp_session_binding_revalidation_response_total

Field	Details
Description	During revalidation, when Policy receives response from BSF, Policy increments metrics with details of DNN, snssai, PCF FQDN, responseCode, and action. For example: If BSF returns 201, responseCode=201 and if the return binding_id is a the same as it was before the revalidation, then the action= "found". If the return binding_id is a new one, action="restored".
Type	Counter
Dimensions	• DNN • snssai • PCF FQDN • responseCode • action • latency
Example	-

Table 9-401 occnp_db_processing_latency_seconds

Field	Details
Description	This metric is used to measure the overall response time for the requested Binding service database operations.
Type	Histogram
Dimensions	• sourceUri • sourceOperationType • tableName • method • responseCode • responseCause • duration • inUri • inOperationType
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-402 occnp_http_in_conn_processing_latency_seconds_bucket

Field	Details
Description	This metric is used to measure the overall response time for request received from downstream components to Binding service database.
Type	Histogram
Dimensions	• sourceUri • sourceOperationType • uri • operationType • priority • responseCode • responseCause • duration
Example	-

Table 9-403 occnp_http_out_conn_processing_latency_seconds_bucket

Field	Details
Description	This metric is used to measure the overall response time for request towards upstream components to Binding service database.
Type	Histogram
Dimensions	• sourceUri • sourceOperationType • uri • operationType • priority • responseCode • responseCause • duration
Example	-

Table 9-404 occnp_binding_index_restore_total

Field	Details
Description	When data is migrated to the `contextbinding` table, but the corresponding index entries are not saved successfully, Binding Service first searches the index tables during binding discovery. If no record is found, it falls back to the `contextbinding` table. If the context is found, the missing entries are restored in the corresponding index tables. This process is called index restoration. Index restoration applies only to records that are successfully migrated in the `contextbinding` table, where `contextId` and `contextBindingId` are equal. This metric counts the number of indexes restored into index table (that is, lookup tables).
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-404 (Cont.) occnp_binding_index_restore_total

Field	Details
Dimensions	• indexed_key Defines which index is restored. Possible values: – SUPI – GPSI – ipv4Addr – ipv6Prefix
Example	occnp_binding_index_restore_total{indexed_key="supi"} 1.0 occnp_binding_index_restore_total{indexed_key="gpsi"} 1.0 occnp_binding_index_restore_total{indexed_key="ipv4Addr"} 1.0 occnp_binding_index_restore_total{indexed_key="ipv6Prefix"} 1.0

Table 9-405 occnp_binding_index_total

Field	Details
Description	This metric counts the number of times index migration was attempted on audit notification. **Note**: Currently this metric is pegged only during audit notification.
Type	Counter
Dimensions	• error Example: `SQLGrammarException` • operation_type
Example	occnp_binding_index_total{error="SQLGrammarException",operation_type="AUDIT"} 1.0 occnp_binding_index_total{error="none",operation_type="AUDIT"} 1.0

For more information about Dimensions, see CNC Policy Metrics.

9.16 Audit Service Metrics

The following table describes the Audit Service metrics and respective dimensions:

Table 9-406 audit_recs_stale_total

Field	Details
Description	Number of records detected as stale.
Type	Counter
Dimension	• ServiceName • TableName
Example	audit_recs_stale_total{ServiceName="pcf-ueservice",TableName="UePolicyAssociation",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-407 audit_recs_notif_total

Field	Details
Description	Number of stale record notifications sent, applicable for modes: NOTIFY and DELETE_NOTIFY
Type	Counter
Dimension	ServiceName
Examples	• audit_recs_notif_total{ServiceName="sm-service"} 50.0 ; Type-Counter • audit_recs_notif_total{ServiceName="pcf-ueservice",} 1.0

Table 9-408 audit_recs_remv_total

Field	Details
Description	Number of stale records deleted, applicable for modes: DELETE and DELETE_NOTIFY.
Type	Counter
Dimension	• ServiceName • TableName
Example	audit_recs_remv_total{ServiceName="sm-service",TableName="SmPolicyAssociation"} 5.0 ; Type-Counter

Table 9-409 audit_recs_remv_ex_total

Field	Details
Description	Number of exceptions hit during attempt to delete a stale record.
Type	Counter
Dimension	• ServiceName • TableName
Example	audit_recs_remv_ex_total{ServiceName="sm-service",TableName="SmPolicyAssociation"} 0.0 ; Type-Counter

Table 9-410 audit_recs_notif_ex_total

Field	Details
Description	Number of exceptions hit during attempt to notify.
Type	Counter
Dimension	ServiceName
Example	audit_recs_notif_ex_total{ServiceName="sm-service"} 0.0 ;

Table 9-411 audit_recs_notif_err_total

Field	Details
Description	Number of error responses received for notifications sent.
Type	Counter
Dimension	ServiceName
Example	audit_recs_notif_err_total{ServiceName="sm-service"} 13.0 ; Type-Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-412 audit_recs_deque_for_notif_total

Field	Details
Description	Number of stale records dequeued to send notification.
Type	Counter
Dimension	ServiceName
Example	audit_recs_deque_for_notif_total{ServiceName="pcf-ueservice",} 1.0

Table 9-413 audit_recs_enque_for_notif_total

Field	Details
Description	Number of stale records enqueued from database.
Type	Counter
Dimension	ServiceName
Example	audit_recs_enque_for_notif_total{ServiceName="pcf-ueservice",} 1.0

Table 9-414 audit_recs_enque_err_total

Field	Details
Description	Number of stale records failed to enqueue if Queue is full.
Type	Counter
Dimension	ServiceName
Example	audit_recs_enque_err_total{ServiceName="sm-service"} 0.0 ; Type-Counter

Table 9-415 oc_db_active_session_count

Field	Details
Description	Reports the session for a given service e.g. SM session.
Type	Gauge
Dimension	• ServiceName • TableName
Examples	• oc_db_active_session_count{Service="sm-service",Table="smassociation",} 177.0 ; Type-Gauge • oc_db_active_session_count{Service="sm-service",Table="Rx",} 0.0 ; Type-Gauge • oc_db_active_session_count{Service="am-service",Table="amassociation",} 0.0 • oc_db_active_session_count{Service="pcrf-core",Table="gxsession",} 0.0 ; • oc_db_active_session_count{Service="pcrf-core",Table="rxsession",} 0.0 ; • oc_db_active_session_count{Service="pcf-ueservice",TableName="UePolicyAssociation",} 1.0

Table 9-416 occnp_pending_binding_reattempts_total

Field	Details
Description	Indicates when a attempt to recreate has been triggered by PCF.
Type	Counter
Dimension	Attempt

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-417 data_repository_invocations_seconds_max

Field	Details
Description	This metric is used to track the maximum execution time of Data repository invocations. It is a useful metric for monitoring the performance of data repositories and identifying slow-running queries.
Type	Gauge
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_max{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-418 data_repository_invocations_seconds_sum

Field	Details
Description	The seconds_sum metric for Data repository invocations is a measure of the total time spent executing repository methods.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-418 (Cont.) data_repository_invocations_seconds_sum

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_sum{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.84.88:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nshv9", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-419 data_repository_invocations_seconds_count

Field	Details
Description	This metric measures the total time spent in Data JPA repository invocations. It is a counter metric, which means that it increments each time a repository method is invoked. The metric is reported in seconds.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-419 (Cont.) data_repository_invocations_seconds_count

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • service • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_count{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="findAll", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditRegistrationsRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-420 occnp_pending_binding_terminate_all_attempts_failed_total

Field	Details
Description	Indicates when session terminate has been triggered when all recreate attempts fail.
Type	Counter
Dimension	• RESPONSE_CODE, • CAUSE

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-421 occnp_pending_binding_reattempt_fail_total

Field	Details
Description	Indicates when each recreate attempt fail.
Type	Counter
Dimension	NA

Table 9-422 occnp_pending_operation_threshold_reached_total

Field	Details
Description	Indicates when pending operation table threshold has been reached.
Type	Counter
Dimension	NA

Table 9-423 occnp_reject_sm_create_threshold_reached_total

Field	Details
Description	Indicates when SM rejects SM CREATE when pending operation threshold has been reached.
Type	Counter
Dimension	• DNN • CAUSE • RESPONSE_CODE

Table 9-424 occnp_pending_operation_records_count

Field	Details
Description	Indicates the amount of entries in the PendingOperation table.
Type	Gauge
Dimension	NA

Table 9-425 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimension	• Service Name • Pod Name

Table 9-426 occnp_timer_count_total

Field	Details
Description	This metrics indicates the number of timers and their states.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-426 (Cont.) occnp_timer_count_total

Field	Details
Dimension	• **timerState** - State of the timer. The possible enum values are: – CREATED - Timer got successfully created in DB, but timer is not yet scheduled. Local site will schedule it when it is near expiry. – SCHEDULED - Timer is scheduled to notify the event. – NOTIFIED - Timer is notified for the event. – NOTIFY_404 - Timer receives 404 response for timer notification (timerId not found in consumer service corresponding to the association Id). – NOTIFY_4XX - Timer receives 4xx response for timer notification. – NOTIFY_5XX - Timer receives 5xx response for timer notification.

Table 9-427 occnp_timer_capacity

Field	Details
Description	This Gauge metrics tracks the number of metrics for timerName.
Type	Gauge
Dimension	• **timerName** - Unique identifier for timer. • **siteId**- Site owning the timer.

Table 9-428 occnp_timer_scan_total

Field	Details
Description	This metric tracks timer scan and the state.
Type	Counter
Dimension	• **state** - State of the scan. The possible enum values are: – **FAILED** - scan failed. – **SUCCESS** - scan succeed.

Table 9-429 occnp_timer_registration_total

Field	Details
Description	This metric indicates number of timer registrations.
Type	Counter
Dimension	• **callbackServiceFqdn** - Service FQDN for callback Service. • **timerName** - Unique identifier for timer.

Table 9-430 occnp_timer_create_failure_total

Field	Details
Description	This metric tracks timer create failure corresponding to `timerName` with error cause and code.
Type	Counter
Dimension	• **timerName** - Unique identifier for timer. • **errorCause** - Reason for timer create failure. • **errorCode** - Response code for timer create failure.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-431 occnp_timer_notify_retry_total

Field	Details
Description	This metric tracks counter metrics to track timer notification retries.
Type	Counter
Dimension	• **callbackUri** - Callback URI for which the notification was retried.

Table 9-432 occnp_timer_state

Field	Details
Description	This gauge metrics is used to track timer in stuck, stale and scheduled state in each scan.
Type	Gauge
Dimension	• **timerName** - Unique identifier for timer. • **timerState** - State of the timer. – **STALE** - Timer is detected as stale. – **STUCK** - Timer is detected as stuck. – **SCHEDULED** - Timer is scheduled to notify the event.

Table 9-433 occnp_timer_scan_activity_total

Field	Details
Description	This metric is incremented each time a particular timer activity runs.
Type	Counter
Dimension	• **activityType** - Indicates the activity type. The possible enum values are: – CLEANUP – HEARTBEAT – ORPHAN_LOCAL_CHECK – ORPHAN_REMOTE_CHECK

Table 9-434 audit_schedule_current_status

Field	Details
Description	This metric defines status of the current audit schedule. This metric is set to 1, if the status is the current audit schedule is "CTRL_SHUTDOWN_INTRPT". This metric is reset to 0, if the status is changed.
Type	Gauge
Dimension	• Service • Table • Status – CTRL_SHUTDOWN_INTRPT – INTERRUPTED – RUNNING – COMPLETED – INITIALISING – DEREGISTERED – QUEUED

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-434 (Cont.) audit_schedule_current_status

Field	Details
Example	audit_schedule_current_status{Service="pcrf-core", Status="CTRL_SHUTDOWN_INTRPT", Table="rxsession", app_kubernetes_io_instance="conv", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="25.2.100-rc.8.0.0", application="occnp", container="audit-service", endpoint="cnc-metrics", engVersion="25.2.100-rc.8", helm_sh_chart="audit-service-25.2.100-rc.8", instance="10.233.97.19:9000", io_kompose_service="conv-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp-audit", mktgVersion="25.2.100-rc.8.0.0", namespace="ch2-ns13", pod="conv-ocpm-audit-service-68999b77f4-2tnxp", pod_template_hash="68999b77f4", vendor="Oracle"}

Table 9-435 occnp_audit_schedule_status_total

Field	Details
Description	This metric indicated the number of times the audit service has transitioned its status for a specific service and table.
Type	Counter
Dimension	• Service • Table • Status – CTRL_SHUTDOWN_INTRPT – INTERRUPTED – RUNNING – COMPLETED – INITIALISING – DEREGISTERED – QUEUED
Example	occnp_audit_schedule_status_total{Service="pcrf-core", Status="COMPLETED", Table="gxsession", app_kubernetes_io_instance="conv", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="25.2.100-rc.8.0.0", application="occnp", container="audit-service", endpoint="cnc-metrics", engVersion="25.2.100-rc.8", helm_sh_chart="audit-service-25.2.100-rc.8", instance="10.233.97.19:9000", io_kompose_service="conv-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp-audit", mktgVersion="25.2.100-rc.8.0.0", namespace="ch2-ns13", pod="conv-ocpm-audit-service-68999b77f4-2tnxp", pod_template_hash="68999b77f4", vendor="Oracle"}

For more information about Dimensions, see CNC Policy Metrics.

9.17 Query Service Metrics

The following table describes the Query Service metrics and respective dimensions:

Table 9-436 queryservice_sessionDelete_request_total

Field	Details
Description	Total number of delete SM service query requests.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-436 (Cont.) queryservice_sessionDelete_request_total

Field	Details
Dimension	• DeleteScope • ResourceLevel • ResourceType
Examples	• queryservice_sessionDelete_request_total{DeleteScope="Local",ResourceLevel="Individual",ResourceType="BINDING"} 1.0 ; Type-Counter • queryservice_sessionDelete_request{"name":"queryservice_sessionDelete_request","measurements":[{"statistic":"COUNT","value":2.0}],"availableTags":[{"tag":"DeleteScope","values":["Local"]},{"tag":"ResourceLevel","values":["Individual"]},{"tag":"ResourceType","values":["SM"]}]}

Table 9-437 queryservice_sessionDelete_response_total

Field	Details
Description	Total number of responses for delete SM service query.
Type	Counter
Dimension	• DeleteScope • ResourceLevel • ResourceType • Result_Code
Examples	• queryservice_sessionDelete_response_total{DeleteScope="Local",ResourceLevel="Individual",ResourceType="BINDING",Result_Code="2XX"} 1.0 ; Type-Counter • queryservice_sessionDelete_response{"name":"queryservice_sessionDelete_response","measurements":[{"statistic":"COUNT","value":2.0}],"availableTags":[{"tag":"DeleteScope","values":["Local"]},{"tag":"ResourceLevel","values":["Individual"]},{"tag":"ResourceType","values":["SM"]},{"tag":"Result_Code","values":["2XX"]}]}

For more information about Dimensions, see CNC Policy Metrics.

9.18 AppInfo Metrics

This section describes the metrics and examples for AppInfo service.

Table 9-438 appinfo_service_running-

Field	Details
Description	Provides the status of monitored services.
Type	Gauge
Dimension	• service • namespace • category
Example	appinfo_service_running{service="xxx",namespace="xxx",category="xxx"} 1

Table 9-439 appinfo_category_running

Field	Details
Description	Provides the status of monitored categories

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-439 (Cont.) appinfo_category_running

Field	Details
Type	Gauge
Dimension	• namespace • category
Example	appinfo_category_running{category="xxx",namespace="xxx"} 1

Table 9-440 appinfo_category_good

Field	Details
Description	Provides the readiness of monitored categories.
Type	Gauge
Dimension	• namespace • category
Example	appinfo_category_good{category="xxx",namespace="xxx"} 1

Table 9-441 nfscore

Field	Details
Description	*factor*: • Contains one of the values: all, successTPS, serviceHealth, signallingConnections, replicationHealth, localityPreference. • When the factor is set to *all* that means NF score is calculated for all the factors. *status*: • *success*: when the factor is enabled and its value is fetched successfully. • *failed*: when the factor is enabled and fetching the value fails. • *notCalculated*: when the factor is disabled.
Type	Gauge
Dimension	• nfInstanceID • factor • Status
Example	nfscore{app="testing-appinfo", app_kubernetes_io_instance="testing", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="appinfo", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.7.1.0.0", application="ocbsf", calculatedStatus="success", container="appinfo", endpoint="cnc-metrics", engVersion="22.4.0", factor="localityPreference", helm_sh_chart="appinfo-22.4.0", instance="10.233.117.146:9000", job="occne-infra/occne-nf-cnc-podmonitor", microservice="bsf-app-info", mktgVersion="1.7.1.0.0", namespace="biloxi-ns", nfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0666", pod="testing-appinfo-78dc65865f-hgrhk", pod_template_hash="78dc65865f", vendor="Oracle"} 5

Table 9-442 nfScoringFactorActualValue

Field	Details
Description	The factor tag would contain one of the following values: successTPS, serviceHealth, signallingConnections, replicationHealth, localityPreference
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-442 (Cont.) nfScoringFactorActualValue

Field	Details
Dimension	• nfInstanceID • factor
Example	nfScoringFactorActualValue{app="testing-appinfo", app_kubernetes_io_instance="testing", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="appinfo", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.7.1.0.0", application="ocbsf", calculatedStatus="success", container="appinfo", endpoint="cnc-metrics", engVersion="22.4.0", factor="localityPreference", helm_sh_chart="appinfo-22.4.0", instance="10.233.117.146:9000", job="occne-infra/occne-nf-cnc-podmonitor", microservice="bsf-app-info", mktgVersion="1.7.1.0.0", namespace="biloxi-ns", nfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0666", pod="testing-appinfo-78dc65865f-hgrhk", pod_template_hash="78dc65865f", vendor="Oracle"} 5

Table 9-443 appinfo_dbmonitor_request_total

Field	Details
Description	On every call to DB API towards cnDBTier, this metric tracks the total instances of a last `clusterDbState` detected.
Type	Counter
Dimension	uri
Example	appinfo_dbmonitor_request_total{uri="http://occne-db-monitor-svc.dbtier-namespace:8080/db-tier/cluster/status/events/1"}

Table 9-444 appinfo_dbmonitorclusterDbState_current

Field	Details
Description	On every call to DB API towards cnDBTier, this metric tracks the currently known `clusterDbState` detected.
Type	Gauge
Dimension	state
Example	appinfo_dbmonitorclusterDbState_current{state="START"} 0

Table 9-445 appinfo_nfDbFunctionalState_change_total

Field	Details
Description	On any change to `runtime_NfDbFunctionalState`, this metric tracks the total change in NF functional state.
Type	Counter
Dimension	• autoTransitionState • previousClusterDbState • newClusterDbState • nfDbFunctionalState
Example	appinfo_nfDbFunctionalState_change_total{autoTransitionState="True",previousClusterDbState="None",newClusterDbState="",nfDbFunctionalState=""} 3.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-446 appinfo_nfDbFunctionalState_current

Field	Details
Description	On any change to `runtime_NfDbFunctionalState`, this metric tracks the current NF functional state with following dimensions.
Type	Gauge
Dimension	• autoTransitionState • clusterDbState • nfDbFunctionalState
Example	appinfo_nfDbFunctionalState_current{autoTransitionState="True",clusterDbState="",nfDbFunctionalState="Running"} 0

Table 9-447 appinfo_http_response_total

Field	Details
Description	On every call to `/status/category/dbClusterState` API, track the total response sent with following dimensions.
Type	Counter
Dimension	• responseCode • ClusterState (incase of 404, it shall be "") • NfState (incase of 404, it shall be "")
Example	appinfo_http_response_total{responseCode="200",ClusterState="",NfState=""} 16.0

For more information about dimensions, see CNC Policy Metrics.

9.19 PerfInfo Metrics

This section describes the metrics and examples for PerfInfo service.

Table 9-448 nf_load_info

Field	Details
Description	Provides information about service load.
Type	Gauge
Dimension	• service • namespace
Example	nf_load_info{namespace="xxx",service="xxx"} 0.8486912141984638

Table 9-449 jvm_cpu_usage

Field	Details
Description	Per service jvm_cpu_usage.
Type	Gauge
Dimension	• service • namespace
Example	jvm_cpu_usage{namespace="xxx",service="xxx"} 0.2758240242725142

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-450 jvm_memory

Field	Details
Description	Per service jvm_memory
Type	Gauge
Dimension	• service • namespace
Example	jvm_memory{namespace="ttz",service="xxx"} 18.361382484436035

Table 9-451 cgroup_cpu_nanoseconds

Field	Details
Description	Reports the total CPU time (in nanoseconds) on each CPU core for all the tasks in the cgroup.
Type	Gauge
Dimension	NA
Example	cgroup_cpu_nanoseconds 2.1782821080274e+013

Table 9-452 cgroup_memory_bytes

Field	Details
Description	Reports the memory usage.
Type	Gauge
Dimension	NA
Example	cgroup_memory_bytes 1.31289088e+08

Table 9-453 load_level

Field	Details
Description	This metric provides information about the load level of a service.
Type	Gauge
Dimension	• service • namespace • isLeaderPod
Example	load_level{service="xxx"} L1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-454 service_resource_stress

Field	Details
Description	This metric tracks CPU, memory, failure count, and pending requests on the basis of which the overload level of a service is calculated. PerfInfo reports the `service_resource_stress` metric when it collects data from the Gateway regardless of the presence of threshold configuration. It is necessary to have the variable `PUBLISH_STRESS_METRIC_WITHOUT_THRESHOLDS_CONFIGURED` as "true" to view this metric without threshold configurations. **Note** Add the *isLeaderPod="True"* query criteria for "Svc resource Overload Stress" and "Load Level" Grafana dashboard queries.
Type	Gauge
Dimension	• type • service • namespace • isLeaderPod
Example	service_resource_stress{isLeaderPod="True",service="my-cnpolicy-occnp-pcf-sm",type="svc_pending_count"}

Table 9-455 service_resource_overload_level

Field	Details
Description	This metric tracks an individual resource's overload level that is calculated based on the resource usage and configured threshold. **Note** Add the *isLeaderPod="True"* query criteria for "Svc resource Overload Stress" and "Load Level" Grafana dashboard queries.
Type	Gauge
Dimension	• type • service • namespace • isLeaderPod
Example	service_resource_overload_level{service="xxx", type="xxx"}2.0

Table 9-456 system_overload_threshold_config_mode

Field	Details
Description	Indicates whether the overload level threshold configuration is based on STANDALONE or PROFILE mode.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-456 (Cont.) system_overload_threshold_config_mode

Field	Details
Dimension	• namespace • isLeaderPod
Example	system_overload_threshold_config_mode 1.0

Table 9-457 active_overload_threshold_fetch_failed

Field	Details
Description	Indicates whether the active profile data is fetched successfully or failed to fetch.
Type	Gauge
Dimension	• namespace • isLeaderPod The value of this dimension can be either 0 or 1. Where 0, represents "Successfully fetched the active threshold"and 1 represents "Failure in fetching the active threshold".
Example	active_overload_threshold_fetch_failed 1.0

Table 9-458 oc_ingressgateway_route_overloadcontrol_discard_total

Field	Details
Description	This metric is pegged when incoming request is discarded by Overload Filter on priority or percentage basis.
Type	Counter
Dimension	• Method • ServiceName • Status • DiscardAction="PriorityBased" or DiscardAction="PercentageBased" • Scheme • InstanceIdentifier • ErrorOriginator • namespace
Example	-

Table 9-459 load_level_report_total

Field	Details
Description	This metric is used to track: • the number of times load level calculation is performed • the number of times load level changes • how long the particular level was active
Type	Counter
Dimension	• level • service • prevLevel • namespace • levelChangeType • isLeaderPod

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-459 (Cont.) load_level_report_total

Field	Details
Example	load_level_report_total{namespace="hi-riley", service="pcf-occnp-pcrf-core", isLeaderPod="True", level="Normal", levelChangeType="-"} 2.0

Table 9-460 service_resource_overload_level_report_total

Field	Details
Description	This metric is used to track: • the number of times load level calculation is performed. • the number of times load level changes. • for how long the particular level was active for each metric type.
Type	Counter
Dimension	• level Possible values: – L1 – L2 – L3 – Normal • service • prevLevel • levelChangeType Possible values: – increment – decrement • isLeaderPod Possible values: – True – False • type Possible values: – cpu – memory – svc_failure_count – svc_pending_count • namespace
Example	service_resource_overload_level_report_total{namespace="hi-riley", service="pcf-occnp-pcrf-core", isLeaderPod="True", level="Normal", levelChangeType="-", type="cpu"} 2.0

Table 9-461 http_out_conn_request

Field	Details
Description	This counter metric is used to count the number of http API Egress requests.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-461 (Cont.) http_out_conn_request

Field	Details
Dimension	• servicenameNon3gpp • serviceResource • serviceVersion • operationType • namespace • params • isLeaderPod
Example	-

Table 9-462 http_out_conn_response

Field	Details
Description	This counter metric is used to count the number of http API Egress responses.
Type	Counter
Dimension	• servicenameNon3gpp • serviceResource • serviceVersion • outcome • namespace • operationType • responseCode • params • cause • isLeaderPod
Example	-

Table 9-463 overload_manager_enabled

Field	Details
Description	This metric indicates whether overload manager is enabled or disabled.
Type	Gauge
Dimension	• source Possible values: – DIAM_GW – INGRESS_GW – PERF_INFO • namespace
Example	overload_manager_enabled{namespace="hi-riley", source="DIAM_GW"} 1

Table 9-464 leader_pod

Field	Details
Description	This metric is used to know the leader pod.
Type	Gauge
Dimension	• namespace

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-464 (Cont.) leader_pod

Field	Details
Example	leader_pod{namespace="hi-riley"} 1

For more information about dimensions, see CNC Policy Metrics.

9.20 Pod Congestion Metrics

This section describes the metrics and examples for pod congestion control.

> **Note**
>
> - **Current behavior in Policy services supporting Pod Congestion Observability Gauge Metrics:**
>
> In Grafana dashboard, the congestion state metric (occnp_pod_congestion_state, occnp_pod_resource_congestion_state) and rejection state metric (um_http_congestion_message_reject_total) graphs show inconsistent behavior. As in the pod congestion state graph shows to be in normal state while discard graph does not show flat line plot but with discard messages.
>
> This is caused because pods with the CPU usage level on the borderline of DANGER_OF_CONGESTION (DOC) level with sudden CPU spikes, pushes the pod to DANGER_OF_CONGESTION (DOC) state or CONGESTION_L1 state. During this CPU spike, based on the Load Shedding rule configured in CNC Console the specific requests are discarded and rejection counter metric is incremented. After the brief spike interval the congestion state is reported in Grafana dashboard as normal.
>
> Prometheus scrape metrics from its targeted instance periodically based on scrape interval. But the scrape interval is not granular enough to capture the abrupt CPU spikes. um_http_congestion_message_reject_total is visualized by using rate() function over a time duration. Due to the above cause the counter metrics increments and when averaged over a time interval the rejection plot seems to be constant although it was incremented for the requests in a few seconds when pod was in not normal state due to abrupt CPU spikes.
>
> - **Prefix and Suffix support for `pod_cong_state_report` and `pod_resource_congestion_state_report` metrics**
>
> In Policy 24.2.x, the `pod_cong_state_report` and `pod_resource_congestion_state_report` metrics supports prefix and suffix. If users have created dashboard in 24.1.x using these metrics, then they should update their dashboards by adding prefix and suffix for these metrics. The default value prefix is `occnp` and suffix is empty string.

Table 9-465 occnp_pod_congestion_state

Field	Details
Description	Tracks congestion state of pod
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-465 (Cont.) occnp_pod_congestion_state

Field	Details
Dimension	level = 0,1,2 (0 = Normal, 1 = DoC, 2 = Congested) are for Bulwark and Diameter Gateway services. level = 0,1,2,3,4 (0=Normal,1=DoC,2=Congestion_L1,3=Congestion_L2,4=Congested) are for other Policy services.
Examples	• occnp_pod_congestion_state 0.0 • occnp_pod_congestion_state 1.0

Table 9-466 occnp_pod_resource_stress

Field	Details
Description	Tracks CPU, memory, queue usage (pending requests) for binding, pds, usage monitoring and SM serivces.
Type	Gauge
Dimension	type = "Queue","CPU","Memory"
Examples	• occnp_pod_resource_stress{type="memory",} 35.0 • occnp_pod_resource_stress{type="cpu",} 50.0

Table 9-467 occnp_pod_resource_congestion_state

Field	Details
Description	Tracks individual resource's congestion state calculated based on the resource usage and configured threshold
Type	Gauge
Dimension	• type = "Queue","CPU","Memory" • level = 0,1,2 (0 = Normal, 1 = DoC, 2 = Congested) for Bulwark and Diameter Gateway services level = 0,1,2,3,4 (0=Normal,1=DoC,2=Congestion_L1,3=Congestion_L2,4=Congested) are for other Policy services
Examples	• occnp_pod_resource_congestion_state{type="memory",} 0.0 • occnp_pod_resource_congestion_state{type="cpu",} 1.0

Table 9-468 occnp_pod_cong_state_report_total

Field	Details
Description	Track the total count of change of congestion state.
Type	Counter
Dimension	• namespace • pod • old_state • new_state where, • **old_state**: Pod congestion state before transition. • **new_state**: Pod congestion state after transition.
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-469 occnp_pod_resource_congestion_state_report_total

Field	Details
Description	Track the total count of change of resource specific congestion state.
Type	Counter
Dimension	• resource • namespace • pod • old_state • new_state where, • **old_state**: Resource congestion state before transition. • **new_state**: Resource congestion state after transition.
Example	occnp_pod_resource_congestion_state_report_total{new_state="0",old_state="4",resource="cpu",} 3.0

Table 9-470 occnp_http_congestion_message_reject_total

Field	Details
Description	Tracks the rejected messages due to pod congestion.
Type	Counter
Dimension	• requestType • operationType • requestUri • rejectionCause • priority → calculated or received priority of message being rejected • responseCode → response code sent with rejected message • ocMsgPriority → oc-message-priority header value • congestion_level → current congestion state in numeric value
Example	-

Table 9-471 um_http_congestion_message_reject_total

Field	Details
Description	Usage Monitoring service tracks the rejected messages due to pod congestion.
Type	Counter
Dimension	• priority • responseCode • operation • uri
Examples	-

Table 9-472 occnp_congestion_http_pending_request_active_counter

Field	Details
Description	Track the current active counter for calculating pending HTTP requests.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-472 (Cont.) occnp_congestion_http_pending_request_active_counter

Field	Details
Dimension	• namespace • pod
Example	-

Table 9-473 occnp_congestion_diam_pending_request_active_counter

Field	Details
Description	Track the current active counter for calculating pending diameter requests.
Type	Gauge
Dimension	• namespace • pod
Example	-

Table 9-474 occnp_congestion_diam_pending_request_end_to_end_id_map_size

Field	Details
Description	Track the congestion control diameter pending requests end to end id map size.
Type	Gauge
Dimension	• namespace • pod • diameterPendingRequestsEndToEndIdMap
Example	-

Table 9-475 occnp_congestion_DiamMsgBuffer_queue_msg_count

Field	Details
Description	Track the congestion control DiamMsgBuffer queue message count.
Type	Gauge
Dimension	• namespace • pod
Example	-

For more information about dimensions, see CNC Policy Metrics.

9.21 PCRF Core Metrics

This section describes the metrics and examples for PCRF Core Metrics.

General Metrics

Table 9-476 occnp_pcrf_core_overall_processing_time_sum_total

Field	Details
Description	Sum of pcrf core overall processing time.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-476 (Cont.) occnp_pcrf_core_overall_processing_time_sum_total

Field	Details
Type	Counter
Dimension	• method • status
Example	occnp_pcrf_core_overall_processing_time_sum_total{method="auditNotification",status="200 OK",} 299.0

Table 9-477 occnp_pcrf_core_overall_processing_time_count_total

Field	Details
Description	Total number of pcrf core overall processing time.
Type	Counter
Dimension	• method • status
Example	occnp_pcrf_core_overall_processing_time_count_total{method="auditNotification",status="200 OK",} 16.0

Table 9-478 http_server_requests_seconds_count

Field	Details
Description	Number of http request received.
Type	Counter
Dimension	• method • outcome • status • uri
Example	http_server_requests_seconds_count{exception="None",method="GET",outcome="SUCCESS",status="200",uri="/pcrfSessionData",} 2.0

Table 9-479 http_server_requests_seconds_max

Field	Details
Description	Maximum number of http requests received.
Type	Counter
Dimension	• method • outcome • status • uri
Example	http_server_requests_seconds_max{exception="None",method="GET",outcome="SUCCESS",status="200",uri="/pcrfSessionData",} 0.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-480 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimension	• Service Name • Pod Name

Diameter Metrics

Table 9-481 occnp_diam_request_local_total (CCR-I)

Field	Details
Description	Number of , CCA-I initial request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType = (CCR-I, CCA-I • origHost • origRealm
Example	occnp_diam_request_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="",destRealm="oracle.com",direction="in",msgType="CCR-I",origHost="pgw1.oracle.com",origRealm="oracle.com",} 1.0 1633975504473

Table 9-482 occnp_app_request_local_process_total

Field	Details
Description	Number of requests sent to PGW during RAR flow along with number of retries sent to PGW.
Type	Counter
Dimension	• appType • destHost • destRealm • msgType • reason • retryAttempts
Example	occnp_app_request_local_process_total{appType="Gx",destHost="pgw.oracle.com",destRealm="oracle.com",msgType="RAR",reason="notification",retryAttempts="1",} 1.0

Table 9-483 occnp_app_response_local_process_total

Field	Details
Description	Number of response received from PGW during RAR flow with response code and cause.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-483 (Cont.) occnp_app_response_local_process_total

Field	Details
Dimension	• appType • errorType • msgType • reason • reqDestHost • reqDestRealm • responseType • retryAttempts
Example	occnp_app_response_local_process_total{appType="Gx",errorType="",msgType="RAA",reason="notification",reqDestHost="pgw.oracle.com",reqDestRealm="oracle.com",responseType="DIAMETER_SUCCESS",retryAttempts="1",} 1.0

Table 9-484 occnp_diam_response_local_total (CCA-I)

Field	Details
Description	Number of CCA initial response received.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	occnp_diam_response_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="",destRealm="",direction="out",msgType="CCA-I",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="",reqDestRealm="oracle.com",reqOrigHost="pgw1.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 1.0 1633975504473

Table 9-485 occnp_diam_request_local_total (CCR-U)

Field	Details
Description	Number of CCR update request sent.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-485 (Cont.) occnp_diam_request_local_total (CCR-U)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	occnp_diam_request_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="XYZ-IN.us.oracle.com",destRealm="oracle.com",direction="in",msgType="CCR-U",origHost="pgw1.oracle.com",origRealm="oracle.com",} 1.0 1633975504473

Table 9-486 occnp_diam_response_local_total (CCA-U)

Field	Details
Description	Number of CCA update response received.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	occnp_diam_response_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="",destRealm="",direction="out",msgType="CCA-U",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="XYZ-IN.us.oracle.com",reqDestRealm="oracle.com",reqOrigHost="pgw1.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 1.0 1633975504473

Table 9-487 occnp_diam_request_local_total (CCR-T)

Field	Details
Description	Number of CCR terminate request sent.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-487 (Cont.) occnp_diam_request_local_total (CCR-T)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	• occnp_diam_request_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="",destRealm="oracle.com",direction="in",msgType="CCR-T",origHost="pgw1.oracle.com",origRealm="oracle.com",} 1.0 1633975504473 • occnp_diam_request_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="XYZ-IN.us.oracle.com",destRealm="oracle.com",direction="in",msgType="CCR-T",origHost="pgw1.oracle.com",origRealm="oracle.com",} 1.0 1633975504473

Table 9-488 occnp_diam_response_local_total (CCA-T)

Field	Details
Description	Number of CCA terminate response received.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	• occnp_diam_response_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="",destRealm="",direction="out",msgType="CCA-T",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="",reqDestRealm="oracle.com",reqOrigHost="pgw1.oracle.com",reqOrigRealm="oracle.com",responseCode="5002",} 1.0 1633975504473 • occnp_diam_response_local_total{appId="16777238",appType="Gx",cmdCode="272",destHost="",destRealm="",direction="out",msgType="CCA-T",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="XYZ-IN.us.oracle.com",reqDestRealm="oracle.com",reqOrigHost="pgw1.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 1.0 1633975504473

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-489 occnp_diam_request_local_total (AAR-I)

Field	Details
Description	Number of AAR initial request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	occnp_diam_request_local_total{appId="16777236",appType="Rx",cmdCode="265",destHost="",destRealm="oracle.com",direction="in",msgType="AAR-I",origHost="af.oracle.com", origRealm="oracle.com",} 1.0 1634756738735

Table 9-490 occnp_diam_response_local_total (AAA-I)

Field	Details
Description	Number of AAA initial response received.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	occnp_diam_response_local_total{appId="16777236",appType="Rx",cmdCode="265",destHost="", destRealm="",direction="out",msgType="AAA-I",origHost="XYZ-IN.us.oracle.com", origRealm="oracle.com",reqDestHost="",reqDestRealm="oracle.com",reqOrigHost="af.oracle.com" ,reqOrigRealm="oracle.com",responseCode="5065",} 2.0 1634756738735

Table 9-491 occnp_diam_request_local_total (AAR-U)

Field	Details
Description	Number of AAR modify requests sent.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-491 (Cont.) occnp_diam_request_local_total (AAR-U)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	occnp_diam_request_local_total{appId="16777236",appType="Rx",cmdCode="265",destHost="pcrf-core",destRealm="oracle.com",direction="in",msgType="AAR-U",origHost="af.oracle.com",origRealm="oracle.com",} 1.0 1635332966264

Table 9-492 occnp_diam_response_local_total (AAA-U)

Field	Details
Description	Number of AAA modify responses received.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	occnp_diam_response_local_total{appId="16777236",appType="Rx",cmdCode="265",destHost="",destRealm="",direction="out",msgType="AAA-U",origHost="pcrf-core",origRealm="oracle.com",reqDestHost="pcrf-core",reqDestRealm="oracle.com",reqOrigHost="af.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 1.0 1635332966264

Table 9-493 occnp_diam_request_local_total (RAR Gx)

Field	Details
Description	Number of RAR Gx request received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-493 (Cont.) occnp_diam_request_local_total (RAR Gx)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm

Table 9-494 occnp_diam_response_local_total (RAA Gx)

Field	Details
Description	Number of RAR Gx response received.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode

Table 9-495 occnp_diam_request_local_total (RAR Rx)

Field	Details
Description	Number of RAR Rx request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-496 occnp_diam_response_local_total (RAA Rx)

Field	Details
Description	Number of RAA Rx response received.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode

Table 9-497 occnp_diam_request_local_total (STR)

Field	Details
Description	Number of STR request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	occnp_diam_request_local_total{appId="16777236",appType="Rx",cmdCode="275",destHost="XYZ-IN.us.oracle.com",destRealm="oracle.com",direction="in", msgType="STR",origHost="app.oracle.com",origRealm="oracle.com",} 2.0 1635332966264

Table 9-498 occnp_diam_response_local_total (STA)

Field	Details
Description	Number of STA response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-498 (Cont.) occnp_diam_response_local_total (STA)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	• occnp_diam_response_local_total{appId="16777236",appType="Rx",cmdCode="275",destHost="",destRealm="",direction="out",msgType="STA",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="",reqDestRealm="oracle.com",reqOrigHost="app.oracle.com",reqOrigRealm="oracle.com",responseCode="5002",} 1.0 1635332966264 • occnp_diam_response_local_total{appId="16777236",appType="Rx",cmdCode="275",destHost="",destRealm="",direction="out",msgType="STA",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="",reqDestRealm="oracle.com",reqOrigHost="app.oracle.com",reqOrigRealm="oracle.com",responseCode="5002",} 1.0 1635332966264

Table 9-499 occnp_diam_request_local_total (ASR)

Field	Details
Description	Number of ASR request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	occnp_diam_request_local_total{appId="16777236",appType="Rx",cmdCode="274",destHost="af.oracle.com",destRealm="oracle.com",direction="out",msgType="ASR",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",} 1.0 1638875554937

Table 9-500 occnp_diam_response_local_total (ASA)

Field	Details
Description	Number of ASA response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-500 (Cont.) occnp_diam_response_local_total (ASA)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	• occnp_diam_response_local_total{appId="16777236",appType="Rx",cmdCode="274",destHost="",destRealm="",direction="in",msgType="ASA",origHost="app.oracle.com", origRealm="oracle.com",reqDestHost="",reqDestRealm="",reqOrigHost="",reqOrigRealm="",responseCode="2001",} 2.0 1635332966264 • occnp_diam_response_local_total{appId="16777236",appType="Rx",cmdCode="274",destHost="",destRealm="",direction="in",msgType="ASA",origHost="",origRealm="",reqDestHost="af.oracle.com",reqDestRealm="oracle.com",reqOrigHost="XYZ-IN.us.oracle.com",reqOrigRealm="oracle.com",responseCode="timeout",} 1.0 1638875554937

Table 9-501 occnp_diam_request_local_total (CER)

Field	Details
Description	Number of CER request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	occnp_diam_request_local_total{appId="0",appType="",cmdCode="257",destHost="",destRealm="",direction="in",msgType="CER",origHost="app.oracle.com", origRealm="oracle.com",} 1.0 1638278712308

Table 9-502 occnp_diam_response_local_total (CEA)

Field	Details
Description	Number of CEA response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-502 (Cont.) occnp_diam_response_local_total (CEA)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	occnp_diam_response_local_total{appId="0",appType="",cmdCode="257",destHost="",destRealm="",direction="out",msgType="CEA",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="",reqDestRealm="",reqOrigHost="pgw1.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 3.0 1638278712308

Table 9-503 occnp_diam_request_local_total (DWR)

Field	Details
Description	Number of DWR request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Examples	• occnp_diam_request_local_total{appId="0",appType="",cmdCode="280",destHost="",destRealm="",direction="out",msgType="DWR",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",} 297.0 1638278712308 • occnp_diam_request_local_total{appId="0",appType="",cmdCode="280",destHost="",destRealm="",direction="in",msgType="DWR",origHost="pgw.oracle.com",origRealm="oracle.com",} 4.0 1640076342932

Table 9-504 occnp_diam_response_local_total (DWA)

Field	Details
Description	Number of DWA response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-504 (Cont.) occnp_diam_response_local_total (DWA)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	• occnp_diam_response_local_total{appId="0",appType="",cmdCode="280",destHost="",destRealm="",direction="in",msgType="DWA",origHost="pgw1.oracle.com",origRealm="oracle.com",reqDestHost="",reqDestRealm="",reqOrigHost="XYZ-IN.us.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 296.0 1638278712308 • occnp_diam_response_local_total{appId="0",appType="",cmdCode="280",destHost="",destRealm="",direction="out",msgType="DWA",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",reqDestHost="",reqDestRealm="",reqOrigHost="pgw.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 4.0 1640076342932

Table 9-505 occnp_diam_request_local_total (DPR)

Field	Details
Description	Number of DPR request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Example	occnp_diam_request_local_total{appId="0",appType="",cmdCode="282",destHost="",destRealm="",direction="in",msgType="DPR",origHost="pgw1.oracle.com", origRealm="oracle.com",} 1.0 1638278712308

Table 9-506 occnp_diam_response_local_total (DPA)

Field	Details
Description	Number of DPA response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-506 (Cont.) occnp_diam_response_local_total (DPA)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Example	occnp_diam_response_local_total{appId="0",appType="",cmdCode="282",destHost="",destRealm="",direction="out",msgType="DPA",origHost="XYZ-IN.us.oracle.com", origRealm="oracle.com",reqDestHost="",reqDestRealm="",reqOrigHost="pgw1.oracle.com",reqOrigRealm="oracle.com",responseCode="2001",} 1.0 1638278712308

Table 9-507 occnp_diam_request_local_total (Timeout Metric RAR)

Field	Details
Description	Number of timeout RAR request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm
Examples	• occnp_diam_request_local_total{appId="16777238",appType="Gx",cmdCode="258",destHost="pgw1.oracle.com",destRealm="oracle.com",direction="out",msgType="RAR", origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",} 6.0 1635335195027 • occnp_diam_request_local_total{appId="16777236",appType="Rx",cmdCode="258",destHost="af.oracle.com",destRealm="oracle.com",direction="out",msgType="RAR", origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",} 1.0 1635425739107 • occnp_diam_request_local_total{appId="16777238",appType="Gx",cmdCode="258",destHost="pgw1.oracle.com",destRealm="oracle.com",direction="out",msgType="RAR",origHost="XYZ-IN.us.oracle.com",origRealm="oracle.com",} 3.0 1638875554937

Table 9-508 occnp_diam_response_local_total (Timeout Metric RAA)

Field	Details
Description	Number of timeout RAA response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-508 (Cont.) occnp_diam_response_local_total (Timeout Metric RAA)

Field	Details
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode
Examples	• occnp_diam_response_local_total{appId="16777236",appType="Rx",cmdCode="258",destHost="",destRealm="",direction="in",msgType="RAA",origHost="app.oracle.com",origRealm="oracle.com", reqDestHost="",reqDestRealm="",reqOrigHost="",reqOrigRealm="",responseCode="2001",} 1.0 1635425739107 • occnp_diam_response_local_total{appId="16777238",appType="Gx",cmdCode="258",destHost="",destRealm="",direction="in",msgType="RAA",origHost="pgw1.oracle.com", origRealm="oracle.com",reqDestHost="",reqDestRealm="",reqOrigHost="",reqOrigRealm="",responseCode="2001",} 1.0 1638875554937 • occnp_diam_response_local_total{appId="16777238",appType="Gx",cmdCode="258",destHost="",destRealm="",direction="in",msgType="RAA",origHost="",origRealm="",reqDestHost="pgw1.oracle.com",reqDestRealm="oracle.com",reqOrigHost="XYZ-IN.us.oracle.com",reqOrigRealm="oracle.com",responseCode="timeout",} 2.0 1638875554937

Table 9-509 occnp_diam_request_local_total (Timeout Metric ASR)

Field	Details
Description	Number of timeout ASR request sent.
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm

Table 9-510 occnp_diam_response_local_total (Timeout Metric ASA)

Field	Details
Description	Number of timeout ASA response received.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-510 (Cont.) occnp_diam_response_local_total (Timeout Metric ASA)

Field	Details
Type	Counter
Dimension	• appId • appType • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • reqDestHost • reqDestRealm • reqOrigHost • reqOrigRealm • responseCode

Bulwark Metrics

Table 9-511 occnp_http_bulwark_lock_request_total

Field	Details
Description	Number of bulwark lock requests sent.
Type	Counter
Dimension	• application • instanceId • operationType • msgType
Example	occnp_http_bulwark_lock_request_total{application="occnp-pcrf-core",instanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",msgType="create",operationType="bulwark_lock",} 2.0

Table 9-512 occnp_http_bulwark_lock_response_total

Field	Details
Description	Number of bulwark lock response received.
Type	Counter
Dimension	• application • instanceId • operationType • responseCode • msgType
Example	occnp_http_bulwark_lock_response_total{application="occnp-pcrf-core",instanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",msgType="create",operationType="bulwark_lock",responseCode="201",} 2.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-513 occnp_http_bulwark_unlock_request_total

Field	Details
Description	Number of bulwark unlock requests sent.
Type	Counter
Dimension	• application • instanceId • operationType • msgType
Example	occnp_http_bulwark_unlock_request_total{application="occnp-pcrf-core",instanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",msgType="create",operationType="bulwark_unlock",} 2.0

Table 9-514 occnp_http_bulwark_unlock_response_total

Field	Details
Description	Number of bulwark unlock response received.
Type	Counter
Dimension	• application • instanceId • operationType • responseCode • msgType
Example	occnp_http_bulwark_unlock_response_total{application="occnp-pcrf-core",instanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",msgType="create",operationType="bulwark_unlock",responseCode="204",} 2.0

Binding and PRE Metrics

Table 9-515 http_out_conn_request_total

Field	Details
Description	Number of connection requests sent.
Type	Counter
Dimension	• application • operationType • serviceResource
Example	http_out_conn_request_total{application="pcrf-core",operationType="DELETE",serviceResource="Binding",} 28.0

Table 9-516 http_out_conn_response_total

Field	Details
Description	Number of connection response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-516 (Cont.) http_out_conn_response_total

Field	Details
Dimension	• application • operationType • responseCode • serviceResource
Example	http_out_conn_response_total{application="pcrf-core",operationType="POST",responseCode="201",serviceResource="Binding",} 33.0

Table 9-517 pcrf_core_binding_ex_total

Field	Details
Description	Accounts for any exceptions that occurred during API calls toward Binding service.
Type	Counter
Dimension	• application • operationType • exception_type
Example	**General Metrics** pcrf_core_binding_ex_total{application="occnp-pcrf-core",exception_type="java.util.concurrent.TimeoutException",operationType="POST",} 2.0 dimensions: **Binding and Pre Metrics** pcrf_core_binding_ex_total{application="occnp-pcrf-core",exception_type="java.util.concurrent.TimeoutException",operationType="POST",} 2.0

Webclient Metrics

Table 9-518 occnp_webclient_sum_total

Field	Details
Description	Sum of webclient requests.
Type	Counter
Dimension	• method • status_code • url
Example	occnp_webclient_sum_total{method="POST",status_code="201",url="/binding/v1/dependentContextBinding/context-owner/PCRF-CORE",} 201.0

Table 9-519 occnp_webclient_count_total

Field	Details
Description	Number of webclient requests.
Type	Counter
Dimension	• method • status_code • url

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-519 (Cont.) occnp_webclient_count_total

Field	Details
Example	occnp_webclient_count_total{method="POST",status_code="201",url="/binding/v1/dependentContextBinding/context-owner/PCRF-CORE",} 6.0

JDBC Metrics

Table 9-520 occnp_jdbc_operation_count_total

Field	Details
Description	Number of jdbc operations.
Type	Counter
Dimension	• method • state • table
Example	occnp_jdbc_operation_count_total{method="removeSQL",state="SUCCESS",table="rxsession",} 6.0

Table 9-521 occnp_jdbc_operation_sum_total

Field	Details
Description	Sum of jdbc operations.
Type	Counter
Dimension	• method • state • table
Example	occnp_jdbc_operation_sum_total{method="removeSQL",state="SUCCESS",table="rxsession",} 25.0

Session Viewer Metrics

Table 9-522 session_oam_request_total

Field	Details
Description	Total number of oam requests sent.
Type	Counter
Dimension	• application • operationType • sessionType
Example	session_oam_request_total{application="pcf_smservice",operationType="terminate",sessionType="SM"} 2.0

Table 9-523 session_oam_response_total

Field	Details
Description	Total number of oam response received.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-523 (Cont.) session_oam_response_total

Field	Details
Dimension	• application • operationType • responseCode • sessionType
Example	session_oam_response_total{application="pcf_smservice",operationType="terminate",responseCode="5xx",sessionType="SM"} 1.0

Jetty HTTP client request timing Metrics

Table 9-524 jetty_client_requests_seconds_max

Field	Details
Description	Number of jetty client requests.
Type	Counter
Dimension	• exception • host • method • outcome • status • uri
Example	jetty_client_requests_seconds_max{exception="None",host="pdincredpolicy-occnp-binding",method="DELETE",outcome="SUCCESS",status="204",uri="",} 0.0

Table 9-525 jetty_client_requests_seconds_sum

Field	Details
Description	Measures the total time spent processing client requests.
Type	Counter
Dimension	• exception • host • method • outcome • status • uri
Example	jetty_client_requests_seconds_sum{exception="None",host="pdincredpolicy-occnp-binding",method="DELETE",outcome="SUCCESS",status="204",uri="",} 0.831213657

Table 9-526 jetty_client_requests_sum_total

Field	Details
Description	measures the total count of client requests.
Type	Counter
Dimension	• method • status_code • url

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-526 (Cont.) jetty_client_requests_sum_total

Field	Details
Example	jetty_client_requests_sum_total{method="POST",status_code="201",url="/binding/v1/dependentContextBinding/context-owner/PCRF-CORE",} 199.0

Table 9-527 jetty_client_request_size_sum_total

Field	Details
Description	Sum of jetty client request size.
Type	Counter
Dimension	• method • status_code • url
Example	jetty_client_request_size_sum_total{method="DELETE",status_code="204",url="/binding/v1/dependentContextBinding/dependentContextId",} 0.0

Table 9-528 jetty_client_requests_count_total

Field	Details
Description	Number of jetty client requests.
Type	Counter
Dimension	• method • status_code • url
Example	jetty_client_requests_count_total{method="POST",status_code="201",url="/binding/v1/dependentContextBinding/context-owner/PCRF-CORE",} 6.0

Cgroup Metrics

Table 9-529 cgroup_cpu_nanoseconds

Field	Details
Description	Reports the total CPU time (in nanoseconds) on each CPU core for all the tasks in the cgroup.
Type	Gauge
Dimension	NA
Example	cgroup_cpu_nanoseconds 2.1782821080274e+013

Table 9-530 cgroup_memory_bytes

Field	Details
Description	Reports the memory usage.
Type	Gauge
Dimension	NA
Example	cgroup_memory_bytes 1.31289088e+08

Copyright © 2019, 2026, Oracle and/or its affiliates.

Startup Probe Metrics

Table 9-531 config_client_audit_complete

Field	Details
Description	Reports the audit completion of config client.
Type	Gauge
Dimension	auditor
Example	config_client_audit_complete_total{auditor="configClientAuditor",} 7768.0

Database Data Encoding Metrics

Table 9-532 occnp_data_encoding_total

Field	Details
Description	PCRF Core gxsession, rxsession and sdsession total of encoded data.
Type	Counter
Dimension	• db (occnp_pcrf_core) • table (gxsession, rxsession, sdsession) • decodingVer (mapping version number used for decoding)
Example	

Table 9-533 occnp_data_decoding_total

Field	Details
Description	PCRF Core gxsession, rxsession and sdsession total of decoded data.
Type	Counter
Dimension	• db (occnp_pcrf_core) • table (gxsession, rxsession, sdsession) • decodingVer (mapping version number used for decoding)
Example	

Table 9-534 occnp_data_decoding_fail_total

Field	Details
Description	PCRF Core gxsession, rxsession and sdsession total of decoding failures
Type	Counter
Dimension	• db (occnp_pcrf_core) • table (gxsession, rxsession, sdsession) • decodingVer (mapping version number used for decoding) • errorCause (json_processing_exception, encode_version_null, empty_key_value_map)
Example	

Table 9-535 occnp_data_encoding_size_before_total

Field	Details
Description	PCRF Core gxsession, rxsession and sdsession total size before encoding.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-535 (Cont.) occnp_data_encoding_size_before_total

Field	Details
Type	Counter
Dimension	• db (occnp_pcrf_core) • table (gxsession, rxsession, sdsession)
Example	

Table 9-536 occnp_data_encoding_size_after_total

Field	Details
Description	PCRF Core gxsession, rxsession and sdsession total size after encoding.
Type	Counter
Dimension	• db (occnp_pcrf_core) • table (gxsession, rxsession, sdsession)
Example	

9.22 Late Arrival Requests and Collision Detection Metrics

The following table describes the late arrival requests and collision detection metrics and their respective dimensions:

Table 9-537 ocpm_late_arrival_rejection_total

Field	Details
Description	Metric that increments when AM, UE, or SM Policy Association late arriving requests are detected and rejected.
Type	Counter
Dimensions	• cause type • servicename_3gpp • operation_type

Table 9-538 ocpm_collision_detection_total

Field	Details
Description	Metric that increments when AM, UE, or SM Policy Association duplicate records are detected and deleted or rejected.
Type	Counter
Dimensions	• service_name • operation_type • cause

For more information about Dimensions, see CNC Policy Metrics.

9.23 Notifier Metrics

The following table describes the Notifier service metrics and their respective dimensions:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-539 http_notification_request_total

Field	Details
Description	This metric tracks the total number of requests towards a given destination.
Type	Counter
Dimensions	notificationEndpoint = IP or FQDN of endpoint version: http1 or http2 https = true or false contentType = <From Content-type header> method = <HTTP method for notification>

Table 9-540 http_notification_response_total

Field	Details
Description	This metric tracks the total number of responses from a given destination.
Type	Counter
Dimensions	notificationEndpoint = IP or FQDN of endpoint version: http1 or http2 https = true or false contentType = <From Content-type header> method = <HTTP method for notification> responseCode = Response code

Table 9-541 http_notification_request_timeout_total

Field	Details
Description	This metric indicates the request timeout period. That is, the maximum time for which the request can last, after which it is considered as timeout.
Type	Counter
Dimensions	notificationEndpoint = IP or FQDN of endpoint version: http11 https = false contentType = <From Content-type header> method = <HTTP method for notification>

Table 9-542 http_in_conn_request_total

Field	Details
Description	This metric indicates the request coming from PRE
Type	Counter
Dimensions	• OperationType : NOTIFY • servicenameNon3gpp : notifier
Example	occnp_http_in_conn_request_total{operationType="NOTIFY",servicenameNon3gpp="notifier",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-543 http_in_conn_response_total

Field	Details
Description	This metric indicates the response sent to PRE
Type	Counter
Dimensions	• OperationType : NOTIFY • responseCode • servicenameNon3gpp : notifier • cause:SMPP is not enabled
Example	occnp_http_in_conn_response_total{operationType="NOTIFY",responseCode="204 NO_CONTENT",servicenameNon3gpp="notifier",} 1.0

Table 9-544 smpp_request_total

Field	Details
Description	This metric indicates the requests sent towards external endpoint such as SMS Gateway and the delivery receipts received.
Type	Counter
Dimensions	• notificationServer: (sms gateway name) • smscName: name • direction:(in/out) • requestType: bind/ unbind/submit_sm/deliver_sm • deliveryMethod: SAR/MESSAGE_PAYLOAD
Examples	• occnp_smpp_request_total{direction="out",notificationServer="gw1",requestType="submit_sm",smscName="host3",} 1.0 • occnp_smpp_request_total{direction="out",notificationServer="",requestType="unbind",smscName="host3",} 1.0 • ccnp_smpp_request_total{direction="out",notificationServer="",requestType="bind",smscName="host3",} 1.0 • occnp_smpp_request_total{direction="in",notificationServer="",requestType="deliver_sm",smscName="host3",} 1.0 • occnp_smpp_request_total{direction="out",notificationServer="sms-gw-1",requestType="submit_sm",smscName="host3",} 1.0

Table 9-545 smpp_response_total

Field	Details
Description	Indicates the number of respoinses received from an external endpoint
Type	Counter
Dimensions	• notificationServer: (sms gateway name) • smscName: hostname • response : (SUCCESS, FAILURE, UNKNOWN) • requestType: bind_resp/unbind_resp/submit_sm_resp/deliver_sm_resp • latency: • cause: (ENROUTE, DELIVRD, EXPIRED,DELETED,UNDELIV,ACCEPTD, UNKNOWN,REJECTD)

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-545 (Cont.) smpp_response_total

Field	Details
Examples	• occnp_smpp_response_total{cause="",direction="in",latency="0",notificationServer="sms-gw-1",requestType="submit_sm_resp",response="SUCCESS",smscName="host3",} 1.0 • occnp_smpp_response_total{cause="",direction="in",latency="9",notificationServer="",requestType="bind_resp",response="SUCCESS",smscName="host3",} 1.0 • occnp_smpp_response_total{cause="",direction="in",latency="0",notificationServer="",requestType="unbind_resp",response="SUCCESS",smscName="host3",} 1.0 • occnp_smpp_response_total{cause="DELIVRD",direction="out",latency="0",notificationServer="",requestType="deliver_sm_resp",response="SUCCESS",smscName="host3",} 1.0 • occnp_smpp_response_total{cause="",direction="in",latency="9",notificationServer="gw1",requestType="submit_sm_resp",response="SUCCESS",smscName="host3",} 1.0

Table 9-546 active_smsc_conn_count

Field	Details
Description	captures total number of active connection with smsc hosts.
Type	Gauge
Dimensions	smscName: name
Example	occnp_active_smsc_conn_count{smscName="host3",} 1.0

Table 9-547 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimensions	• Service Name • Pod Name

Histograms

```
# HELP occnp_smpp_message_processing_latency_seconds
# TYPE occnp_smpp_message_processing_latency_seconds histogram
occnp_smpp_message_processing_latency_seconds{requestType="bind",quantile="0.5
",} 1.207959552
occnp_smpp_message_processing_latency_seconds{requestType="bind",quantile="0.9
",} 2.483027968
occnp_smpp_message_processing_latency_seconds{requestType="bind",quantile="0.9
5",} 2.483027968
occnp_smpp_message_processing_latency_seconds{requestType="bind",quantile="0.9
9",} 2.483027968
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="0.
01",} 0.0
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="0.
02",} 0.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="0.
04",} 0.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="0.
08",} 2.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="0.
1",} 2.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="0.
2",} 2.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="0.
5",} 2.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="1.
0",} 70.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="5.
0",} 73.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="bind",le="+I
nf",} 73.0
occnp_smpp_message_processing_latency_seconds_count{requestType="bind",} 73.0
occnp_smpp_message_processing_latency_seconds_sum{requestType="bind",} 55.069

occnp_smpp_message_processing_latency_seconds{requestType="submit_sm",quantile
="0.5",} 0.014680064
occnp_smpp_message_processing_latency_seconds{requestType="submit_sm",quantile
="0.9",} 0.01835008
occnp_smpp_message_processing_latency_seconds{requestType="submit_sm",quantile
="0.95",} 0.01835008
occnp_smpp_message_processing_latency_seconds{requestType="submit_sm",quantile
="0.99",} 0.01835008
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="0.01",} 3.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="0.02",} 6.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="0.04",} 6.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="0.08",} 7.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="0.1",} 7.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="0.2",} 7.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="0.5",} 7.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="1.0",} 7.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="5.0",} 7.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="submit_sm",l
e="+Inf",} 8.0
occnp_smpp_message_processing_latency_seconds_count{requestType="submit_sm",}
8.0
occnp_smpp_message_processing_latency_seconds_sum{requestType="submit_sm",}
6.084

occnp_smpp_message_processing_latency_seconds{requestType="unbind",quantile="0
.5",} 0.017825792
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
occnp_smpp_message_processing_latency_seconds{requestType="unbind",quantile="0
.9",} 0.017825792
occnp_smpp_message_processing_latency_seconds{requestType="unbind",quantile="0
.95",} 0.017825792
occnp_smpp_message_processing_latency_seconds{requestType="unbind",quantile="0
.99",} 0.017825792
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
0.01",} 0.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
0.02",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
0.04",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
0.08",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
0.1",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
0.2",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
0.5",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
1.0",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
5.0",} 1.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="unbind",le="
+Inf",} 1.0
occnp_smpp_message_processing_latency_seconds_count{requestType="unbind",} 1.0
occnp_smpp_message_processing_latency_seconds_sum{requestType="unbind",} 0.018


occnp_smpp_message_processing_latency_seconds{requestType="deliver_sm",quantil
e="0.5",} 0.009404416
occnp_smpp_message_processing_latency_seconds{requestType="deliver_sm",quantil
e="0.9",} 0.015171584
occnp_smpp_message_processing_latency_seconds{requestType="deliver_sm",quantil
e="0.95",} 0.015171584
occnp_smpp_message_processing_latency_seconds{requestType="deliver_sm",quantil
e="0.99",} 0.015171584
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="0.01",} 3.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="0.02",} 4.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="0.04",} 4.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="0.08",} 4.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="0.1",} 4.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="0.2",} 4.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="0.5",} 4.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="1.0",} 4.0
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="5.0",} 4.0
```


Copyright © 2019, 2026, Oracle and/or its affiliates.

```
occnp_smpp_message_processing_latency_seconds_bucket{requestType="deliver_sm",
le="+Inf",} 4.0
occnp_smpp_message_processing_latency_seconds_count{requestType="deliver_sm",}
 4.0
occnp_smpp_message_processing_latency_seconds_sum{requestType="deliver_sm",}
0.035


# HELP occnp_smpp_message_processing_latency_seconds_max
# TYPE occnp_smpp_message_processing_latency_seconds_max gauge
occnp_smpp_message_processing_latency_seconds_max{requestType="bind",} 0.803
occnp_smpp_message_processing_latency_seconds_max{requestType="unbind",} 0.018
occnp_smpp_message_processing_latency_seconds_max{requestType="submit_sm",}
0.025
occnp_smpp_message_processing_latency_seconds_max{requestType="deliver_sm",}
0.015
```

9.24 Usage Monitoring Metrics

The following table describes the Usage Monitoring service metrics and their respective dimensions:

Table 9-548 usage_mon_ingress_request_total

Field	Details
Description	This metric is incremented when Usage Monitoring service receives an incoming HTTP request message.
Type	Counter
Dimensions	• requestor_nf • operation_type • dnn • snssai • hostname
Example	-

Table 9-549 usage_mon_ingress_response_total

Field	Details
Description	This metric is incremented when Usage Monitoring service responds to an incoming HTTP request message.
Type	Counter
Dimensions	• requestor_nf • operation_type • dnn • snssai • response_code • latency • hostname
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-550 usage_mon_profile_activated_total

Field	Details
Description	This metric is incremented when UM Data Limit Profile is activated.
Type	Counter
Dimensions	• limit_id • hostname
Example	usage_mon_profile_activated_total {hostname="ocpcf-usage-mon-b564d6cf8-shzhg",limit_id="mk1",} 3.0

Table 9-551 occnp_usage_mon_profile_selected_total

Field	Details
Description	This metric is incremented when UM Data Limit Profile is selected.
Type	Counter
Dimensions	• limit_id • hostname
Example	usage_mon_profile_selected_total{hostname="ocpcf-usage-mon-b564d6cf8-shzhg",limit_id="mk1",} 7.0

Note

When the Data Limit Profile is received from UDR, occnp_usage_mon_limit_selected metric is pegged and when Data Limit Profile is received through CNC Console, occnp_usage_mon_profile_selected metric is pegged.

Table 9-552 usage_mon_grant_success_total

Field	Details
Description	This metric is incremented when a grant is successfully allocated from a given UM Data Limit Profile.
Type	Counter
Dimensions	• limit_id • hostname
Example	-

Table 9-553 usage_mon_grant_failure_total

Field	Details
Description	This metric is incremented when a grant could not be allocated from a given UM Data Limit Profile.
Type	Counter
Dimensions	• limit_id • hostname
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-554 usage_mon_usage_reported_total

Field	Details
Description	This metric is incremented when usage report is processed for a given UM Data Limit Profile.
Type	Counter
Dimensions	• limit_id • hostname
Example	usage_mon_usage_reported_total {hostname="ocpcf-usage-mon-b564d6cf8-shzhg",limit_id="mk1",} 9.0

Table 9-555 usage_mon_usage_threshold_total

Field	Details
Description	This metric is incremented when usage usage crosses a particular threshold level.
Type	Counter
Dimensions	• limit_id • level • hostname
Example	-

Table 9-556 usage_mon_usage_reset_total

Field	Details
Description	This metric is incremented when usage is reset according to the reset time in a given UM Data Limit Profile.
Type	Counter
Dimensions	• limit_id • hostname
Example	-

Table 9-557 usage_mon_egress_pds_request_total

Field	Details
Description	This metric is incremented when Usage Monitoring service sends a request to PDS service.
Type	Counter
Dimensions	• operation_type • hostname
Example	-

Table 9-558 usage_mon_egress_pds_response_total

Field	Details
Description	This metric is incremented when Usage Monitoring service receives a response from PDS service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-558 (Cont.) usage_mon_egress_pds_response_total

Field	Details
Type	Counter
Dimensions	• operation_type • response_code • latency • hostname
Example	-

Table 9-559 session_oam_request_total

Field	Details
Description	This metric is pegged when Session Viewer API is called to get the number of session requests.
Type	Request
Dimensions	• Operation Type • Session Type • hostname
Example	session_oam_request_total {hostname="ocpcf-usage-mon-b564d6cf8-shzhg",operation_type="get",session_type="um_session",}1.0

Table 9-560 session_oam_response_total

Field	Details
Description	This metric is pegged when Session Viewer API is called to get the number of session responses.
Type	Response
Dimensions	• Response Code • Operation Type • Session Type • hostname
Example	session_oam_response_total {hostname="ocpcf-usage-mon-b564d6cf8-shzhg",operation_type="get",response_code="2xx",session_type="um_session",}1.0

Table 9-561 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimensions	• Service Name • Pod Name • hostname
Example	-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-562 occnp_db_overall_processing_time_seconds_count

Field	Details
Description	Indicates the count of the overall processing time on UmDataContext table for Usage Monitoring.
Type	Gauge
Dimensions	• Table • Method • Status • compressionScheme • hostname
Example	occnp_db_overall_processing_time_seconds_count {Method="get",Status="Success",Table="UmContext",compressionScheme="DISABLED",hostname="ocpcf-usage-mon-b564d6cf8-shzhg",} 30.0 occnp_db_overall_processing_time_seconds_count{Method="put",Status="Success",Table="UmContext",compressionScheme="DISABLED",hostname="ocpcf-usage-mon-b564d6cf8-shzhg",} 29.0 occnp_db_overall_processing_time_seconds_count{Method="delete",Status="Success",Table="UmContext",compressionScheme="",hostname="ocpcf-usage-mon-b564d6cf8-shzhg",} 6.0

Table 9-563 occnp_db_overall_processing_time_seconds_sum

Field	Details
Description	Indicates the sum of the overall processing time on UmDataContext table for Usage Monitoring.
Type	Gauge
Dimensions	• Table • Method • Status • compressionScheme • hostname
Example	occnp_db_overall_processing_time_seconds_sum{Method="get",Status="Success",Table="UmContext",compressionScheme="DISABLED",hostname="ocpcf-usage-mon-b564d6cf8-shzhg",}0.110589513 occnp_db_overall_processing_time_seconds_sum{Method="put",Status="Success",Table="UmContext",compressionScheme="DISABLED",hostname="ocpcf-usage-mon-b564d6cf8-shzhg",}0.139773756 occnp_db_overall_processing_time_seconds_sum{Method="delete",Status="Success",Table="UmContext",compressionScheme="",hostname="ocpcf-usage-mon-b564d6cf8-shzhg",}0.012469739

Table 9-564 usage_mon_context_found_total

Field	Details
Description	This metric is incremented when session lookup happens on the main table or sliced tables for old sessions of the subscribers when table slicing is enabled.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-564 (Cont.) usage_mon_context_found_total

Field	Details
Dimensions	• table_count • operation_type • table_number • hostname
Example	-

Table 9-565 occnp_um_audit_deleted_maxttl

Field	Details
Description	This metric is incremented when MaxTTL is reached for a enforcement session.
Type	Counter
Dimensions	• siteId • hostname
Example	-

Table 9-566 occnp_um_audit_query_sent_total

Field	Details
Description	This metric is incremented when the Usage Monitoring service sends a query to PCRF Core to check session staleness.
Type	Counter
Dimensions	• siteId • hostname
Example	-

Table 9-567 occnp_um_audit_session_found_total

Field	Details
Description	This metric is incremented when Usage Monitoring receives 2xx response code from PCRF Core for a session GET request.
Type	Counter
Dimensions	• siteId • hostname
Example	-

Table 9-568 occnp_um_audit_session_not_found_total

Field	Details
Description	This metric is incremented when Usage Monitoring receives 404 response code from PCRF Core for session GET request.
Type	Counter
Dimensions	• siteId • hostname

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-568 (Cont.) occnp_um_audit_session_not_found_total

Field	Details
Example	-

Table 9-569 occnp_um_audit_query_error_response_total

Field	Details
Description	This metric is incremented when Usage Monitoring receives 3xx, 4xx (except 404) and 5xx response code from PCRF Core for a session GET request.
Type	Counter
Dimensions	• siteId • response_code • hostname
Example	-

Table 9-570 occnp_um_audit_query_exception_total

Field	Details
Description	This metric is incremented when Usage Monitoring service ends up with an exception while sending GET request to PCRF Core service.
Type	Counter
Dimensions	• siteId • hostname
Example	-

Table 9-571 occnp_usage_mon_plan_exhausted_total

Field	Details
Description	This metric is incremented when the allowed usage is exhausted.
Type	Counter
Dimensions	• limitId • type • hostname
Example	occnp_usage_mon_plan_exhausted_total {hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1",type="base",}14.0

Table 9-572 occnp_usage_mon_limit_selected_total

Field	Details
Description	This metric is incremented when a UM Data Limit Profile is selected.
Type	Counter
Dimensions	• limitId • type • hostname

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-572 (Cont.) occnp_usage_mon_limit_selected_total

Field	Details
Example	occnp_usage_mon_limit_selected_total {hostname="ocpcf-usage-mon-b564d6cf8-shzhg",limit_id="mk1",type="base",} 7.0 occnp_usage_mon_limit_selected_total {hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-9f51e",type="roll-over-def",}1.0 occnp_usage_mon_limit_selected_total{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-640e7",type="roll-over-def",}1.0 occnp_usage_mon_limit_selected_total{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-8b066",type="roll-over-def",}1.0 occnp_usage_mon_limit_selected_total{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-9161c",type="roll-over-def",}1.0

Note

When the Data Limit Profile is received from UDR, occnp_usage_mon_limit_selected metric is pegged and when Data Limit Profile is received through CNC Console, occnp_usage_mon_profile_selected metric is pegged.

Table 9-573 usage_mon_rollover_def_create

Field	Details
Description	This metric is increment when current rollover def created using current rollover usage.
Type	Counter
Dimensions	• limitId • rollOverCount • hostname
Example	usage_mon_rollover_def_create{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-56937",rollover_count="1",}1.0 usage_mon_rollover_def_create{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-33423",rollover_count="1",}1.0 usage_mon_rollover_def_create{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk2-roll-over-def-71740",rollover_count="1",}1.0

Table 9-574 occnp_usage_mon_rollover_capped_total

Field	Details
Description	This metric is incremented when rollover reaches maximum data limit cap.
Type	String
Dimensions	• limit_id • hostname

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-574 (Cont.) occnp_usage_mon_rollover_capped_total

Field	Details
Example	occnp_usage_mon_rollover_capped_total{hostname="my-cnpolicy-usage-mon-6ff7947d8f-rcrxs",limit_id="mk1-roll-over-def-fa74b",} 1.0 occnp_usage_mon_rollover_capped_total {hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-18e63",}1.0 occnp_usage_mon_rollover_capped_total{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-ef270",}1.0 occnp_usage_mon_rollover_capped_total{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-63e0c",}1.0 occnp_usage_mon_rollover_capped_total{hostname="ocpcf-usage-mon-b564d6cf8-d5d79",limit_id="mk1-roll-over-def-10685",}1.0

Table 9-575 ocpm_udr_tracking_exception_total

Field	Details
Description	ocpm_udr_tracking_exception_total metric is incremented for a successful operation_type="subscribe" response if the apiroot in the Location header is invalid.
Type	Counter
Dimensions	• HostName • application • hostname • nf_instance_id • nf_name • operration_type • service_resource • service_subresource • service_version • servicename_3gpp
Example	ocpm_udr_tracking_exception_total{HostName="",application="pcf_userservice",hostname="policy-occnp-udr-connector-68f57cc698-rx28l",nf_instance_id="fe7d992b-0541-4c7d-ab84-111112222211",nf_name="nf2stub.altair-ns10.svc",operration_type="get",service_resource="policy-data",service_subresource="sm-data",service_version="v1",servicename_3gpp="nudr-dr"}

9.25 Bulwark Metrics

The following table describes the Bulwark service metrics and their respective dimensions:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 Dimension Glossary

Dimension	Possible values from your Queries	Explanation
namespace	$namespace, or real values like dev, qa, prod	Kubernetes namespace where Bulwark service running

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
exported_application	bulwark	Log_category_application_name attached to exported metrics

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanations
requestType	acquireLock, releaseLock	Type of lock operation being processed

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
pod	values like bulwark-6d7b8c9f4f-xyz12	kubernetes_pod_name, used for pod_breakdown

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
		down

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
container	bulwark	Container name, indicates the pod that exposes the metric

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
uri	/v1/locks, /v1/locks/{lockID}	HTTP endpoint path being called

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
status	200, 201, 204, 400, 404, 409, 500	HTTP response status code returned by the API. Exact value

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
		used dependent on the metric name

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
le	0.005, 0.01, 0.025, 0.05, 0.075, 0.1, 0.25, 0.5, 0.75, 1, 2.5, 5, 10, inf	Histogram bucket upper bound. For example, 0.005

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
		y means <= 5ms, and n if means service_thing above the last b

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
		ucket

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
name	Task Dispatcher Engine Fixed Thread Pool	Executor.threadpool_name for executor_threadpool_gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
totalLockAttempts	1, 2, 3, 4, ...	Number of attempts needed to get the lock request processed

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-576 (Cont.) Dimension Glossary

Dimension	Possible values from your Queries	Explanation
		cedaf_na_response_

Table 9-577 lock_request_total

Field	Details
Description	Total number of lock requests received at Bulwark per service or pod.
Type	Counter
Dimensions	• application • podName • requestType (releaseLock, acquireLock) • serviceName
Examples	• lock_request_total{application="bulwark",podName="abc-cnv-rls-bulwark-856556f674-twkfn",requestType="releaseLock",serviceName="serviceId", } 2.0 • lock_request_total{application="bulwark",podName="abc-cnv-rls-bulwark-856556f674-twkfn",requestType="acquireLock",serviceName="serviceId", } 2.0

Table 9-578 http_server_requests_seconds_count

Field	Details
Description	Total number of HTTP requests served by Bulwark. Useful for request rate and response-code distribution for lock or unlock APIs.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-578 (Cont.) http_server_requests_seconds_count

Field	Details
Dimensions	• namespace • container • uri • status • pod
Examples	• http_server_requests_seconds_count{namespace="$namespace", container="bulwark", uri="/v1/locks"}[2m] • http_server_requests_seconds_count{namespace="$namespace", container="bulwark",uri="/v1/locks/{lockID}"}[2m]

Table 9-579 lockAcquisitionResponseWaitingLatency_seconds_bucket

Field	Details
Description	Distribution of lock-acquisition response latency, showing how long to wait for lock responses across latency buckets.
Type	Histogram bucket
Dimensions	• namespace • container • le
Examples	• lockAcquisitionResponseWaitingLatency_seconds_bucket{le="0.005",namespace="$namespace", container="bulwark"}[2m] • lockAcquisitionResponseWaitingLatency_seconds_bucket{le="0.01",namespace="$namespace", container="bulwark"}[2m] • lockAcquisitionResponseWaitingLatency_seconds_bucket{le="0.025",namespace="$namespace", container="bulwark"}[2m] • lockAcquisitionResponseWaitingLatency_seconds_bucket{le="0.05",namespace="$namespace", container="bulwark"}[2m] • lockAcquisitionResponseWaitingLatency_seconds_bucket{le="0.075",namespace="$namespace", container="bulwark"}[2m]

Table 9-580 unlockResponseWaitingLatency_bucket

Field	Details
Description	Distribution of unlock-response latency, showing how long unlock requests take across latency buckets.
Type	Histogram bucket
Dimensions	• namespace • container • le

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-580 (Cont.) unlockResponseWaitingLatency_bucket

Field	Details
Examples	• unlockResponseWaitingLatency_bucket{le="0.005",namespace="$namespace", container="bulwark"}[2m] • unlockResponseWaitingLatency_bucket{le="0.01",namespace="$namespace", container="bulwark"}[2m] • unlockResponseWaitingLatency_bucket{le="0.025",namespace="$namespace", container="bulwark"}[2m] • unlockResponseWaitingLatency_bucket{le="0.05",namespace="$namespace", container="bulwark"}[2m] • unlockResponseWaitingLatency_bucket{le="0.075",namespace="$namespace", container="bulwark"}[2m]

Table 9-581 coherenceLockProcessingMs_bucket

Field	Details
Description	Distribution of time spent in coherence/backend processing during lock requests.
Type	Histogram bucket
Dimensions	• namespace • container • le
Examples	• coherenceLockProcessingMs_bucket{le="0.005",namespace="$namespace", container="bulwark"}[2m] • coherenceLockProcessingMs_bucket{le="0.01",namespace="$namespace", container="bulwark"}[2m] • coherenceLockProcessingMs_bucket{le="0.025",namespace="$namespace", container="bulwark"}[2m] • coherenceLockProcessingMs_bucket{le="0.05",namespace="$namespace", container="bulwark"}[2m] • coherenceLockProcessingMs_bucket{le="0.075",namespace="$namespace", container="bulwark"}[2m]

Table 9-582 coherenceUnlockProcessingMs_bucket

Field	Details
Description	Distribution of time spent in coherence/backend processing during unlock requests.
Type	Histogram bucket
Dimensions	• namespace • container • le

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-582 (Cont.) coherenceUnlockProcessingMs_bucket

Field	Details
Examples	• coherenceUnlockProcessingMs_bucket{le="0.005",namespace="$namespace", container="bulwark"}[2m] • coherenceUnlockProcessingMs_bucket{le="0.01",namespace="$namespace", container="bulwark"}[2m] • coherenceUnlockProcessingMs_bucket{le="0.025",namespace="$namespace", container="bulwark"}[2m] • coherenceUnlockProcessingMs_bucket{le="0.05",namespace="$namespace", container="bulwark"}[2m] • coherenceUnlockProcessingMs_bucket{le="0.075",namespace="$namespace", container="bulwark"}[2m]

Table 9-583 internal_pending_lock_req_ctx_storage_map_size

Field	Details
Description	Current number of pending lock request contexts stored internally by Bulwark.
Type	Gauge
Dimensions	• namespace • container • pod
Examples	• internal_pending_lock_req_ctx_storage_map_size{namespace="$namespace", container="bulwark"}

Table 9-584 executor_queued_tasks

Field	Details
Description	Current number of tasks waiting in the executor queue for the Bulwark thread pool.
Type	Gauge
Dimensions	• namespace • container • name • pod
Examples	• executor_queued_tasks{namespace="$namespace", container="bulwark", name="Task Dispatcher Engine Fixed Thread Pool"}

Table 9-585 executor_active_threads

Field	Details
Description	Current number of active executor threads processing work.
Type	Gauge
Dimensions	• namespace • container • name • pod
Examples	• executor_active_threads{namespace="$namespace", container="bulwark", name="Task Dispatcher Engine Fixed Thread Pool"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-586 coherenceLockInvokeTimeout_total

Field	Details
Description	Total number of coherence invocation timeouts seen during lock processing.
Type	Counter
Dimensions	• namespace
Examples	• coherenceLockInvokeTimeout_total{namespace="$namespace"}[2m]

Table 9-587 lock_response_total

Field	Details
Description	Total number of lock responses sent by Bulwark per service or pod.
Type	Counter
Dimensions	• RequestType (acquire) • ResponseType (success, failure) • ResponseStatus • consumerServiceName • totalLockAttempts • retryOnAlreadyLocked (true, false)
Examples	• lock_response_total{application="bulwark",podName="abc-cnv-rls-bulwark-856556f674-twkfn",requestType="acquireLock",responseStatus="201" ,responseType="success" ,serviceName="SM-Service", } 2.0 • lock_response_total{application="bulwark",podName="abc-cnv-rls-bulwark-856556f674-twkfn",requestType="acquireLock",responseStatus="423" ,responseType="failure" ,serviceName="SM-Service", } 2.0 • lock_response_total{application="bulwark",podName="abc-cnv-rls-bulwark-856556f674-twkfn",requestType="releaseLock",responseStatus="204" ,responseType="success" ,serviceName="serviceId", } 2.0

Table 9-588 lock_collision_total

Field	Details
Description	Tracks the total count of all the collisions occurred for single/multi lock request failure.
Type	Counter
Dimensions	• bulwarkPodName • consumerServiceName • lockRequestKeysTotal
Examples	lock_collision_total{application="bulwark",noOfKeysPerRequest="1",podName="pcf-bulwark-776df8bb5c-6g2f6",serviceName="policyds",} 80.0 lock_collision_total{application="bulwark",noOfKeysPerRequest="2",podName="pcf-bulwark-776df8bb5c-6g2f6",serviceName="occnp_pcf_sm",} 8.0 lock_collision_total{application="bulwark",noOfKeysPerRequest="1",podName="pcf-bulwark-776df8bb5c-6g2f6",serviceName="occnp_pcf_sm",} 92.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-589 coherence_callback_operation_total

Field	Details
Description	Tracks the total count all the register/deregister requests towards coherence.
Type	Counter
Dimensions	• bulwarkPodName • opType (Registration, Deregistration) • Status (SUCCESS, FAILED)
Examples	coherence_callback_operation_total{application="bulwark",opStatus="success",opType="Deregistration",podName="test-bulwark-5f44788c69-qjdhd",} 0 coherence_callback_operation_total{application="bulwark",opStatus="success",opType="Registration",podName="test-bulwark-5f44788c69-qjdhd",} 0

Table 9-590 coherence_callback_response_total

Field	Details
Description	Tracks the total coherence callback responses from coherence to bulwark
Type	Counter
Dimensions	bulwarkPodName
Examples	coherence_callback_response_total{application="bulwark",podName="test-bulwark-8f8b9bc67-dpf85",} 0

For more information about Dimensions, see CNC Policy Metrics.

9.26 CHF Metrics

The following table describes the CHF service metrics and their respective dimensions:

Table 9-591 ocpm_chf_tracking_request_total

Field	Details
Description	Total number of CHF tracking requests.
Type	Counter
Dimensions	• HostName • application • nf_instance_id • nf_name • operation_type • service_resource • service_version • servicename_3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-591 (Cont.) ocpm_chf_tracking_request_total

Field	Details
Examples	• ocpm_chf_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="unsubscribe",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter • ocpm_chf_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="put",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter • ocpm_chf_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="subscribe",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 1.0 ; Type-Counter

Table 9-592 ocpm_chf_tracking_response_total

Field	Details
Description	Total number of CHF tracking response.
Type	Counter
Dimensions	• HostName • application • nf_instance_id • nf_name • operation_type • service_resource • service_version • servicename_3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-592 (Cont.) ocpm_chf_tracking_response_total

Field	Details
Examples	• ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="subscribe",response_code="5xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter • ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="put",response_code="4xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter • ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="put",response_code="1xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter • ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="unsubscribe",response_code="4xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter • ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",nf_name="chf.xxxx.com",operation_type="unsubscribe",response_code="2xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter

9.27 UDR Metrics

The following table describes the UDR service metrics and their respective dimensions:

Table 9-593 ocpm_udr_tracking_request_total

Field	Details
Description	Total number of UDR tracking request.
Type	Counter
Dimensions	• HostName • application • nf_instance_id • operation_type • service_resource • service_subresource • service_version • servicename_3gpp

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-593 (Cont.) ocpm_udr_tracking_request_total

Field	Details
Examples	• ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",hostname="pcf_userservice",nf_instance_id="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="fqdn",operation_type="get",service_resource="policy-data",service_subresource="operator-specific-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",hostname="hummingbirds-pcf190rc4-occnp-udr-connector-7d648f5765-zrwc9",nf_name="udr.xxxx.com",nf_instance_id="fe7d992b-0541-4c7d-ab84-6d70b1babc1",operation_type="put",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",operation_type="subscribe",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 ; Type-Counter • ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",operation_type="unsubscribe",service_resource="policy-data",service_subresource="sm-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",operation_type="unsubscribe",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",operation_type="get",service_resource="policy-data",service_subresource="ue-policy-set",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",binding_id="",binding_level="",discovery_id="",discovery_parameter="",hostname="titans-occnp-udr-connector-694f9795d8-gmdl4",nf_instance_id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf1stub.rigelns6.svc",operation_type="lookup_subscribe",service_resource="subscription-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 • ocpm_udr_tracking_request_total{HostName="",application="pcf_userservice",binding_id="",binding_level="",discovery_id="",discovery_parameter="",hostname="policy16-occnp-udr-connector-6d69dd58bc-qdprw",nf_instance_id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf1stub.hi-ns16.svc",operation_type="patch",service_resource="policy-data",service_subresource="operator-specific-data",service_version="v1",servicename_3gpp="nudr-dr"}

Table 9-594 ocpm_udr_tracking_response_total

Field	Details
Description	This metric captures all the responses recieved by UDR Connector on it is communication with UDR.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-594 (Cont.) ocpm_udr_tracking_response_total

Field	Details
Type	Counter
Dimensions	• HostName • Application • NfInstanceId • QueryType • DataSourceType • RequestMapping

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-594 (Cont.) ocpm_udr_tracking_response_total

Field	Details
Examples	• ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com", operation_type="subscribe",response_code="2xx",service_resource="policy-data",service_subresource="",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="unsubscribe",response_code="5xx",service_resource="policy-data",service_subresource="am-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="unsubscribe",response_code="1xx",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="put",response_code="1xx",service_resource="policy-data",service_subresource="sm-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="subscribe",response_code="3xx",service_resource="policy-data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="get",response_code="2xx",service_resource="policy-data",service_subresource="",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",nf_name="udr.xxxx.com",operation_type="patch",response_code="2xx",service_resource="policy-data",service_subresource="am-data",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",hostname="pcf_userservice",nf_instance_id="3db4b97c-04dc-4aff-ab20-2e156dbd02d2",nf_name="fqdn",operation_type="get",response_code="2xx",service_resource="policy-data",service_subresource="operator-specific-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",hostname="my-cnpolicy-occnp-udr-connector-7ddfc965b9-s8nwq",nf_instance_id="fe7d992b-0541-4c7d-ab84-333334444433",nf_name="nf2stub.h3-ns10.svc",operation_type="put",response_code="3xx",service_resource="policy-data",service_subresource="sm-data",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",hostname="titans-occnp-udr-connector-694f9795d8-gmdl4",nf_instance_id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf1stub.rigelns6.svc",operation_type="lookup_subscribe",response_code="2xx",service_resource="subscription-

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-594 (Cont.) ocpm_udr_tracking_response_total

Field	Details
	data",service_subresource="subs-to-notify",service_version="v1",servicename_3gpp="nudr-dr",} 1.0 • ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",hostname="policy16-occnp-udr-connector-6d69dd58bc-f4fd5",nf_instance_id="fe7d992b-0541-4c7d-ab84-555552222222",nf_name="nf1stub.hi-ns16.svc",operation_type="patch",response_code="4xx",service_resource="policy-data",service_subresource="operator-specific-data",service_version="v1",servicename_3gpp="nudr-dr"}

Table 9-595 ocpm_nfDiscovery_request_total

Field	Details
Description	PCF measures the total number of successful/failed discovery query of UDR using "group-id-list".
Type	Counter
Dimensions	queryParameters="service-names,group-id-list,target-nf-type
Example	ocpm_nfDiscovery_request_total{app_kubernetes_io_instance="test", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="1.0.0", application="occnp", container="user-service", endpoint="cnc-metrics", engVersion="23.4.0-ocngf-incredibles", exported_application="pcf_userservice", helm_sh_chart="user-service-23.4.0-ocngf-incredibles", hostname="test-occnp-udr-connector-868c766947-fr7zx", instance="10.233.93.4:9000", io_kompose_service="test-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="1.0.0", namespace="s-euler", pod="test-occnp-udr-connector-868c766947-fr7zx", pod_template_hash="868c766947", queryParameters="service-names,group-id-list,target-nf-type,requester-nf-type", targetNfType="UDR", vendor="Oracle"}

Table 9-596 ocpm_nfDiscovery_response_total

Field	Details
Description	PCF measures the total number of successful/failed discovery query of UDR using "group-id-list".
Type	Counter
Dimensions	• queryParameters • responseCode • target_nf_type • cause

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-596 (Cont.) ocpm_nfDiscovery_response_total

Field	Details
Example	ocpm_nfDiscovery_response_total{app_kubernetes_io_instance="test", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="1.0.0", application="occnp", container="user-service", endpoint="cnc-metrics", engVersion="23.4.0-ocngf-incredibles", exported_application="pcf_userservice", helm_sh_chart="user-service-23.4.0-ocngf-incredibles", hostname="test-occnp-udr-connector-868c766947-fr7zx", instance="10.233.93.4:9000", io_kompose_service="test-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="1.0.0", namespace="s-euler", pod="test-occnp-udr-connector-868c766947-fr7zx", pod_template_hash="868c766947", queryParameters="service-names,group-id-list,target-nf-type,requester-nf-type", responseCode="424", targetNfType="UDR", vendor="Oracle"}

Table 9-597 occnp_group_id_list_discovery_header_sent_total

Field	Details
Description	PCF measures the number of GET or POST request sent to UDR with 3gpp-Sbi-Discovery-group-Id-list for delegated discovery of UDR toward SCP.
Type	Counter
Dimensions	• operation_type • target_nf_type
Example	occnp_group_id_list_discovery_header_sent_total{app_kubernetes_io_instance="test", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="1.0.0", application="occnp", container="user-service", endpoint="cnc-metrics", engVersion="23.4.0-ocngf-incredibles", exported_application="pcf_userservice", helm_sh_chart="user-service-23.4.0-ocngf-incredibles", hostname="test-occnp-udr-connector-79df49b796-gc77c", instance="10.233.72.203:9000", io_kompose_service="test-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="1.0.0", namespace="s-euler", operation_type="get", pod="test-occnp-udr-connector-79df49b796-gc77c", pod_template_hash="79df49b796", vendor="Oracle"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

9.28 User-Agent Header Metrics

Table 9-598 oc.ingressgateway.http.requests

Field	Details
Description	This metric is pegged for every incoming request on Ingress Gateway. This will be independent of User Agent validation feature at ingress gateway. If the User-Agent header is not present, then UNKNOWN will be pegged only for the following dimensions: • consumerNfType- consumerNfType obtained from the User-Agent header in incoming request • consumerInstanceId- consumer Instance Id obtained from the User-Agent header in incoming request • ConsumerFqdn- consumer Fqdn obtained from the User-Agent header in the incoming request If User-Agent header is present then respective dimensions are pegged as per user-agent header. **Note**: Only dimensions are part of the User-Agent.
Type	Counter
Dimensions	• consumerNfType • consumerInstanceId • ConsumerFqdn
Examples	Example when User-agent is not present: {ClientCertIdentity="N/A",ConsumerFqdn="UNKNOWN",DestinationHost="UNKNOWN",Host="ocpcf-occnp-ingress-gateway.ss-gate-beta-b-16965005-gate-pcf.svc.cosmos.lab.us.oracle.com",HttpVersion="HTTP/2.0",InstanceIdentifier="UNKNOWN_ingressgateway",Method="POST",NFServiceType="nnrf-client",NFType="NRF",Route_path="/nnrf-client/**",Scheme="HTTP",consumerInstanceId="UNKNOWN",consumerNfType="UNKNOWN",oAuthTokenPresent="false",}38.0 Example when User-agent not present: occnp_oc_ingressgateway_http_requests_total{ClientCertIdentity="N/A",ConsumerFqdn="nsmf-consp-001.bltnmn86.mw.smf.5gc.vzims.com",DestinationHost="UNKNOWN",Host="ocpcf-occnp-ingress-gateway.ss-gate-beta-b-16965005-gate-pcf.svc",HttpVersion="HTTP/2.0",InstanceIdentifier="UNKNOWN_ingressgateway",Method="POST",NFServiceType="npcf-smpolicycontrol",NFType="PCF",Route_path="/npcf-smpolicycontrol/*/sm-policies/{policy-id}/update",Scheme="HTTP",consumerInstanceId="52304af4-1111-45f1-9025-555552222222", consumerNfType="SMF",oAuthTokenPresent="false",} 61.0

9.29 NWDAF Agent Metrics

The following table describes the NWDAF Agent metrics and their respective dimensions:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-599 subscription_failure

Field	Details
Description	Gauge of failures for configured slice load levels doing autonomous subscription during configuration changes.
Type	Gauge
Dimensions	• serviceResource • snssai • operationType • responseCode • requestType
Example	subscription_failure{operationType="POST",requestType="autonomous",responseCode="500",serviceResource="SLICE_LOAD_LEVEL",snssai="14-aaaa14",} 1.0

Table 9-600 http_backend_request_total

Field	Details
Description	Counter for backend requests
Type	Counter
Dimensions	• serviceNameNon3gpp • serviceResource • operationType
Example	http_backend_request_total{operationType="POST",serviceNameNon3gpp="autonomous",serviceResource="SLICE_LOAD_LEVEL",} 26.0

Table 9-601 http_backend_response_total

Field	Details
Description	Counter for responses to backend requests
Type	Counter
Dimensions	• serviceNameNon3gpp • serviceResource • serviceVersion • responseCode
Example	http_backend_response_total{operationType="POST",responseCode="201",serviceNameNon3gpp="autonomous",serviceResource="SLICE_LOAD_LEVEL",} 25.0

Table 9-602 http_in_conn_request_total

Field	Details
Description	Counter for NWDAF notification requests
Type	Counter
Dimensions	• serviceName3gpp • serviceResource • serviceVersion • operationType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-602 (Cont.) http_in_conn_request_total

Field	Details
Example	http_in_conn_request_total{operationType="POST",serviceName3gpp="NWDAF",serviceResource="NF_LOAD",serviceVersion="v1",} 1.0

Table 9-603 http_in_conn_response_total

Field	Details
Description	Counter for responses to NWDAF notification requests
Type	Counter
Dimensions	• serviceName3gpp • serviceResource • serviceVersion • operationType • responseCode
Example	http_in_conn_response_total{operationType="POST",responseCode="204",serviceName3gpp="NWDAF",serviceResource="NF_LOAD",serviceVersion="v1",} 1.0

Table 9-604 http_out_conn_request_total

Field	Details
Description	Counter for requests sent from nwdaf-agent to NWDAF
Type	Counter
Dimensions	• serviceName3gpp • serviceResource • serviceVersion • host • instanceId • isAlternateRoute • isRetryAttempt • operationType
Example	http_out_conn_request_total{host="floki-occnp-egress-gateway/nnwdaf-eventssubscription/v1",instanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0621",isAlternateRoute="",isRetryAttempt="",operationType="POST",serviceName3gpp="NWDAF",serviceResource="SLICE_LOAD_LEVEL",serviceVersion="v1",} 26.0

Table 9-605 http_out_conn_response_total

Field	Details
Description	Counter for responses from NWDAF
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-605 (Cont.) http_out_conn_response_total

Field	Details
Dimensions	• serviceName3gpp • serviceResource • serviceVersion • host • instanceId • isAlternateRoute • isRetryAttempt • operationType • responseCode
Example	http_out_conn_response_total{host="floki-occnp-egress-gateway/nnwdaf-eventssubscription/v1",instanceId="fe7d992b-0541-4c7d-ab84-c6d70b1b0621",isAlternateRoute="",isRetryAttempt="",operationType="POST",responseCode="500",serviceName3gpp="NWDAF",serviceResource="SLICE_LOAD_LEVEL",serviceVersion="v1",} 1.0

Table 9-606 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimensions	• Service Name • Pod Name

Table 9-607 data_repository_invocations_seconds_max

Field	Details
Description	This metric is used to track the maximum execution time of Data repository invocations. It is a useful metric for monitoring the performance of Data repositories and identifying slow-running queries.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-607 (Cont.) data_repository_invocations_seconds_max

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_max{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-608 data_repository_invocations_seconds_sum

Field	Details
Description	The seconds_sum metric for Data repository invocations is a measure of the total time spent executing repository methods.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-608 (Cont.) data_repository_invocations_seconds_sum

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_sum{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.84.88:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="getQueuedTablesToAudit", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nshv9", pod_template_hash="6b6f85f7b9", repository="AuditSchedulerRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

Table 9-609 data_repository_invocations_seconds_count

Field	Details
Description	This metric measures the total time spent in Data JPA repository invocations. It is a counter metric, which means that it increments each time a repository method is invoked. The metric is reported in seconds.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-609 (Cont.) data_repository_invocations_seconds_count

Field	Details
Dimension	• app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • exception • helm_sh_chart • instance • io_kompose_service • job • method • microservice • mktgVersion • namespace • pod • service • pod_template_hash • repository • security_istio_io_tlsMode • service_istio_io_canonical_name • service_istio_io_canonical_revision • state • vendor
Example	data_repository_invocations_seconds_count{app_kubernetes_io_instance="ocbsf", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="audit-service", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.0.0.0", application="ocbsf", container="audit-service", endpoint="cnc-metrics", engVersion="24.1.4", exception="None", helm_sh_chart="audit-service-24.1.4", instance="10.233.127.211:9000", io_kompose_service="ocbsf-ocpm-audit-service", job="occne-infra/occne-nf-cnc-podmonitor", method="findAll", microservice="ocbsf-audit", mktgVersion="1.0.0.0", namespace="ocbsf", pod="ocbsf-ocpm-audit-service-6b6f85f7b9-nmzr4", pod_template_hash="6b6f85f7b9", repository="AuditRegistrationsRepository", security_istio_io_tlsMode="istio", service_istio_io_canonical_name="audit-service", service_istio_io_canonical_revision="1.0.0.0", state="SUCCESS", vendor="Oracle"}

9.30 PRE Metrics

The following table describes the PRE Service metrics and respective dimensions:

Table 9-610 http_in_conn_request_total

Field	Details
Description	The requests received by a Microservice from the downstream application.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-610 (Cont.) http_in_conn_request_total

Field	Details
Dimensions	• operationType • servicenameNon3gpp • workerId
Example	http_in_conn_request_total{operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}1

Table 9-611 http_in_conn_response_total

Field	Details
Description	The response sent for incoming requests to a micro-service.
Type	Counter
Dimensions	• operationType • servicenameNon3gpp • responseCode • workerId
Example	http_in_conn_response_total{operationType="post",servicenameNon3gpp="pcf-sm",responseCode="200",workerId="1"}1

Table 9-612 http_in_conn_processing_latency_ms

Field	Details
Description	The overall response time for request, received from the downstream application.
Type	Histogram
Dimensions	• le • operationType • servicenameNon3gpp • workerId

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-612 (Cont.) http_in_conn_processing_latency_ms

Field	Details
Examples	• http_in_conn_processing_latency_ms_bucket{le="2",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}0 • http_in_conn_processing_latency_ms_bucket{le="5",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}1 • http_in_conn_processing_latency_ms_bucket{le="10",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}1 • http_in_conn_processing_latency_ms_bucket{le="20",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}3 • http_in_conn_processing_latency_ms_bucket{le="50",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5 • http_in_conn_processing_latency_ms_bucket{le="100",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5 • http_in_conn_processing_latency_ms_bucket{le="200",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5 • http_in_conn_processing_latency_ms_bucket{le="500",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5 • http_in_conn_processing_latency_ms_bucket{le="1000",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5 • http_in_conn_processing_latency_ms_bucket{le="2000",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5 • http_in_conn_processing_latency_ms_bucket{le="+Inf",operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5 • http_in_conn_processing_latency_ms_sum{operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}82 • http_in_conn_processing_latency_ms_count{operationType="post",servicenameNon3gpp="pcf-sm",workerId="1"}5

Table 9-613 http_out_conn_request_total

Field	Details
Description	The requests sent by a micro-service to upstream.
Type	Counter
Dimensions	• operationType • host • httpVersion • isRetryAttempt • servicenameNon3gpp • workerId
Example	http_out_conn_request_total{operationType="POST",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}1

Table 9-614 http_out_conn_response_total

Field	Details
Description	The response received for upstream requests to a micro-service.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-614 (Cont.) http_out_conn_response_total

Field	Details
Dimensions	• operationType • responseCode • host • httpVersion • isRetryAttempt • servicenameNon3gpp • workerId
Example	http_out_conn_response_total{operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}1

Table 9-615 http_out_conn_processing_latency_ms

Field	Details
Description	The overall response time for request towards upstream.
Type	Histogram
Dimensions	• le • operationType • responseCode • host • httpVersion • isRetryAttempt • servicenameNon3gpp • workerId

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-615 (Cont.) http_out_conn_processing_latency_ms

Field	Details
Examples	• http_out_conn_processing_latency_ms_bucket{le="2",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}0 • http_out_conn_processing_latency_ms_bucket{le="5",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}2 • http_out_conn_processing_latency_ms_bucket{le="10",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}3 • http_out_conn_processing_latency_ms_bucket{le="20",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5 • http_out_conn_processing_latency_ms_bucket{le="50",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5 • http_out_conn_processing_latency_ms_bucket{le="100",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5 • http_out_conn_processing_latency_ms_bucket{le="200",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5 • http_out_conn_processing_latency_ms_bucket{le="500",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5 • http_out_conn_processing_latency_ms_bucket{le="1000",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5 • http_out_conn_processing_latency_ms_bucket{le="2000",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5 • http_out_conn_processing_latency_ms_bucket{le="+Inf",operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"} 5 • http_out_conn_processing_latency_ms_sum{operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}41 • http_out_conn_processing_latency_ms_count{operationType="POST",responseCode="502",host="localhost:8080",httpVersion="1",isRetryAttempt="false",servicenameNon3gpp="PER",workerId="1"}5

Table 9-616 occnp_policy_processing_latency_ms

Field	Details
Description	Overall response time for request received from downstream when executing Policy. **Note**: This metric is associated only with 'Call Policy' block. For more information, see "Public Category" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.
Type	Histogram

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-616 (Cont.) occnp_policy_processing_latency_ms

Field	Details
Dimensions	• le • operationType • policyName • servicenameNon3gpp • workerId
Examples	• occnp_policy_processing_latency_ms_bucket{le="2", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}0 • occnp_policy_processing_latency_ms_bucket{le="5", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="10", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="20", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="50", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="100", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="200", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="500", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="1000", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="2000", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_bucket{le="+Inf", operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_sum{operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 • occnp_policy_processing_latency_ms_count{ operationType="post", policyName="AM_Policy_Audit", servicenameNon3gpp="pcf-am", workerId="2"}1 **Note**: This metric is associated with 'Call Policy' block. For more information, see "Public Category" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-617 occnp_block_counter_label

Field	Details
Description	Tracks total number of given custom block is invoked for corresponding label. **Note**: This metric is associated with 'Increment Counter Label' block. For more information, see "Public Category" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.
Type	Counter
Dimensions	• serviceType • operationType • workerId • label • subLabel
Example	occnp_block_counter_label{serviceType="pcf-sm",operationType="post",workerId="2",label="lml",subLabel=""}1

Table 9-618 occnp_block_exec_time_ns

Field	Details
Description	Tracks overall time taken by all the blocks captured as part of this block. Since this metric is in nanoseconds, execution time below 0 are not recorded. It will be visible with traffic around 10k TPS. **Note**: This metric is associated with 'Time' block. For more information, see "Public Category" section in Oracle Communications Cloud Native Core, Converged Policy Design Guide.
Type	Histogram
Dimensions	• serviceType • operationType • workerId • label • subLabel

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-618 (Cont.) occnp_block_exec_time_ns

Field	Details
Example	• occnp_block_exec_time_ns_bucket{le="2",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="5",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="10",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="20",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="50",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="100",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="200",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="500",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="1000",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="2000",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_bucket{le="+Inf",serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_sum{serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1 • occnp_block_exec_time_ns_count{serviceType="pcf-sm",operationType="post",workerId="2",label="lnl",subLabel=""}1

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-619 occnp_policy_project_state_change_total

Field	Details
Description	Tracks the total number of policy project state changes for each service whenever a project transitions between *dev* and *prod* states (or vice versa). It is designed to provide a way to identify and increment policy project state counters across various policy execution legs. The metric is pegged at the worker level, providing an aggregated count across all active workers. For example, if there are 4 workers running in production, each state transition between dev and prod (or vice versa) will increment the counter by 4. A successful state transition is indicated when the metric increases by the full number of active workers (e.g., an increment of 4 for 4 workers). Any value less than the total number of workers suggests a failure, indicating that one or more workers may not have successfully applied the updated configuration. **Metric Calculation:** The total possible combinations of records for this metric are calculated using the formula: Total Combinations = (Number of Services) × (Maximum Number of Projects per Service) × (Number of States) Where: • Number of Services = 6 (AM, SM, UE, PDS, pcrf-core, Usage-mon) • Maximum Number of Projects per Service = 20 (configurable via Helm, typically set to 20) • Number of States = 2 (dev, prod)
Type	Counter
Dimensions	• serviceType • projectName • state
Examples	occnp_policy_project_state_change_total{serviceType="pcf-ue",projectName="PCFUE",state="dev"} 2 occnp_policy_project_state_change_total{serviceType="pcf-sm",projectName="PcfSMClone",state="dev"} 2 occnp_policy_project_state_change_total{serviceType="pcf-sm",projectName="PCFSM",state="dev"} 4 occnp_policy_project_state_change_total{serviceType="pcf-sm",projectName="PCFSM",state="prod"} 2 occnp_policy_project_state_change_total{serviceType="pcf-ue",projectName="PCFUE",state="prod"} 2 occnp_policy_project_state_change_total{serviceType="pcf-sm",projectName="PcfSMClone",state="prod"} 2

Table 9-620 occnp_policy_project_current_state

Field	Details
Description	Provides a real-time, numerical representation of the current deployment state for each unique policy project within the system. It reflects whether a policy project is in a development (dev) or production (prod) state. The metric is pegged at the master level to provide current state of projects. **Possible Values and Interpretation:** • 0: The policy project is in a *dev* state. • 1: The policy project is in a *prod* state.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-620 (Cont.) occnp_policy_project_current_state

Field	Details
Type	Gauge
Dimensions	• serviceType • projectName
Example	• occnp_policy_project_current_state{serviceType="pcf-ue",projectName="PCFUE"} 1 • occnp_policy_project_current_state{serviceType="pcf-sm",projectName="PcfSMClone"} 1 • occnp_policy_project_current_state{serviceType="pcf-sm",projectName="PCFSM"} 0

For more information about Dimensions, see CNC Policy Metrics.

9.31 NRF Client Metrics

NF status and NF load metrics:

Table 9-621 nrfclient_perf_info_nf_profile_load

Field	Details
Description	The current Load of the NF.
Type	Gauge
Dimensions	-

Table 9-622 nrfclient_current_nf_status

Field	Details
Description	The current operative status of the NF. The gauge shall be indicate the status as below: • 0 - REGISTERED • 1 - DEREGISTERED • 2 - SUSPENDED • 3 - UNDISCOVERABLE • 4 - UNKNOWN
Type	Gauge
Dimensions	• NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-623 nrfclient_nf_status_with_nrf

Field	Details
Description	The operative status of the NF communicated to the NRF. The gauge shall be indicate the status as below: • 0 - REGISTERED • 1 - DEREGISTERED • 2 - SUSPENDED • 3 - UNDISCOVERABLE • 4 - UNKNOWN
Type	Gauge
Dimensions	• NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

NRF Health Status:

Table 9-624 nrfclient_nrf_operative_status

Field	Details
Description	The current operative status of the NRF Instance. If the metric has value • 0 - NRF is unavailable or unhealthy • 1 - NRF is available or healthy
Type	Gauge
Dimensions	NrfUri - URI of the NRF Instance

Table 9-625 nrfclient_nrf_status_total

Field	Details
Description	Total number of times an NRF instance is marked as healthy or unhealthy. The apiRoot is specified in the format *'scheme'://'fqdn':'port'*. **Note**: If health check procedure is disabled, all NRF instances are marked as HEALTHY after successful NF registration.
Type	Counter
Dimensions	NrfUri- URI of the NRF InstanceHealthStatus FailureReason - Reason for the status

Table 9-626 nrfclient_nrf_successive_healthy_count

Field	Details
Description	The metric shows the consecutive number of times the NRF is considered as healthy. The metric has a minimum value of 0 and maximum value of *healthCheckCount*.
Type	Counter
Dimensions	NrfUri- URI of the NRF Instance

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-627 nrfclient_nrf_successive_unhealthy_count

Field	Details
Description	The metric shows the consecutive number of times the NRF is considered as unhealthy
Type	Counter
Dimensions	NrfUri- URI of the NRF Instance

NF - NRF-Client metrics:

Table 9-628 nrfclient_on_demand_conn_in_request_total

Field	Details
Description	Total number of on-demand requests received from the backend NF to NRF Client.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Table 9-629 nrfclient_on_demand_conn_out_response_total

Field	Details
Description	Total number of on-demand responses sent to the backend NF to NRF Client.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile. • StatusCode - The HttpStatusCode as received from the NRF or generated by NRF-client.

Table 9-630 nrfclient_on_demand_processing_latency_seconds_bucket

Field	Details
Description	Total message processing time duration in seconds.
Type	Histogram
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Table 9-631 ocpm_nrf_tracing_request_timeout_total

Field	Details
Description	Total number of requests timeout sent to the backend NF from NRF Client.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-631 (Cont.) ocpm_nrf_tracing_request_timeout_total

Field	Details
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

NRF-Client DNS Lookup metrics:

Table 9-632 nrfclient_dns_lookup_request_total

Field	Details
Description	Total number of times a DNS lookup request is sent to the alternate route service. **Note**: The metric is pegged only if `enableVirtualNrfResolution` is set to true.
Type	Counter
Dimensions	• Scheme - HTTP or HTTPS • VirtualFqdn - Fqdn that shall be used by the alternate service for the DNS lookup

Table 9-633 nrfclient_dns_lookup_response_total

Field	Details
Description	Total number of times a DNS lookup response is received from the alternate route service. **Note**: The metric is pegged only if `enableVirtualNrfResolution` is set to true.
Type	Counter
Dimensions	• Scheme - HTTP or HTTPS • VirtualFqdn - Fqdn that shall be used by the alternate service for the DNS lookup • HttpStatusCode - The status code as received in the response.

Table 9-634 nrfclient_dns_register_request_total

Field	Details
Description	Total number of times a DNS register request is sent to the alternate route service. **Note**: The metric is pegged only if `enableVirtualNrfResolution` is set to true.
Type	Counter
Dimensions	• Scheme - HTTP or HTTPS • VirtualFqdn - Fqdn that shall be used by the alternate service for the DNS lookup

NRF-Client - NRF metrics:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-635 nrfclient_nw_conn_out_request_total

Field	Details
Description	Total number of times NRF-client has sent a request to NRF. This includes autonomous requests as well as on-demand requests.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile. • NrfURI - URI of the NRF Instance • OutgoingPriorityHeader - Header name for the outgoing request. • Priority - Priority value of the messageType object. • TargetNfType - Indicates request is for which target NF type.
Example	nrfclient_nw_conn_out_request_total {MessageType="AutonomousNfRegistration",NfFqdn="ocpcf-occnp-ingress-gateway.gate-beta-b-25671603-gate-pcf.svc.cluster.local",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0420",NfType="PCF",NrfURI="ocnrf-ingressgateway.gate-beta-b-25671603-gate-nrf.svc.cluster.local:80",OutgoingPriorityHeader="UNKNOWN",Priority="UNKNOWN",TargetNfType="UNKNOWN"} 2.0 nrfclient_nw_conn_out_request_total {MessageType="NfHeartBeat",NfFqdn="ocpcf-occnp-ingress-gateway.gate-beta-b-25671603-gate-pcf.svc.cluster.local",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0420",NfType="PCF",NrfURI="ocnrf-ingressgateway.gate-beta-b-25671603-gate-nrf.svc.cluster.local:80",OutgoingPriorityHeader="UNKNOWN",Priority="UNKNOWN",TargetNfType="UNKNOWN"} 11000.0

Table 9-636 nrfclient_nw_conn_in_response_total

Field	Details
Description	Total number of times NRF-client has received a response from NRF.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile. • StatusCode - The HttpStatusCode as received from the NRF or generated by NRF-client.
Example	occnp_nrfclient_nw_conn_in_response_total{ApplicationError="INVALID_API",MessageType="NfDiscovery",NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",StatusCode="400",} 2.0

Table 9-637 nrfclient_nw_conn_in_notify_request_total

Field	Details
Description	Total number of nfStatusNotify requests received from NRF.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-637 (Cont.) nrfclient_nw_conn_in_notify_request_total

Field	Details
Dimensions	• EventType - The EventType for which the notification is triggered. • NfInstanceID - The NfInstanceId for which the notification is triggered.

Table 9-638 nrfclient_nw_conn_out_notify_response_total

Field	Details
Description	Total number of *nfStatusNotify* responses sent to NRF.
Type	Counter
Dimensions	• EventType - The EventType for which the notification is triggered. • NfInstanceID - The NfInstanceId for which the notification is triggered. • HttpStatusCode - The HttpStatusCode sent by NRF-Client.
Example	occnp_nrfclient_nw_conn_out_notify_response_total # TYPE occnp_nrfclient_nw_conn_out_notify_response_total counter occnp_nrfclient_nw_conn_out_notify_response_total{EventType="NF_REGISTERED",HttpStatusCode="400",NfInstanceID="4947a69a-f61b-4bc1-b9da-47c9c5d14b64",} 1.0

Table 9-639 nrfclient_network_message_processing_latency

Field	Details
Description	Total message processing time duration.
Type	Histogram
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Table 9-640 occnp_nrfclient_discovery_cache_support_force_discovery_total

Field	Details
Description	Indicates the total number of requests received from backend services with header OC-Force-Rediscovery is enabled, and response is retrieved from NRF.
Type	Counter
Dimensions	• NfType • NfInstanceID • NfFqdn • QueryParams

Table 9-641 occnp_nrfclient_discovery_cache_support_cache_hit_total

Field	Details
Description	Indicates the total number of requests for which discovery response is returned from the cache.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-641 (Cont.) occnp_nrfclient_discovery_cache_support_cache_hit_total

Field	Details
Dimensions	• NfType • NfInstanceID • NfFqdn • QueryParams

Table 9-642 occnp_nrfclient_discovery_cache_support_about_to_expire_total

Field	Details
Description	Indicates the total number of cache records identified as about to be expired. This metric counts cases when a cached discovery response is eligible to be returned but also triggers a background request to get an updated response. **Note** This metrics is incremented when a valid cached discovery response is found and its remaining lifetime is within refreshBeforeExpiryTime, and not immediately when the threshold condition is reached.
Type	Counter
Dimensions	• NfType • NfInstanceID • NfFqdn • QueryParams

Table 9-643 occnp_nrfclient_discovery_cache_support_expired_total

Field	Details
Description	Metric for expired cache record scenario. This metric counts cases when a cached discovery response is not eligible to be returned due to expiration and a new response must be retrieved again from NRF.
Type	Counter
Dimensions	• NfType • NfInstanceID • NfFqdn • QueryParams

Table 9-644 occnp_nrfclient_discovery_cache_support_failover

Field	Details
Description	Metric for cache fail over scenario. This metric counts cases when the response was returned by the cache fail over logic.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-644 (Cont.) occnp_nrfclient_discovery_cache_support_failover

Field	Details
Dimensions	• NfType • NfInstanceID • NfFqdn • QueryParams

Table 9-645 occnp_nrfclient_discovery_cache_support_cache_non_cache_total

Field	Details
Description	Metric for non-cache scenario. This metrics counts cases when the discovery request parameters do not fully match with the configuration parameters.
Type	Counter
Dimensions	• NfType • NfInstanceID • NfFqdn

Table 9-646 occnp_nrfclient_discovery_cache_support_empty_response_total

Field	Details
Description	Metric for empty response scenario. This metric will count cases when an empty response was returned to NF from Cache or NRF.
Type	Counter
Dimensions	• NfType • NfInstanceID • NfFqdn • QueryParams • TypeSource

Table 9-647 occnp_nrfclient_discovery_cache_support_cache_lookup_seconds

Field	Details
Description	Metric for cache lookups. This metric measures time taken to perform cache lookups from cache or DB without considering the complete request flow.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn

Table 9-648 occnp_nrfclient_discovery_cache_support_backend_response_seconds

Field	Details
Description	Metric for cached and non-cached responses returned to backend NF. This metric measures the time taken to perform the complete request flow when response was taken from cache or DB or NRF.
Type	Histogram

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-648 (Cont.) occnp_nrfclient_discovery_cache_support_backend_response_seconds

Field	Details
Dimensions	• NfType • NfInstanceID • NfFqdn • TypeSource

Table 9-649 occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_bucket

Field	Details
Description	This metric is used to perform the cache lookup.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn
Examples	occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_bucket{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",le="0.01",} 19.0

Table 9-650 occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_count

Field	Details
Description	This metric is used to get a count of cache lookup requests.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn
Examples	occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_count{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",} 19.0

Table 9-651 occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_max

Field	Details
Description	This metric provides the maximum value of cache lookup.
Type	Gauge
Dimensions	• NfType • NfInstanceID • NfFqdn
Examples	occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_max{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",} 1.7408E-5

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-652 occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_sum

Field	Details
Description	This metric provides the sum of cache lookup.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn
Examples	occnp_nrfclient_discovery_cache_support_cache_lookup_seconds_sum{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",} 0.001040425

Table 9-653 occnp_nrfclient_discovery_cache_support_backend_response_seconds_bucket

Field	Details
Description	This metric is used to peg the backend response time for cached and non-cached responses
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_backend_response_seconds_bucket{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="Cache",le="0.01",} 19.0

Table 9-654 occnp_nrfclient_discovery_cache_support_backend_response_seconds_count

Field	Details
Description	This metric provides the count of cached responses.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_backend_response_seconds_count{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="Cache",} 19.0

Table 9-655 occnp_nrfclient_discovery_cache_support_backend_response_seconds_max

Field	Details
Description	This metric provides maximum backend response time for cached responses.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-655 (Cont.) occnp_nrfclient_discovery_cache_support_backend_response_seconds_max

Field	Details
Type	Gauge
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_backend_response_seconds_max{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="Cache",} 3.2963E-5

Table 9-656 occnp_nrfclient_discovery_cache_support_backend_response_seconds_sum

Field	Details
Description	This metric provides the sum of backend response time for cached responses.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_backend_response_seconds_sum{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="Cache",} 0.001164615

Table 9-657 occnp_nrfclient_discovery_cache_support_profiles_per_response_bucket

Field	Details
Description	This metric is used to measure the number of producer profiles returned to backend NF.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_profiles_per_response_bucket{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="Cache",le="1.0",} 1.0

Table 9-658 occnp_nrfclient_discovery_cache_support_profiles_per_response_count

Field	Details
Description	This metric provides the count of number of producer profiles returned to backend NF for all responses.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-658 (Cont.) occnp_nrfclient_discovery_cache_support_profiles_per_response_count

Field	Details
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_profiles_per_response_count{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="Cache",} 19.0

Table 9-659 occnp_nrfclient_discovery_cache_support_profiles_per_response_max

Field	Details
Description	This metric provides the maximum number of producer profiles returned to backend NF in particular response.
Type	Gauge
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_profiles_per_response_max{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="Cache",} 5.0

Table 9-660 occnp_nrfclient_discovery_cache_support_profiles_per_response_sum

Field	Details
Description	This metric provides the sum of producer profiles returned to backend NF in all responses.
Type	Histogram
Dimensions	• NfType • NfInstanceID • NfFqdn • SourceType
Examples	occnp_nrfclient_discovery_cache_support_profiles_per_response_sum{NfFqdn="occnp-ocpm-ingress-gateway.ocpcf.svc",NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0123",NfType="PCF",SourceType="NRF",} 420.0

Table 9-661 occnp_nrfclient_nfUpdate_status

Field	Details
Description	This metric marks the status of the NfUpdate Service Operation.
Type	Gauge

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-661 (Cont.) occnp_nrfclient_nfUpdate_status

Field	Details
Dimensions	• NfFqdn • NfInstanceID • NfType • app_kubernetes_io_instance • app_kubernetes_io_managed_by • app_kubernetes_io_name • app_kubernetes_io_part_of • app_kubernetes_io_version • application • container • endpoint • engVersion • helm_sh_chart • instance • io_kompose_service • job • microservice • mktgVersion • namespace • pod • pod_template_hash • vendor
Examples	occnp_nrfclient_nfUpdate_status{NfFqdn="occnp-occnp-ingress-gateway.occnp", NfInstanceID="fe7d992b-0541-4c7d-ab84-c6d2410a2410", NfType="PCF", app_kubernetes_io_instance="occnp", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="nrf-client-nfmanagement", app_kubernetes_io_part_of="nrf-client", app_kubernetes_io_version="24.1.5.0.0", application="occnp", container="nrf-client-nfmanagement", endpoint="cnc-metrics", engVersion="24.1.5", helm_sh_chart="nrf-client-nfmanagement-24.1.5", instance="10.233.109.152:9000", io_kompose_service="occnp-occnp-nrf-client-nfmanagement", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp-nrf-client-nfmanagement", mktgVersion="24.1.5.0.0", namespace="occnp", pod="occnp-occnp-nrf-client-nfmanagement-8f94667cf-bbhls", pod_template_hash="8f94667cf", vendor="Oracle"}

9.32 Error Mapping Metrics

Table 9-662 occnp_error_handler_in_total

Field	Details
Description	This metric counts the number of requests reached the error-handler. This metric is incremented on initialization of error handling.
Type	Counter
Dimensions	• application • application_exception • wrapped_exception
Example	occnp_error_handler_in_total{application="policyds",application_exception="HttpException",wrapped_exception="TimeoutException",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-663 occnp_error_handler_exec_total

Field	Details
Description	This metric counts the number of times error handling is performed. It will only increment if a rule is found and executed. Metric on error handling performed by framework.
Type	Counter
Dimensions	• application • application_exception • error_type • operation • origin • rule_name • source_interface • target • wrapped_exception
Example	occnp_error_handler_exec_total{application="policyds",application_exception="HttpException",error_type="INTERNAL",operation="LOOKUP",origin="HTTP",rule_name="HTTP_REQUEST",source_interface="POLICY",status="502",target_interface="BSF",wrapped_exception="BadGateway",} 1.0

Table 9-664 occnp_error_handler_out_total

Field	Details
Description	This metric counts the number of requests exited the error-handler. This metric is incremented on completion of error handling.
Type	Counter
Dimensions	• application • application_exception • error_resolved • wrapped_exception
Example	occnp_error_handler_out_total{application="policyds",application_exception="HttpException",error_resolved="true",wrapped_exception="BadRequest",} 1.0

9.33 Metrics for Automated Certificate Lifecycle Management

The following metrics are used to support automated certificate lifecycle management for Policy:

Table 9-665 oc_certificatemanagement_tls_certificate_info

Field	Details
Description	This metric is used to peg status of TLS certificates.
Type	Guage
Dimensions	• CertificateName • SecretName • Status (VALID,CORRUPT,MISSING,EXPIRED) • Service (IngressGateway,EgressGateway)
Example	

Copyright © 2019, 2026, Oracle and/or its affiliates.

9.34 Common Metrics

This section describes the metrics and examples for metrics that are common to all the services.

Table 9-666 occnp_http_message_priority_request_count_total

Field	Details
Description	This metric is pegged when PCF receives an incoming request or there is an outgoing request from PCF. This metric applies to the SM service, User Services (CHF Connector and UDR Connector), and Binding Services. Future releases might add support for additional services.
Type	Counter
Dimensions	• application • direction Possible values: – in – out • rcvd_priority Possible values: any value between 0 and 31 • eval_priority Possible values: any value between 0 and 31 • interfaceType Possible values: – nudr-dr – nchf-spendinglimitcontrol – nbsf_Management – npcf-SMPolicyControl – npcf_PolicyAuthorization • msgType Possible values: – Create – Update – Delete – UpdateNotify – TerminateNotify – Register – Deregister – Query – Subscribe – Resubscribe – Unsubscribe

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-666 (Cont.) occnp_http_message_priority_request_count_total

Field	Details
Example	occnp_http_message_priority_request_count_total{app_kubernetes_io_instance="xxx", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="sm-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="26.1.200-ocngf-pre-dev-xxx.0.0", application="occnp", container="sm-service", direction="in", endpoint="cnc-metrics", engVersion="26.1.200-ocngf-pre-dev-titans", eval_priority="24", exported_application="pcf_smservice", helm_sh_chart="sm-service-26.1.200-ocngf-pre-dev-xxx", hostname="xxx-pcf-smservice-74d9d88474-jqn4m", instance="10.233.114.76:9000", interfaceType="Npcf_SMPolicyControl", io_kompose_service="xxx-pcf-smservice", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_sm", mktgVersion="26.1.200-ocngf-pre-dev-xxx.0.0", msgType="Create", namespace="hm3-ns03", pod="titans-pcf-smservice-74d9d88474-jqn4m", pod_template_hash="74d9d88474", rcvd_priority="24", vendor="Oracle"} 1.0 occnp_http_message_priority_request_count_total{app_kubernetes_io_instance="xxx", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="26.1.200-ocngf-pre-dev-xxx.0.0", application="occnp", container="user-service", direction="out", endpoint="cnc-metrics", engVersion="26.1.200-ocngf-pre-dev-xxx", eval_priority="NA", exported_application="pcf_userservice", helm_sh_chart="user-service-26.1.200-ocngf-pre-dev-xxx", hostname="xxx-occnp-udr-connector-7f75dcf879-nlp6m", instance="10.233.114.174:9000", interfaceType="Nudr_DataRepository", io_kompose_service="xxx-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="26.1.200-ocngf-pre-dev-xxx.0.0", msgType="Get_Policy_Data", namespace="hm3-ns03", pod="xxx-occnp-udr-connector-7f75dcf879-nlp6m", pod_template_hash="7f75dcf879", rcvd_priority="24", vendor="Oracle"} 1.0

Table 9-667 occnp_http_message_priority_response_count_total

Field	Details
Description	This metric is pegged when PCF receives an incoming response or when there is an outgoing response from PCF. This metric applies to the SM service, User Services (CHF Connector and UDR Connector), and Binding Services. Future releases might add support for additional services.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-667 (Cont.) occnp_http_message_priority_response_count_total

Field	Details
Dimensions	• application • direction Possible values: – in – out • rcvd_priority Possible values: any value between 0 and 31 • eval_priority Possible values: any value between 0 and 31 • interfaceType Possible values: – nudr-dr – nchf-spendinglimitcontrol – nbsf_Management – npcf-SMPolicyControl – npcf_PolicyAuthorization • msgType Possible values: – Create – Update – Delete – UpdateNotify – TerminateNotify – Register – Deregister – Query – Subscribe – Resubscribe – Unsubscribe • response_code Possible values: – 1xx – 2xx – 3xx – 4xx – 5xx **Note:** response_code always reflects the specific code received, such as 200, 201, 404, or 500. References to 1xx, 2xx, 3xx, 4xx, or 5xx are used as placeholders for groups of response codes and should not be interpreted as actual output values from the metric.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-667 (Cont.) occnp_http_message_priority_response_count_total

Field	Details
Example	occnp_http_message_priority_response_count_total{app_kubernetes_io_instance="xxx", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="sm-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="26.1.200-ocngf-pre-dev-xxx.0.0", application="occnp", container="sm-service", direction="out", endpoint="cnc-metrics", engVersion="26.1.200-ocngf-pre-dev-titans", eval_priority="NA", exported_application="pcf_smservice", helm_sh_chart="sm-service-26.1.200-ocngf-pre-dev-xxx", hostname="xxx-pcf-smservice-74d9d88474-jqn4m", instance="10.233.114.76:9000", interfaceType="Npcf_SMPolicyControl", io_kompose_service="xxx-pcf-smservice", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_sm", mktgVersion="26.1.200-ocngf-pre-dev-xxx.0.0", msgType="Create", namespace="hm3-ns03", pod="xxx-pcf-smservice-74d9d88474-jqn4m", pod_template_hash="74d9d88474", rcvd_priority="NA", responseCode="201", vendor="Oracle"} occnp_http_message_priority_response_count_total{app_kubernetes_io_instance="xxx", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="user-service", app_kubernetes_io_part_of="occnp", app_kubernetes_io_version="26.1.200-ocngf-pre-dev-xxx.0.0", application="occnp", container="user-service", direction="in", endpoint="cnc-metrics", engVersion="26.1.200-ocngf-pre-dev-xxx", eval_priority="NA", exported_application="pcf_userservice", helm_sh_chart="user-service-26.1.200-ocngf-pre-dev-xxx", hostname="xxx-occnp-udr-connector-7f75dcf879-nlp6m", instance="10.233.114.174:9000", interfaceType="Nudr_DataRepository", io_kompose_service="xxx-occnp-udr-connector", job="occne-infra/occne-nf-cnc-podmonitor", microservice="occnp_pcf_user", mktgVersion="26.1.200-ocngf-pre-dev-titans.0.0", msgType="Subscribe", namespace="hm3-ns03", pod="xxx-occnp-udr-connector-7f75dcf879-nlp6m", pod_template_hash="7f75dcf879", rcvd_priority="NA", responseCode="201", vendor="Oracle"}

Table 9-668 hikaricp_connections_idle

Field	Details
Description	Number of established but idle connections.
Type	Gauge
Dimension	• application • name
Example	hikaricp_connections_idle{application="bsf-management-service",name="dataSource",

Table 9-669 hikaricp_connections_max

Field	Details
Description	Maximum number of active connections that can be allocated at the same time.
Type	Gauge
Dimension	• application • name
Example	hikaricp_connections_max{application="bsf-management-service",name="dataSource",

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-670 hikaricp_connections_min

Field	Details
Description	Minimum number of idle connections in the pool.
Type	Gauge
Dimension	• application • name
Example	hikaricp_connections_min{application="bsf-management-service",name="dataSource",

Table 9-671 hikaricp_connections_active

Field	Details
Description	Current number of active connections that have been allocated from the data source.
Type	Gauge
Dimension	• application • name
Example	hikaricp_connections_active{application="bsf-management-service",name="dataSource",

Table 9-672 executor_queued_tasks

Field	Details
Description	
Type	Gauge
Dimension	• application • hostname • name
Example	executor_queued_tasks{application="xxx",hostname="xx", name="HttpServerCustomThreadPoolExecutor"} 0.0

Table 9-673 executor_active_threads

Field	Details
Description	
Type	Gauge
Dimension	• application • hostname • name
Example	executor_active_threads{application="xxx",hostname="xx", name="HttpServerCustomThreadPoolExecutor"}

Table 9-674 executor_pool_max_threads

Field	Details
Description	Undertow max worker pool size.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-674 (Cont.) executor_pool_max_threads

Field	Details
Type	Gauge
Dimensions	• application • hostname • name
Example	executor_pool_max_threads{application="xx",hostname="xx", name="HttpServerCustomThreadPoolExecutor"} 16.0

Table 9-675 executor_pool_size_threads

Field	Details
Description	Undertow worker pool size.
Type	Gauge
Dimensions	• application • hostname • name
Example	executor_pool_size_threads{application="xx",hostname="xx", name="HttpServerCustomThreadPoolExecutor"} 4.0

9.35 ASM Metrics

This section describes the ASM metrics.

Table 9-676 upstream_rq_timeout

Field	Details
Description	Maximum duration allowed for a request to an upstream service to complete, including any retries. This timeout is a critical configuration in proxy services like Envoy, which sits between downstream clients and upstream servers.
Type	Counter
Dimension	• cluster_name • microservice
Example	{cluster_name="inbound|8000||", microservice="occnp_pcf_sm"}

Table 9-677 upstream_rq_active

Field	Details
Description	Tracks the number of currently active, or in-flight, requests to an upstream service. This metric is crucial for monitoring service mesh performance and resource utilization.
Type	Gauge
Dimension	• cluster_name • microservice
Example	{cluster_name="inbound|8000||", microservice="occnp-occnp-ingress-gateway"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-678 upstream_rq_rx_reset

Field	Details
Description	Its an Envoy proxy counter that tallies the number of upstream requests that were terminated by a TCP connection reset from the remote, or upstream, host.
Type	Counter
Dimension	• cluster_name • microservice
Example	{cluster_name="inbound|8000||", microservice="occnp-occnp-egress-gateway"}

Table 9-679 upstream_rq_tx_reset

Field	Details
Description	It is an Envoy-level counter that tracks the total number of HTTP requests that were reset locally by the Envoy proxy before receiving a response from the upstream service.
Type	Counter
Dimension	• cluster_name • microservice
Example	{cluster_name="inbound|38868||", microservice="oc-diam-gateway"}

Table 9-680 upstream_cx_active

Field	Details
Description	It is an Envoy metric that tracks the number of currently active connections from an Envoy proxy to its upstream cluster. It is used in service mesh technologies like Istio and AWS App Mesh, which rely on the Envoy proxy for their data plane.
Type	Gauge
Dimension	• cluster_name • microservice
Example	{cluster_name="prometheus_stats", microservice="occnp_pcf_sm"}

Table 9-681 downstream_cx_ssl_total

Field	Details
Description	It is a counter used by the Envoy proxy to track the total number of new downstream client connections that used a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) handshake.
Type	Counter
Dimension	• cluster_name • microservice
Example	{cluster_name="xds-grpc", microservice="occnp_pcf_sm"}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table 9-682 downstream_cx_http2_active

Field	Details
Description	It refers to the number of currently active HTTP/2 connections from a client (the "downstream").
Type	Gauge
Dimensions	• cluster_name • microservice
Example	{cluster_name="prometheus_stats", microservice="occnp-occnp-egress-gateway"}

Table 9-683 downstream_cx_active

Field	Details
Description	It measures the number of active network connections to a service proxy like Envoy, and is used to monitor the performance and stability of a service.
Type	Gauge
Dimensions	• cluster_name • microservice
Example	{cluster_name="prometheus_stats", microservice="occnp-occnp-ingress-gateway"}

Table 9-684 downstream_cx_total

Field	Details
Description	Counts the total number of connections that Envoy has accepted from its downstream clients (like web browsers or mobile apps) to a specific listener. It's a counter metric that helps in understanding overall connection volume and can be used to calculate connections per second (CPS) and analyze connection churn, indicating the rate at which clients are creating and closing connections to the proxy.
Type	Counter
Dimensions	• cluster_name • microservice
Example	{cluster_name="xds-grpc", microservice="occnp-occnp-egress-gateway"}

9.36 Sbi-NF-Peer-Info Header Metrics

The following table describes the Sbi-NF-Peer-Info Header Metrics:

The metrics are implemented as part of this feature with the following dimensions:

- `operation_type`: Identifies the SBI operation associated with the `NF-Peer-Info` header. Supported values are:
  - `create`: Used for create operations, such as SM Create and Binding Register to BSF.
  - `update`: Used for update operations, such as SM Update.
  - `delete`: Used for delete operations, such as SM Delete, Binding Deregister to BSF, and UDR connector delete operations.
  - `update_notify`: Used for update notification messages sent to the SMF.
  - `terminate_notify`: Used for termination notification messages sent to the SMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

  - `subscribe`: Used for subscription requests sent to the CHF.
  - `unsubscribe`: Used for unsubscription requests sent to the CHF.
  - `AuditNotify`: Used for BSF audit operations in the binding service.
  - `get`: Used for UDR connector get operations.
  - `post`: Used for UDR connector post operations.
  - `patch`: Used for UDR connector patch operations.
  - `put`: Used for UDR connector put operations.
  - `notify`: Used for notifications sent to the UDR or CHF connector.
- `external_nf`: Identifies the external NF that participates in the communication. Supported values are:
  - `SMF`: Communication between PCF and SMF.
  - `UDR`: Communication between PCF and UDR.
  - `CHF`: Communication between PCF and CHF.
  - `BSF`: Communication between PCF and BSF.
- `validation_status`: Indicates whether the received 3gpp-Sbi-NF-Peer-Info header satisfies the NF-Peer-Info validation rules defined for this feature. Supported values are:
  - `invalid`: Set when the received NF-Peer-Info header contains the srcservinst parameter without the corresponding srcinst parameter.
  - `valid`: Set for all received headers that do not meet the invalid condition.
  - `NA`: Used for all metrics associated with NF-Peer-Info headers sent by PCF to external NFs.

> **Note**
>
> The `validation_status` dimension is based only on the NF-Peer-Info attribute dependency validation defined earlier. It does not validate the format, syntax, or contents of individual header parameters, such as `srcinst`, `srcservinst`, `dstinst`, or `dstservinst`. For example, UUID format validation is not performed when determining the dimension value.

Table 9-685 occnp_nf_peer_info_header_received_total

Field	Details
Description	The PCF reports the total number of incoming HTTP messages that include the 3gpp-Sbi-NF-Peer-Info header.
Metric Type	Counter
Dimensions	• operation_type • external_nf • dst_instance • dst_serv_instance • src_instance • src_serv_instance • validation_status

Copyright © 2019, 2026, Oracle and/or its affiliates.

Example:

- occnp_nf_peer_info_header_received_total{application="pcf_smservice",dst_instance="di48b3cb-265d-40fe-9368-db4ac72b7716",dst_serv_instance="dsi48b3cb-265d-40fe-9368-db4ac72b7716",external_nf="SMF",operation_type="create",src_instance="si48b3cb-265d-40fe-9368-db4ac72b7716",src_serv_instance="ss48b3cb-265d-40fe-9368-db4ac72b7716",validation_status="valid"} 1.0
- occnp_nf_peer_info_header_received_total{application="pcf_smservice",dst_instance="di48b3cb-265d-40fe-9368-db4ac72b7716",dst_serv_instance="",external_nf="SMF",operation_type="create",src_instance="",src_serv_instance="ssi48b3cb-265d-40fe-9368-db4ac72b7716",validation_status="invalid"} 1.0

Table 9-686 occnp_nf_peer_info_header_sent_total

Field	Details
Description	The PCF reports the total number of outgoing HTTP messages that include the 3gpp-Sbi-NF-Peer-Info header.
Metric Type	Counter
Dimensions	• operation_type • external_nf • dst_instance • dst_serv_instance • src_instance • src_serv_instance • validation_status

Example:

- occnp_nf_peer_info_header_sent_total{application="pcf_smservice",dst_instance="si48b3cb-265d-40fe-9368-db4ac72b7716",dst_serv_instance="ss48b3cb-265d-40fe-9368-db4ac72b7716",external_nf="SMF",operation_type="create",src_instance="site1",src_serv_instance="03063893-cf9e-4f7a-9827-067f6fa9dd02",validation_status="NA"} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

10 CNC Policy KPIs

This section provides information about Key Performance Indicators (KPIs) used for Cloud Native Core Policy.

> **Note**
>
> Sample CNC Policy dashboard for Grafana is delivered to the customer through CNC Policy Custom Templates. The metrics and functions used to achieve KPIs are covered in CNC Policy Custom Templates as well.

CPU and Memory Usage

KPI Name	KPI Details	Metric used for KPI
POD-Count	Measures the number of PCF SM Service pods available in the system.	count(container_memory_usage_bytes{container_name='pcf-smservice',namespace=\"$namespace\"})
POD-Count	Measures the number of PCF User Service pods available in the system.	count(container_memory_usage_bytes{container_name='pcf-userservice',namespace=\"$namespace\"})
POD-Count	Measures the number of PRE pods available in the system.	count(container_memory_usage_bytes{container_name='ocpm-pre',namespace=\"$namespace\"})
POD-Count	Measures the number of PCF AM Service pods available in the system.	count(container_memory_usage_bytes{container_name='pcf-amservice',namespace=\"$namespace\"})
POD-Count	Measures the number of NRF Client-NRF Discovery pods available in the system.	count(container_memory_usage_bytes{container_name='nrf-client-nfdiscovery',namespace=\"$namespace\"})
POD-Count	Measures the number of Ingress Gateway pods available in the system.	count(container_memory_usage_bytes{container_name='ingress-gateway',namespace=\"$namespace\"})
POD-Count	Measures the number of Egress Gateway pods available in the system.	count(container_memory_usage_bytes{container_name='egress-gateway',namespace=\"$namespace\"})

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI
Total TPS	Measures the rate of (Ingress + Egress + Diameter) Gateway requests received at CNC Policy.	sum(rate(occnp_oc_ingressgateway_http_requests_total{$namespacelbl="$namespace"}[2m])) + sum(rate(occnp_oc_egressgateway_http_requests_total{$namespacelbl="$namespace",Direction="egressOut"}[2m])) + sum(rate(occnp_diam_request_network_total{$namespacelbl="$namespace", appId!="0"}[2m]))
Memory-Usage	Measures the current memory usage in bytes.	sum(container_memory_usage_bytes{image!=",namespace=\"$namespace\"})
Memory-Usage	Measures the memory usage (in bytes) for the top 16 memory users by each pod.	topk(16,sum(container_memory_usage_bytes{image!=",namespace=\"$namespace\"}) by (container_name))
CPU-Usage	Measures the number of cores being used by each pod.	sum(rate(container_cpu_usage_seconds_total{image!=",namespace=\"$namespace\",container_name!='POD'}[2m])) by (container_name)

Session Management Service

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
SM Create Requests	Measures the rate of requests received at PCF to create SM policy association.	sum(rate(ocpm_ingress_request_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"create\",dnn=\"dnn1\",snssai=\"11-abc123\"}[2m]))	Create	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
SM Create Success Response	Measures the rate of requests for which SM policy associations are created successfully.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"create\",response_code=\"2xx\"}[2m])) **Note**: [2m] determines the rate interval at which the value needs to be calculated. This value is strictly used for calculation purpose and can be modified accordingly as per customer requirements. It can be changed either before or after adding the sample to Policy Grafana dashboard.	Create	2xx
SM Create Failure Response	Measures the rate at which create requests for SM policy association are rejected by PCF due to certain errors.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"create\",response_code!=\"2xx\"}[2m]))	Create	2xx
SM Update Request	Measures the rate at which requests are received at PCF to update the SM Policy association data.	sum (rate(ocpm_ingress_request_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"update\",dnn=\"dnn1\",snssai=\"11-abc123\"}[2m]))	Update	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
SM Update Success Response	Measures the rate at which requests for updating SM policy association (already existing) are updated successfully.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"update\",response_code=\"2xx\"}[2m]))	Update	2xx
SM Update Failure Response	Measures the rate at which requests for updating SM policy association (already existing) are rejected by PCF due to certain errors at the consumer end.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"update\",response_code=\"4xx\"}[2m]))	Update	4xx
SM Delete Requests	Measures the rate of requests received at PCF to delete (or deregister) SM policy association.	sum (rate(ocpm_ingress_request_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"delete\",dnn=\"dnn1\",snssai=\"11-abc123\"}[2m]))	Delete	Not Applicable
SM Delete Success Responses	Measures the rate at which requests for deleting SM policy association (already existing) are deleted successfully.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"delete\",response_code=\"2xx\"}[2m]))	Delete	2xx
SM Delete Failure Responses	Measures the rate at which requests for deleting SM policy association (already existing) are rejected by PCF due to certain errors at the consumer end.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"delete\",response_code!=\"2xx\"}[2m]))	Delete	2xx

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
SM Update Notify Requests	Measures the rate at which requests are initiated by PCF towards SMF to update the PCC rules PDU session related policy context.	sum (rate(ocpm_egress_request_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"update_notify\"}[2m]))	Update Notify	Not Applicable
SM Update Notify Success Response	Measures the rate at which update requests received at SMF (initiated by PCF) are updated successfully.	sum (rate(ocpm_egress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"update_notify\",response_code=\"2xx\"}[2m]))	Update Notify	2xx
SM Update Notify Failure Response	Measures the rate at which update requests received at SMF (initiated by PCF) are rejected due to certain errors.	sum (rate(ocpm_egress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"update_notify\",response_code!=\"2xx\"}[2m]))	Update Notify	2xx
SM Terminate Notify Requests	Measures the rate at which requests are initiated by PCF towards SMF to delete SM Policy association of a PDU session.	sum (rate(ocpm_egress_request_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"terminate_notify\"}[2m]))	Terminate Notify	Not Applicable
SM Terminate Notify Success Response	Measures the rate at which delete requests received at SMF (initiated by PCF) are processed successfully.	sum (rate(ocpm_egress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"terminate_notify\",response_code=\"2xx\"}[2m]))	Terminate Notify	2xx

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
SM Terminate Notify Failure Response	Measures the rate at which delete requests received at SMF (initiated by PCF) are rejected due to certain errors.	sum (rate(ocpm_egress_response_total{kubernetes_namespace=\"$namespace\",servicename_3gpp=\"npcf-smpolicycontrol\",operation_type=\"terminate_notify\",response_code!=\"2xx\"}[2m]))	Terminate Notify	2xx

Diameter Gateway Request and Response

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Rx AAR Initial Request	Measures the rate of Rx AAR initial messages received by Diameter Gateway.	sum (rate(ocpm_ingress_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"create\",servicename_3gpp=\"rx\"}[2m]))	Create	Not Applicable
Rx AAA Initial Response Success	Measures the rate at which Diameter Gateway processes Rx AAR messages successfully by sending Rx AAA as initial response.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"create\",servicename_3gpp=\"rx\",response_code=\"2xxx\"}[2m]))	Create	2xxx
Rx AAR Update Request	Measures the rate of Rx AAR update requests received by Diameter Gateway.	sum (rate(ocpm_ingress_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"update\",servicename_3gpp=\"rx\"}[2m]))	Update	Not Applicable
Rx AAR Update Response Success	Measures the rate at which Diameter Gateway processes Rx AAR update requests successfully.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"update\",servicename_3gpp=\"rx\",response_code=\"2xxx\"}[2m]))	Update	2xxx

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Rx STR Request	Measures the rate of the Session-Termination-Request (STR) messages received by Diameter Gateway.	sum (rate(ocpm_ingress_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"terminate\",servicename_3gpp=\"rx\",response_code=\"2xxx\"}[2m]))	Terminate	2xxx
Rx STR Response Success	Measures the rate at which Diameter Gateway processes Rx STR messages successfully.	sum (rate(ocpm_ingress_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"terminate\",servicename_3gpp=\"rx\",response_code=\"2xxx\"}[2m]))	Terminate	2xxx

UDR Tracking Request and Response

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Query SM Data UDR Request	Measures the number of query requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"get\",service_version=\"v1\",servicename_3gpp=\"nudr-dr\"}[2m]))	GET	Not Applicable
Unsubscribe UDR Request	Measures the number of unsubscribe requests sent by PCF to UDR.	sum(rate(ocpm_udr_tracking_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nudr-dr\"}[2m]))	Unsubscribe	Not Applicable
Subscribe Total UDR Request	Measures the number of subscribe requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nudr-dr\"}[2m]))	Subscribe	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Subscribe UDR Success	Measures the number of success responses received for subscribe requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nudr-dr\",response_code=\"2xx\"}[2m]))	Subscribe	2xx
Subscribe UDR Failed	Measures the number of unsuccessful responses received for subscribe requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nudr-dr\",response_code!=\"2xx\"}[2m]))	Subscribe	2xx
Query SM Data Success	Measures the number of success responses received for query requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"get\",servicename_3gpp=\"nudr-dr\",response_code=\"2xx\"}[2m]))	GET	2xx
Query SM Data Failed	Measures the number of unsuccessful responses received for query requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"get\",servicename_3gpp=\"nudr-dr\",response_code!=\"2xx\"}[2m]))	GET	2xx
Unsubscribe UDR Success	Measures the number of success responses received for unsubscribe requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nudr-dr\",response_code=\"2xx\"}[2m]))	Unsubscribe	2xx

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Unsubscribe UDR Failed	Measures the number of unsuccessful responses received for unsubscribe requests sent by PCF to UDR.	sum (rate(ocpm_udr_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nudr-dr\",response_code!=\"2xx\"}[2m]))	Unsubscribe	2xx
Unsubscribe UDR Timeout	Measures the number of unsubscribe requests not processed successfully at UDR due to timeout error.	sum (rate(ocpm_udr_tracking_request_timeout_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nudr-dr\"}[2m]))	Unsubscribe	Not Applicable
Subscribe UDR Timeout	Measures the number of subscribe requests not processed successfully at UDR due to timeout error.	sum (rate(ocpm_udr_tracking_request_timeout_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nudr-dr\"}[2m]))	Subscribe	Not Applicable
Query UDR Timeout	Measures the number of query requests not processed successfully at UDR due to timeout error.	sum (rate(ocpm_udr_tracking_request_timeout_total{kubernetes_namespace=\"$namespace\",operation_type=\"get\",servicename_3gpp=\"nudr-dr\"}[2m]))	GET	Not Applicable

Diameter Egress Request and Response

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Rx RAR Request	Measures the number of requests sent to external NFs through Egress Gateway.	sum (rate(ocpm_egress_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"update_notify\",servicename_3gpp=\"rx\"}[2m]))	Update Notify	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Rx RAR Response Success	Measures the number of success responses received for requests sent to external NFs through Egress Gateway.	sum (rate(ocpm_egress_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"update_notify\",servicename_3gpp=\"rx\",response_code=\"2xxx\"}[2m]))	Update Notify	2xxx

User Service Inbound

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
GET Request to User Service	Measures the number of query requests received at User Service.	sum (rate(ocpm_userservice_inbound_count_total{kubernetes_namespace=\"$namespace\",operation_type=\"get\",service_resource=\"user-service\"}[2m]))	GET	Not Applicable
Delete Request to User Service	Measures the number of delete requests received at User Service.	sum (rate(ocpm_userservice_inbound_count_total{kubernetes_namespace=\"$namespace\",operation_type=\"delete\",service_resource=\"user-service\"}[2m]))	DELETE	Not Applicable
Notify Request to User Service	Measures the number of notify requests received at User Service.	sum (rate(ocpm_userservice_inbound_count_total{kubernetes_namespace=\"$namespace\",operation_type=\"notify\",service_resource=\"user-service\"}[2m]))	Notify	Not Applicable

Diameter Connector

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Diameter Connector	Measures the total number of connections established towards Diameter Gateway.	sum (rate(occnp_diam_conn_network{kubernetes_namespace=\"$namespace\"}[2m]))	Not Applicable	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Diameter Connector	Measures the total number of connections established towards SM service application.	sum (rate(occnp_diam_conn_app_network{kubernetes_namespace=\"$namespace\"}[2m]))	Not Applicable	Not Applicable

Egress Request and Response

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Egress Delete Request	Measures the number of delete requests sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_requests_total{kubernetes_namespace=\"$namespace\",Method='DELETE'}[2m]))	DELETE	Not Applicable
Egress Delete Response	Measures the number of responses to Delete requests – sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_responses_total{kubernetes_namespace=\"$namespace\",Method='DELETE'}[2m]))	DELETE	Not Applicable
Egress GET request	Measures the number of query requests sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_requests_total{kubernetes_namespace=\"$namespace\",Method='GET'}[2m]))	GET	Not Applicable
Egress GET response	Measures the number of responses to query requests – sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_responses_total{kubernetes_namespace=\"$namespace\",Method='GET'}[2m]))	GET	Not Applicable
Egress POST request	Measures the number of POST requests sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_requests_total{kubernetes_namespace=\"$namespace\",Method='POST'}[2m]))	POST	Not Applicable
Egress POST response	Measures the number of responses to POST requests – sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_responses_total{kubernetes_namespace=\"$namespace\",Method='POST'}[2m]))	POST	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

CHF Tracking Request

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
CHF-Subscribe-request	Total number of subscribe requests (spending limit status information) from CHF server.	sum (rate(ocpm_chf_tracking_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\"}[2m]))	Subscribe	Not Applicable
CHF-Unsubscribe-request	Total number of unsubscribe requests (spending limit status information) being sent to CHF server.	sum (rate(ocpm_chf_tracking_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\"}[2m]))	Unsubscribe	Not Applicable

PolicyDS

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Client Request Total Search	Measures the number of messages sent to LDAP gateway from PolicyDS for LDAP search requests.	sum (rate(client_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"SEARCH\",workflow=\"LDAP\"}[2m]))		
Client Response Total Search	Measures the number of responses sent by LDAP gateway for LDAP search requests from PolicyDS.	sum (rate(client_response_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"SEARCH\",workflow=\"LDAP\",response=\"200\"}[2m]))		

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Server Request User Service	Measures the number of messages sent to LDAP gateway from PolicyDS for User service search requests.	sum (rate(server_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"SEARCH\",task=\"USER_SERVICE\"}[2m]))		
Server Request LDAP	Measures the number of messages sent to LDAP gateway from PolicyDS for LDAP retrieve requests.	sum (rate(server_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"GET\",task=\"LDAP\"}[2m]))		
Server Request PRE	Measures the number of messages sent to PRE from PolicyDS for inserting the user data.	sum (rate(server_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"INSERT\",task=\"PRE\"}[2m]))		
Server Response Success POST	Measures the number of success responses received for POST requests by PolicyDS.	sum (rate(server_response_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"POST\",response=\"200\"}[2m]))	POST	200

CHF Tracking Response

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Subscribe Success	Measures the total number of success responses for subscribe/fetch spendingLimitStatus requests at CHF connector.	sum (rate(ocpm_chf_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\",response_code=\"2xx\"}[2m]))	Subscribe	2xx

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Subscribe Failure	Measures the total number of failed responses for subscribe/fetch spendingLimitStatus requests at CHF connector.	sum (rate(ocpm_chf_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\",response_code!=\"2xx\"}[2m]))	Subscribe	2xx
Unsubscribe Success	Measures the total number of success responses for unsubscribe spendingLimitStatus requests at CHF connector.	sum (rate(ocpm_chf_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\",response_code=\"2xx\"}[2m]))	Unsubscribe	2xx
Unsubscribe Failure	Measures the total number of failed responses for unsubscribe spendingLimitStatus requests at CHF connector.	sum (rate(ocpm_chf_tracking_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\",response_code!=\"2xx\"}[2m]))	Unsubscribe	2xx
Unsubscribe Timeout	Measures the total number of requests that got timed out at CHF Connector when trying to unsubscribe spendingLimitStatus.	sum (rate(ocpm_chf_tracking_request_timeout_total{kubernetes_namespace=\"$namespace\",operation_type=\"unsubscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\"}[2m]))	Unsubscribe	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Subscribe Timeout	Measures the total number of requests that got timed out at CHF Connector when trying to subscribe/fetch spendingLimitStatus.	sum (rate(ocpm_chf_tracking_request_timeout_total{kubernetes_namespace=\"$namespace\",operation_type=\"subscribe\",servicename_3gpp=\"nchf-spendinglimitcontrol\"}[2m]))	Subscribe	Not Applicable

LDAP

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
LDAP Total Requests	Measures the rate of total number of requests received at LDAP.	sum (rate(ldap_request_total{kubernetes_namespace=\"$namespace\",ReqType=\"GET\"}[2m]))	All	Not Applicable
LDAP Response Success	Measures the rate of total number of successful responses sent to network NFs by LDAP.	sum (rate(ldap_response_total{kubernetes_namespace=\"$namespace\",ReqType=\"GET\",Code=\"2xx\"}[2m]))	All	2xx
LDAP Response Failure	Measures the rate of total number of requests that have been rejected by LDAP due to errors at the end of NF consumers.	sum (rate(ldap_response_total{kubernetes_namespace=\"$namespace\",ReqType=\"GET\",Code!=\"2xx\"}[2m]))	All	2xx

Policy DS

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Client_request_total_search	Measures the sum of total number of requests policyds sends for LDAP Search.	sum (rate(client_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"SEARCH\",workflow=\"LDAP\"}[2m]))	SEARCH	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
Client_response_total_search	Measures the sum of total number of success responses received by policyds for LDAP Search.	sum (rate(client_response_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"SEARCH\",workflow=\"LDAP\",response=\"200\"}[2m]))	SEARCH	200
Server_request_user_service	Measures the total requests received by PolicyDS from NF consumers for UserService search.	sum (rate(server_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"SEARCH\",task=\"USER_SERVICE\"}[2m]))	SEARCH	Not Applicable
Server_request_LDAP	Measures the total number or requests policyds received for LDAP Get request.	sum (rate(server_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"GET\",task=\"LDAP\"}[2m]))	GET	Not Applicable
Server_request_PRE	Measures the total number or requests policyds received for PRE Insert request.	sum (rate(server_request_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"INSERT\",task=\"PRE\"}[2m]))	INSERT	Not Applicable
Server_response_sucess_POST		sum (rate(server_response_total{kubernetes_namespace=\"$namespace\",application=\"policyds\",operation=\"POST\",response=\"200\"}[2m]))	POST	200

10.1 PCRF KPIs

This section provides information about Key Performance Indicators (KPIs) used for PCRF in CNC Policy.

Copyright © 2019, 2026, Oracle and/or its affiliates.

> **Note**
>
> Sample PCRF dashboard for Grafana is provided in the CNC Policy Custom Templates folder as part of the documentation.

CPU, Memory, and Load Level

KPI Name	KPI Details	Metric used for KPI
Pod Health	Shows the health of pods available in the system.	appinfo_service_running{vendor=\"Oracle\", application=\"occnp\", namespace=\"$namespace\"}
POD-Count	Shows the number of PCRF pods available in the system.	count(container_memory_usage_bytes{container='pcrf-core',namespace=\"$namespace\"})
POD-Count	Shows the number of Diameter Gateway pods available in the system.	count(container_memory_usage_bytes{container='diam-gateway',namespace=\"$namespace\"})
POD-Count	Shows the number of PRE pods available in the system.	count(container_memory_usage_bytes{container='pre-service',namespace=\"$namespace\"})
POD-Count	Shows the number of Policy Datasource pods available in the system.	count(container_memory_usage_bytes{container='policyds',namespace=\"$namespace\"})
POD-Count	Shows the number of LDAP Gateway pods available in the system.	count(container_memory_usage_bytes{container='ldap-gateway',namespace=\"$namespace\"})
POD-Count	Shows the number of CM service pods available in the system.	count(container_memory_usage_bytes{container='cm-service',namespace=\"$namespace\"})
POD-Count	Shows the number of Config Server pods available in the system.	count(container_memory_usage_bytes{container='config-server',namespace=\"$namespace\"})
Memory Usage	Shows the current memory usage in bytes.	sum(container_memory_usage_bytes{image!='',namespace=\"$namespace\"})
Memory Usage	Shows the memory usage (in bytes) for the top 10 memory users by each pod.	topk(10, sum(container_memory_usage_bytes{namespace=\"$namespace\"}) by (container))
Service Load Level	Shows the load level of each service.	avg(load_level) by (service)
CPU Usage	Shows the CPU usage by each pod.	sum(rate(container_cpu_usage_seconds_total{image!='',namespace=\"$namespace\",container_name!='POD'}[2m])) by (container_name)

Copyright © 2019, 2026, Oracle and/or its affiliates.

PCRF Success Response

KPI Name	KPI Details	Metric used for KPI	Response Code
CCA_SUCCESS_COUNT	Shows the rate of success responses received at PCRF for CCA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"CCA.*\", responseCode=~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	2xx
AAA_SUCCESS_COUNT	Shows the rate of success responses received at PCRF for AAA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"AAA.*\", responseCode=~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	2xx
ASA_SUCCESS_COUNT	Shows the rate of success responses received at PCRF for ASA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"ASA\", responseCode=~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	2xx
RAA_SUCCESS_COUNT	Shows the rate of success responses received at PCRF for RAA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"RAA\", responseCode=~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	2xx
STA_SUCCESS_COUNT	Shows the rate of success responses received at PCRF for STA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"STA\", responseCode!=\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	2xx

PCRF Failure Response

KPI Name	KPI Details	Metric used for KPI	Response Code
CCA_FAIL_COUNT	Shows the rate of failure responses received at PCRF for CCA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"CCA.*\", responseCode!~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	Other than 2xx
AAA_FAIL_COUNT	Shows the rate of failure responses received at PCRF for AAA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"AAA.*\", responseCode!~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	Other than 2xx

Copyright © 2019, 2026, Oracle and/or its affiliates.

KPI Name	KPI Details	Metric used for KPI	Response Code
ASA_FAIL_COUNT	Shows the rate of failure responses received at PCRF for ASA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"ASA\", responseCode!~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	Other than 2xx
RAA_FAIL_COUNT	Shows the rate of success responses received at PCRF for RAA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"RAA\", responseCode!~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	Other than 2xx
STA_FAIL_COUNT	Shows the rate of failure responses received at PCRF for STA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"STA\", responseCode!~\"2.*\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))	Other than 2xx

PCRF Timeout Failure

KPI Name	KPI Details	Metric used for KPI
ASA_TIMEOUT_COUNT	Shows the rate of failure responses due to timeout for ASA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"ASA\", responseCode=\"timeout\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))
RAA_TIMEOUT_COUNT	Shows the rate of failure responses due to timeout for RAA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"RAA\", responseCode=\"timeout\", namespace=\"$namespace\",container=\"pcrf-core\"}[5m]))

Diameter Gateway Timeout Failure

KPI Name	KPI Details	Metric used for KPI
CCA_TIMEOUT_COUNT	Shows the rate of failure responses due to timeout received at Diameter Gateway for CCA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"CCA.*\", responseCode=\"timeout\", namespace=\"$namespace\",container=\"diam-gateway\"}[5m]))
AAA_TIMEOUT_COUNT	Shows the rate of failure responses due to timeout received at Diameter Gateway for AAA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"AAA.*\", responseCode=\"timeout\", namespace=\"$namespace\",container=\"diam-gateway\"}[5m]))
STA_TIMEOUT_COUNT	Shows the rate of failure responses due to timeout received at Diameter Gateway for STA message type.	sum(rate(occnp_diam_response_local_total{msgType=~\"STA\", responseCode=\"timeout\", namespace=\"$namespace\",container=\"diam-gateway\"}[5m]))

Copyright © 2019, 2026, Oracle and/or its affiliates.

Diameter Gateway Response

KPI Name	KPI Details	Metric used for KPI	Service Operation	Response Code
FAILURE_RATE	Shows the percentage of total failure responses of all incoming messages (for Diameter Gateway and PCRF) per unit time.	sum(rate(occnp_diam_response_local_total{namespace=\"$namespace\",responseCode!~\"2.*\"}[5m])) / sum(rate(occnp_diam_response_local_total{namespace=\"$namespace\"}[5m]))*100	Not Applicable	Other than 2xx
SUCCESS_RATE	Shows the percentage of total success responses of all incoming messages (for Diameter Gateway and PCRF) per unit time.	sum(rate(occnp_diam_response_local_total{namespace=\"$namespace\",responseCode=~\"2.*\"}[5m])) / sum(rate(occnp_diam_response_local_total{namespace=\"$namespace\"}[5m]))*100	Not Applicable	2xx

Copyright © 2019, 2026, Oracle and/or its affiliates.

A

Ingress Gateway Metrics

Ingress Gateway Metrics

Ingress Metrics Common Tags

Tags	Description	Possible Values
Method	Http method.	• GET • PUT • POST • DELETE • PATCH
NFType	Name of the NF Type.	For example: Path is /n**xxx-yyy**/v**z**/..... Where **XXX(Upper Case)** is NFType UNKNOWN if unable to extract NFType from the path
NFServiceType	Name of the Service with in the NF.	For example: Path is /n**xxx-yyy**/v**z**/..... Where nxxx-yyy is NFServiceType UNKNOWN if unable to extract NFServiceType from the path
Host	Port of ingress gateway (Ip or fqdn).	NA
HttpVersion	Http protocol version.	• HTTP/1.1 • HTTP/2.0
Scheme	Http protocol scheme.	HTTP, HTTPS, UNKNOWN
ClientCertIdentity	Certificate Identity of the client.	SAN=127.0.0.1,localhost CN=localhost, N/A if data is not available
Route_Path	Path predicate/Header predicate that matched the current request.	NA
InstanceIdentifier	Prefix of the pod configured in helm when there are multiple instances in same deployment.	Prefix configured in helm otherwise UNKNOWN
ErrorOriginator	This tag captures the ErrorOriginator.	ServiceProducer, Nrf, IngresGW, None
oc_ingressgateway_route_ratelimit_**Status** oc_ingressgateway_global_ratelimit_**Status**	Request accepted or dropped.	accepted, dropped
oc_ingressgateway_connection_failure_**Host**	Destination ip/fqdn.	NA
oc_ingressgateway_connection_failure_**Port**	Destination port.	NA

Copyright © 2019, 2026, Oracle and/or its affiliates.

Tags	Description	Possible Values
oc_ingressgateway_xfcc_header_validate_**Status**	Https Status value after performing xfccHeaderValidation at Ingress Gateway.	200 (OK), 400 (BAD_REQUEST)
oc_ingressgateway_xfcc_header_validate_**Cause**	This tag determines the validation cause for the xfcc header validation metric being pegged.	VALIDATION_FAILURE, VALIDATION_SUCCESS, HEADER_NOT_FOUND
oc_ingressgateway_xfcc_header_validate_**CertsCompared**	This tag captures the total number of certificates compared in XFCC header at ingress gateway during the header validation.	Count of the certificates compared (0,1,2..)
oc_configclient_request_total_**release Version**	This tag indicates the current release version of ingress gateway.	Picked from helm chart{{ .Chart.Version }}
oc_configclient_request_total_**configVersion**	This tag indicates the configuration version that ingress gateway is currently maintaining.	Initial value is 0. Incremental value received from config server whenever there is an update from config server (0, 1, 2...)
oc_configclient_response_total_**release Version**	This tag indicates the current release version of ingress gateway.	Picked from helm chart {{ .Chart.Version }}
oc_configclient_response_total_**configVersion**	This tag indicates the configuration version that ingress gateway is currently maintaining.	Value received from config server (1, 2...)
oc_configclient_response_total_**updated**	This tag indicates whether the configuration was updated or not.	true/false

Ingress Gateway Metrics

Table A-1 oc_ingressgateway_http_requests_total

Field	Details
Description	This metric is pegged as soon as the request reaches the Ingress gateway in the first custom filter of the application.
Type	Counter
Dimension	• NFType • NFServiceType • Host • HttpVersion • Scheme • Route_path • InstanceIdentifier • ClientCertIdentity

Table A-2 occnp_oc_ingressgateway_http_responses_total

Field	Details
Description	This metric is pegged in the last custom filter of the Ingress gateway while the response is being sent back to the consumer NF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table A-2 (Cont.) occnp_oc_ingressgateway_http_responses_total

Field	Details
Type	Counter
Dimension	• Status • Method • Route_path • NFType • NFServiceType • Host • HttpVersion • Scheme • Identifier • ClientCertIdentity

Table A-3 occnp_oc_ingressgateway_server_latency_seconds_bucket

Field	Details
Description	This metric is pegged in the last custom filter of the Ingress gateway while the response is being sent back to the consumer NF. This metric tracks the amount of time taken for processing the request. It starts as soon the request reaches the first custom filter of the application and lasts till the response is sent back to the consumer NF from the last custom filter of the application.
Type	Timer
Dimension	• quartile • InstanceIdentifier

Table A-4 oc_ingressgateway_connection_failure_total

Field	Details
Description	This metric is pegged in the customized Jetty Client as soon as it fails to connect to the destination service with direction as ingressOut. Here in case of Ingress gateway, the destination service is a backend microservice of the NF. And TLS connection failure metrics when connecting to ingress with direction as ingress.
Type	Counter
Dimension	• Host • Port • Direction • InstanceIdentifier • error_reason

Table A-5 oc_ingressgateway_global_ratelimit_total

Field	Details
Description	This metric is pegged in the custom filter implemented to check the global rate limit conditions.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table A-5 (Cont.) oc_ingressgateway_global_ratelimit_total

Field	Details
Dimension	• Method • Route_path • Scheme • InstanceIdentifier • Status (Rate limit Status field is different here)

Table A-6 oc_ingressgateway_route_ratelimit_total

Field	Details
Description	This metric is pegged in the custom filter implemented to check the route level rate limit conditions.
Type	Counter
Dimension	• Method • Route_path • Scheme • InstanceIdentifier • Status (Rate limit Status field is different here)

Table A-7 oc_ingressgateway_request_processing_latency_seconds

Field	Details
Description	This metric is pegged in the last custom filter of the Ingress gateway while the response is being sent back to the consumer NF. This metric captures the amount of time taken for processing of the request only within Ingress gateway. It starts as soon the request reaches the first custom filter of the application and lasts till the request is forwarded to the destination.
Type	Timer
Dimension	• quartile • InstanceIdentifier

Table A-8 oc_ingressgateway_jetty_request_stat_metrics_total

Field	Details
Description	This metric is pegged for every event occurred when a request is sent to IGW.
Type	Counter
Dimension	• event • client_type • InstanceIdentifier

Table A-9 oc_ingressgateway_jetty_response_stat_metrics_total

Field	Details
Description	This metric is pegged for every event occurred when a response is received by IGW
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table A-9 (Cont.) oc_ingressgateway_jetty_response_stat_metrics_total

Field	Details
Dimension	• event • client_type • InstanceIdentifier

Table A-10 oc_ingressgateway_jetty_latency_seconds

Field	Details
Description	This metric is pegged in Jetty response listener that captures the amount of time taken for processing of the request by jetty client.
Type	Timer
Dimension	• quartile • InstanceIdentifier

Table A-11 oc_ingressgateway_netty_latency_seconds

Field	Details
Description	This metric is pegged in Netty outbound handler that captures the amount of time taken for processing of the request by netty server.
Type	Timer
Dimension	• quartile • InstanceIdentifier

Table A-12 oc_ingressgateway_request_content_metrics_total

Field	Details
Description	This metric is pegged by default filter RequestContentMetrics. It pegs whether request has request body or not.
Type	Counter
Dimension	• method • content_available • InstanceIdentifier

Table A-13 oc_ingressgateway_xfcc_header_validate_total

Field	Details
Description	This metric is pegged when xfccHeaderValidation is enabled in XfccHeaderValidationFilter. This metric along with the specified dimension captures the successful/ un-successful validation of XFCC header in the incoming request.
Type	Counter

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table A-13 (Cont.) oc_ingressgateway_xfcc_header_validate_total

Field	Details
Dimension	• Route_path • Status • Cause • CertsCompared • InstanceIdentifier • ErrorOriginator

Table A-14 oc_configclient_request_total

Field	Details
Description	This metric is pegged whenever config client is polling for configuration update from common configuration server.
Type	Counter
Dimension	• Release version • Config version

Table A-15 oc_configclient_response_total

Field	Details
Description	This metrics is pegged whenever config client receives response from common configuration server.
Type	Counter
Dimension	• Release version • Config version • Updated

Oauth Metrics

OAuth Metrics Common Tags

Tags	Description	Possible Values
scope	NF service name(s) of the NF service producer(s), separated by white spaces.	NA
issuer	NF instance id of NRF.	NA
subject	NF instance id of service consumer.	NA
reason	reason contains the human readable message for oauth validation failure.	NA

Below are the metrics and their respective tags that are available in Oauth:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table A-16 oc_oauth_validation_successful _total

Field	Details
Description	This metric is pegged in the OAuth validator implementation if the received OAuth token is validated successfully. The implementation of OAuth validator is used in Ingress Gateway.
Type	Counter
Dimension	• issuer • subject • scope

Table A-17 oc_oauth_validation_failure _total

Field	Details
Description	This metric is pegged in the implementation of OAuth validator if the validation of the the received OAuth token fails. The implementation of OAuth validator is used in Ingress G;gateway.
Type	Counter
Dimension	• issuer • subject • scope • reason

Table A-18 oc_ingressgateway_msgcopy_requests_total

Field	Details
Description	This is incremented whenever ingress request message is sent or acknowledged from Kafka.
Type	Counter
Dimension	
Example	

Table A-19 oc_ingressgateway_msgcopy_responses_total

Field	Details
Description	This is incremented whenever ingress response message is sent or acknowledged from Kafka.
Type	Counter
Dimension	
Example	

Table A-20 oc_ingressgateway_incoming_ip_type

Field	Details
Description	Pegs IP address type of the active incoming connections from the client to Ingress Gateway.
Type	Gauge
Dimension	ReceivedAddressType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table A-20 (Cont.) oc_ingressgateway_incoming_ip_type

Field	Details
Example	oc_ingressgateway_incoming_ip_type{ReceivedAddressType="IPv4",} 0.0

Table A-21 oc_ingressgateway_outgoing_ip_type

Field	Details
Description	Pegs IP address type of the active outgoing connections from Ingress Gateway to the destination.
Type	Gauge
Dimension	DestinationHostAddressType
Example	oc_ingressgateway_outgoing_ip_type{DestinationHostAddressType="IPv6",} 4.0

Table A-22 oc_ingressgateway_incoming_connections

Field	Details
Description	Gauge metric that pegs active incoming connections from client to Ingress Gateway.
Type	Gauge
Dimension	• Direction • Host • InstanceIdentifier • scheme
Example	oc_ingressgateway_incoming_connections{Direction="ingress", Host="10.233.78.18", InstanceIdentifier="UNKNOWN_ingressgateway, scheme="https",} 1.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

B
Egress Gateway Metrics

Egress Gateway Metrics

The following table describes the Egress Gateway Metrics.

Table B-1 occnp_oc_egressgateway_http_requests_total

Field	Details
Available Tags	• Method • NFType • NFServiceType • HttpVersion • Scheme • Proxy • InstanceIdentifier
Pegging Instance	This metric is pegged as soon as the request reaches the Egress Gateway in the first custom filter of the application.

Table B-2 occnp_oc_egressgateway_http_responses_total

Field	Details
Available Tags	• Status • Method • NFType • NFServiceType • HttpVersion • Scheme • InstanceIdentifier • Direction • BlacklistedFqdn
Pegging Instance	This metric will be pegged in the last custom filter of the Egress gateway while the response is being sent back to backend NF microservice with direction as egress. This will also be pegged when the response is fetched in Jetty responseListener with direction as egressOut. BlacklistedFqdn tag will be filled with BlacklistedFqdn when request is sent with blacklisted producer.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-3 occnp_oc_egressgateway_server_latency_seconds_bucket

Field	Details
Available Tags	• quartile • InstanceIdentifier
Pegging Instance	This metric is pegged in the last custom filter of the Ingress Gateway while the response is being sent back to the consumer NF. This metric tracks the amount of time taken for processing the request. It starts as soon as the request reaches the first custom filter of the application and lasts till, the response is sent back to the consumer NF from the last custom filter of the application.

Table B-4 oc_egressgateway_connection_failure_total

Field	Details
Available Tags	• InstanceIdentifier • Direction
Pegging Instance	This metric will be pegged in the customized Jetty Client as soon as it fails to connect to the destination service. Here in case of Egress gateway, the destination service will be Producer NF. This will also be pegged when the request to Producer NF fails in Jetty request Listener with direction as egressOut

Table B-5 oc_egressgateway_notification_ratelimit_total

Field	Details
Available Tags	• Method • Scheme • InstanceIdentifier
Pegging Instance	This metric is pegged in the custom filter implemented to check the notification rate limit conditions.

Table B-6 oc_egressgateway_request_processing_latency_seconds

Field	Details
Available Tags	• quartile • InstanceIdentifier
Pegging Instance	This metric is pegged in the last custom filter of the Egress Gateway while the response is sent back to the consumer NF. This metric tracks the amount of time taken for processing the request only within Egress Gateway. It starts as soon as the request reaches the first custom filter of the application and lasts till the request is forwarded to the destination.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-7 oc_egressgateway_jetty_request_stat_metrics_total

Field	Details
Available Tags	• event • client_type • InstanceIdentifier
Pegging Instance	This metric is pegged for every event occurred when a request is sent to EGW

Table B-8 oc_egressgateway_jetty_response_stat_metrics_total

Field	Details
Available Tags	• event • client_type • InstanceIdentifier
Pegging Instance	This metric is pegged for every event occurred when a response is received by EGW

Table B-9 oc_egressgateway_jetty_response_stat_metrics_total

Field	Details
Available Tags	• event • client_type • InstanceIdentifier
Pegging Instance	This metric is pegged for every event occurred when a response is received by EGW

Table B-10 oc_egressgateway_jetty_latency_seconds

Field	Details
Available Tags	• quartile • InstanceIdentifier
Pegging Instance	This metric is pegged in Jetty response listener that captures the amount of time taken for processing of the request by jetty client

Table B-11 oc_egressgateway_jetty_latency_seconds

Field	Details
Available Tags	• quartile • InstanceIdentifier
Pegging Instance	This metric is pegged in Jetty response listener that captures the amount of time taken for processing of the request by jetty client

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-12 oc_egressgateway_netty_latency_seconds

Field	Details
Available Tags	• quartile • InstanceIdentifier
Pegging Instance	This metric is pegged in Netty outbound handler that captures the amount of time taken for processing of the request by netty server

Table B-13 oc_egressgateway_request_content_metrics_total

Field	Details
Available Tags	• method • content_available • InstanceIdentifier
Pegging Instance	This metric is pegged by default filter RequestContentMetrics. It pegs whether request has request body or not and the method.

Table B-14 oc_egressgateway_blacklisted_producer_total

Field	Details
Available Tags	• NFType • NFServiceType • InstanceIdentifier • Host • Route_path
Pegging Instance	This metric is a counter. Track number of times producer is blacklisted.

Table B-15 oc_configclient_request_total

Field	Details
Available Tags	• Release version • Config version
Pegging Instance	This metric will be pegged whenever config client is polling for configuration update from common configuration server

Table B-16 oc_configclient_response_total

Field	Details
Available Tags	• Release version • Config version • Updated
Pegging Instance	This metrics will be pegged whenever config client receives response from common configuration server

Copyright © 2019, 2026, Oracle and/or its affiliates.

Egress Gateway Metrics Common Tags

The following table describes the common tags used in Egress Gateway Metrics.

Table B-17 Method

Field	Details
Available Tags	Http method
Pegging Instance	GET, PUT, POST, DELETE, PATCH

Table B-18 NFType

Field	Details
Available Tags	Name of the NF Type
Pegging Instance	"UNKNOWN" (Updates are available when Ingress is 5G aware)

Table B-19 NFServiceType

Field	Details
Available Tags	Name of the Service within the NF
Pegging Instance	"UNKNOWN" (Updates are available when Ingress is 5G aware)

Table B-20 Host

Field	Details
Available Tags	(IP or fqdn): port of ingress gateway
Pegging Instance	Not Applicable

Table B-21 HttpVersion

Field	Details
Available Tags	Http protocol version (http1.1/ http2)
Pegging Instance	HTTP1.1, HTTP2.0

Table B-22 Scheme

Field	Details
Available Tags	Http protocol scheme (http/https)
Pegging Instance	HTTP, HTTPS, UNKNOWN

Table B-23 Proxy

Field	Details
Available Tags	Value received for "x-custom-egress-proxy-header".

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-23 (Cont.) Proxy

Field	Details
Pegging Instance	Unknown or value of "x-custom-egress-proxy-header".

Table B-24 oc_egressgateway_connection_failure_Host

Field	Details
Available Tags	destination ip/fqdn
Pegging Instance	Not Applicable

Table B-25 oc_egressgateway_connection_failure_Port

Field	Details
Available Tags	destination port
Pegging Instance	Not Applicable

Table B-26 BlacklistedFqdn

Field	Details
Available Tags	Blacklisted Producer Fqdn
Pegging Instance	Unknown or Blacklisted Producer Fqdn

Table B-27 oc_configclient_request_total_release Version

Field	Details
Available Tags	This tag indicates the current release version of egress gateway
Pegging Instance	Picked from helm chart{{ .Chart.Version }}

Table B-28 oc_configclient_request_total_configVersion

Field	Details
Available Tags	This tag indicates the configuration version that egress gateway is currently maintaining
Pegging Instance	Initial value is 0. Incremental value received from config server whenever there is an update from config server (0, 1, 2...)

Table B-29 oc_configclient_response_total_release Version

Field	Details
Available Tags	This tag indicates the current release version of egress gateway
Pegging Instance	Picked from helm chart{{ .Chart.Version }}

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-30 oc_configclient_response_total_configVersion

Field	Details
Available Tags	This tag indicates the configuration version that egress gateway is currently maintaining
Pegging Instance	Value received from config server (1, 2...)

Table B-31 oc_configclient_response_total_updated

Field	Details
Available Tags	This tag indicates whether the configuration was updated or not
Pegging Instance	true/false

SCP Metrics

The following table describes the different metrics and their respective tags that are available in the SCP Module:

> **Note**
>
> The actual names of these metrics may vary based on the configured metricPrefix and metricSuffix. For example, if the configured metricPrefix is `occnp_`, the prefix must be added to the metric name.

Table B-32 oc_egressgateway_sbiRouting_http_requests_total

Field	Details
Available Tags	• Scp_Fqdn • Reroute_Path • Attempt • HttpVersion • Scheme • InstanceIdentifier
Pegging Instance	This metric will be pegged when SBIRouting feature is enabled for a route to which request is sent to EGW

Table B-33 oc_egressgateway_sbiRouting_http_responses_total

Field	Details
Available Tags	• Scp_Fqdn • Reroute_Path • Status • Attempt • HttpVersion • Scheme • InstanceIdentifier • ErrorOriginator

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-33 (Cont.) oc_egressgateway_sbiRouting_http_responses_total

Field	Details
Pegging Instance	This metric is pegged only when SBIRouting feature is enabled for a route to which request is sent to EGW and reroute mechanism is executed.

Table B-34 oc_egressgateway_sbiRouting_request_distribution

Field	Details
Available Tags	• request_distribution_type:<Priority_Based/ Weight_Based> • oc_alternateroute_attempt:<oc_alternateroute _attempt>
Pegging Instance	For every request, this metric should be pegged to depict whether request would follow RFC(weight-based) or it will go through priority based routing.

Table B-35 oc_egressgateway_sbiRouting_weightBased_distribution

Field	Details
Available Tags	• virtual_Fqdn:<virtual_Fqdn> • host:<host> • port:<port>
Pegging Instance	This metric will be pegged to show the distribution of traffic on virtual fqdn only when weight-based-algorithm is applied.

Table B-36 oc_egressgateway_sbiRouting_http_error_responses_total

Field	Details
Available Tags	• statusCode • InstanceIdentifier • authority • targetDestination
Pegging Instance	This metric will be pegged to show the number of error responses received by egress gateway.

Table B-37 oc_egressgateway_sbiRouting_retry

Field	Details
Available Tags	• attempt • retryStatusCode • retryReason • InstanceIdentifier • authority • targetDestination
Pegging Instance	This metric will be pegged to show the number of retry made out of egress gateway.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-38 oc_egressgateway_sbiRouting_reroute

Field	Details
Available Tags	• attempt • rerouteStatusCode • InstanceIdentifier • authority • targetDestination
Pegging Instance	This metric will be pegged to show the number of re-route made out of egress gateway.

Table B-39 oc_egressgateway_sbiRouting_response_body_fetch

Field	Details
Available Tags	NA
Pegging Instance	This metric will be pegged to show the number of times EGW had to block and fetch the response payload.

Table B-40 occnp_oc_egressgateway_sbiRouting_cause_based_validation_success_total

Field	Details
Available Tags	NA
Pegging Instance	This metric will be pegged to show the number of times the cause-based validation was successful.

Table B-41 occnp_oc_egressgateway_sbiRouting_cause_based_validation_failure_total

Field	Details
Available Tags	• cause
Pegging Instance	This metric will be pegged to show the number of times the cause-based validation failed.

Table B-42 occnp_oc_egressgateway_sbiRouting_attempts_to_fulfill_request

Field	Details
Available Tags	NA
Pegging Instance	This metrics will be pegged to show the number of attempts taken to fulfill a request.

SCP Metrics common tags

The following table describes common tags used in SCP Metrics.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-43 Scp_Fqdn

Field	Details
Description	SCP Fqdn
Possible Values	Not Applicable

Table B-44 Reroute_Path

Field	Details
Description	Path that matched the request to over corresponding route Example: `/nef/**`
Possible Values	Not Applicable

Table B-45 Status

Field	Details
Description	Sbi peer response status code.
Possible Values	200 OK

Table B-46 Attempt

Field	Details
Description	Attempt number for scp re-route. Example: 1, 2 etc.
Possible Values	Not Applicable

Table B-47 HttpVersion

Field	Details
Description	Http protocol version (http1.1/ http2)
Possible Values	HTTP/1.1, HTTP/2.0

Table B-48 Scheme

Field	Details
Description	Http protocol scheme (http/https)
Possible Values	HTTP, HTTPS, UNKNOWN

Table B-49 InstanceIdentifier

Field	Details
Description	Prefix of the pod configured in helm when there are multiple instances in same deployment
Possible Values	Prefix configured in helm otherwise UNKNOWN

Copyright © 2019, 2026, Oracle and/or its affiliates.

Oauth Metrics

The following table includes metrics and their respective tags that are available in the Oauth Module:

Table B-50 oc_oauth_nrf_request_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope • NrfFqdn
Pegging Instance	This metric is pegged in the OAuth client implementation if the request is sent to NRF for requesting the OAuth token. OAuth client implementation will be used in Egress gateway.

Table B-51 oc_oauth_nrf_response_success_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope • StatusCode • NrfFqdn
Pegging Instance	This metric is pegged in the OAuth client implementation if an OAuth token is successfully received from the NRF. OAuth client implementation is used in the Egress Gateway.

Table B-52 oc_oauth_nrf_response_failure_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope • StatusCode • ErrorOriginator • NrfFqdn
Pegging Instance	This metric is pegged in the OAuthClientFilter in Egress Gateway whenever GetAccessTokenFailedException is caught.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-53 oc_oauth_request_failed_internal_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope • StatusCode • ErrorOriginator • NrfFqdn
Pegging Instance	This metric is pegged in the OAuthClientFilter in Egress Gateway whenever InternalServerErrorException is caught.

Table B-54 oc_oauth_token_cache_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope
Pegging Instance	This metric is pegged in the OAuth Client Implementation if the OAuth token is found in the cache.

Table B-55 oc_oauth_request_invalid_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope • StatusCode • ErrorOriginator
Pegging Instance	This metric is pegged in the OAuthClientFilter in Egress Gateway whenever a BadAccessTokenRequestException/ JsonProcessingException is caught.

Table B-56 oc_egressgateway_ouath_access_token_request_header_missing

Field	Details
Available Tags	NA
Pegging Instance	This metric is pegged in the OAuthClientFilter in Egress Gateway whenever oc-access-token-request-info header is missing in the request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-57 oc_oauth_cert_expiryStatus

Field	Details
Available Tags	• id • certificateName • secretName
Pegging Instance	This Gauge metric is used to peg expiry date of the certificate. This metric is further used for raising alarms if certificate expires within 30 days or 7 days.

Table B-58 oc_oauth_cert_loadStatus

Field	Details
Available Tags	• id • certificateName • secretName
Pegging Instance	This gauge metric is used to peg expiry date of the certificate. This metric is further used for raising alarms if certificate expires within 30 days or 7 days.

Table B-59 oc_oauth_request_failed_cert_expiry

Field	Details
Available Tags	• target nf type • target nf instance id • consumer nf instance id • nrf instance id • service name of nf producer service • key id
Pegging Instance	This counter metric is used to keep track of number of requests with keyId in token that failed due to certificate expiry. It is pegged whenever oAuth Validator module throws oauth custom exception due to certificate expiry for an incoming request.

Table B-60 oc_oauth_keyid_count_total

Field	Details
Available Tags	• target nf type • target nf instance id • consumer nf instance id • nrf instance id • service name of nf producer service • key id
Pegging Instance	This counter metric used to keep track of number of requests received with keyId in token. It is pegged whenever a request with an access token containing keyid in header comes to oAuth Validator.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-61 oc_oauth_nrf_token_retrieval_failure_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope • StatusCode • ErrorOriginator • ErrorDetail • NrfFqdn
Pegging Instance	This metric is pegged to track requests discarded due to oAuth token retrieval failure from NRF.

OAuth Metrics (NRF-Client Mgmt Service Call-Flow)

Table B-62 oc_oauth_nrf_client_subscription_request_total

Field	Details
Available Tags	• NrfClientUrl • EgwNotificationUrl
When it is pegged	This metric will be pegged in the OAuth client implementation module when a subscription request is sent from EGW to NRF-Client Mgmt Svc with request-URL (NrfClientUrl) and request body containing notification-URL of EGW (EgwNotificationUrl) for Oauth Client notification requests generated from NRF-Client Mgmt Svc to EGW. OAuth client implementation will be used in Egress gateway.

Table B-63 oc_oauth_nrf_client_notification_request_total

Field	Details
Available Tags	None
When it is pegged	This metric will be pegged in the OAuth client implementation module when a notification request is sent from NRF-Client Mgmt Svc to EGW.OAuth client implementation will be used in Egress gateway.

Table B-64 oc_oauth_nrf_client_subscription_response_total

Field	Details
Available Tags	• NrfClientUrl • EgwNotificationUrl • StatusCode

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-64 (Cont.) oc_oauth_nrf_client_subscription_response_total

Field	Details
When it is pegged	This metric will be pegged in the OAuth client implementation module when a subscription response is sent from NRF-Client Mgmt Svc having URL (NrfClientUrl) to EGW having URL (EgwNotificationUrl). StatusCode tag will capture the corresponding response status obtained from NRF-Client. OAuth client implementation will be used in Egress gateway.

Table B-65 oc_oauth_nrf_client_notification_response_total

Field	Details
Available Tags	• StatusCode
When it is pegged	This metric will be pegged in the OAuth client implementation module when a notification response is sent from EGW to NRF-Client Mgmt Svc.StatusCode tag will capture the corresponding response status sent From EGW. OAuth client implementation will be used in Egress gateway.

Table B-66 oc_oauth_nrf_client_active_nrf_instances

Field	Details
Available Tags	• NrfFqdn
When it is pegged	This is a GAUGE metric which keeps track of healthy NRF Fqdns received from NRF-Client Mgmt Svc as part of subscription response/ notification request to EGW.

OAuth Metrics common tags

The following table describes common tags used in the OAuth Module.

Table B-67 ConsumerNFInstanceId

Field	Details
Description	NF instance id of the NF service consumer
Possible Values	Not Applicable

Table B-68 ConsumerNFType

Field	Details
Description	The NF type of the NF service consumer

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-68 (Cont.) ConsumerNFType

Field	Details
Possible Values	NRF, UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC,5G_EIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF

Table B-69 TargetNFType

Field	Details
Description	The NF type of the NF service producer
Possible Values	NRF, UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC,5G_EIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF

Table B-70 TargetNFInstanceId

Field	Details
Description	NF instance id of the NF service producer
Possible Values	Not Applicable

Table B-71 scope

Field	Details
Description	NF service name(s) of the NF service producer(s), separated by white spaces
Possible Values	Not Applicable

Table B-72 StatusCode

Field	Details
Description	Status code of NRF access token request
Possible Values	Bad Request, Internal Server Error etc. (HttpStatus.*)

Table B-73 ErrorOriginator

Field	Details
Description	from where error is originated (nrf or egress)
Possible Values	Nrf, Egress GW

Table B-74 issuer

Field	Details
Description	NF instance id of NRF
Possible Values	Not Applicable

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-75 subject

Field	Details
Description	NF instance id of service consumer
Possible Values	Not Applicable

Table B-76 reason

Field	Details
Description	reason contains the human readable message for oauth validation failure
Possible Values	Not Applicable

Table B-77 NrfFqdn

Field	Details
Description	NrfFqdn tag determines the corresponding fqdn of NRF where the request has been forwarded to.
Possible Values	Nrf-Fqdn (dynamic value based on Fqdn), NA

Table B-78 NrfClientUrl

Field	Details
Description	This tag determines the url of NRF-Client Mgmt Svc where subscription requests are sent from OAuth Client module in EGW.
Possible Values	URL of NRF-Client Mgmt Svc (Dynamic value)

Table B-79 EgwNotificationUrl

Field	Details
Description	This tag determines the notification URL mapped in OAuth Client module of EGW where NRF-Client Mgmt Svc will send notifications requests.
Possible Values	Notification URL (Dynamic value)

Table B-80 Configuration Type

Field	Details
Description	This tag determines the type of configuration in place for OAuth Client in Egress Gateway. If nrfClientQueryEnabled Helm parameter in oauthClient Helm configurations at Egress Gateway is false then the ConfigurationType is STATIC, else DYNAMIC.
Possible Values	STATIC, DYNAMIC

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-81 oc_egressgateway_msgcopy_requests_total

Field	Details
Description	This is incremented whenever egress request message is sent or acknowledged from Kafka.
Type	Counter
Dimension	
Example	

Table B-82 oc_egressgateway_msgcopy_responses_total

Field	Details
Description	This is incremented whenever egress response message is sent or acknowledged from Kafka.
Type	Counter
Dimension	
Example	

Table B-83 oc_egressgateway_incoming_ip_type

Field	Details
Description	Pegs IP address type of the active incoming connections from the client to Egress Gateway.
Type	Gauge
Dimension	ReceivedAddressType
Example	oc_egressgateway_incoming_ip_type{ReceivedAddressType="IPv6",} 4.0

Table B-84 oc_egressgateway_outgoing_ip_type

Field	Details
Description	Pegs IP address type of the active outgoing connections from Egress Gateway to the destination.
Type	Gauge
Dimension	DestinationHostAddressType
Example	oc_egressgateway_outgoing_ip_type{DestinationHostAddressType="IPv6",} 4.0

Table B-85 oc_egressgateway_dualstack_ip_rejected_total

Field	Details
Description	Counts the total number of IP address rejections because the IP address type configured in the egressRoutingMode does not match the IP address type returned by DNS resolution.
Type	Counter
Dimension	• service • egressRoutingMode • dnsRecivedIpType

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table B-85 (Cont.) oc_egressgateway_dualstack_ip_rejected_total

Field	Details
Example	oc_egressgateway_dualstack_ip_rejected_total{"service":"nrf-svc1", "egressRoutingMode":"IPv6", "dnsRecivedIpType":"IPv4"} 10.0 oc_egressgateway_dualstack_ip_rejected_total{"service":"pcf-svc1", "egressRoutingMode":"IPv4", "dnsRecivedIpType":"IPv6"} 5.0

Copyright © 2019, 2026, Oracle and/or its affiliates.

C

HTTP Error Codes Supported by Policy

HTTP Error Codes supported for Policy as a consumer of AMF - UE Policy

Policy as a consumer of AMF - UE Policy

Table C-1 Policy as a consumer of AMF - UE Policy.

Error Code-Message	Cause Code	Description
307 Temporary Redirect	NF_CONSUMER_REDIRECT_ONE_TXN	The request is redirected to a specified target.
403 Forbidden	HANDOVER_FAILURE	UE context creation in the target AMF fails during the handover procedure.
403 Forbidden	INTEGRITY_CHECK_FAIL	The integrity check of the complete registration message in the UE context transfer request fails.
403 Forbidden	EBI_EXHAUSTED	EPS Bearer ID allocation fails due to exhaustion of EBI because the UE has already been allocated the maximum number of EBIs.
403 Forbidden	EBI_REJECTED_LOCAL_POLICY	EPS Bearer ID allocation fails because of local policy at the AMF, as specified in clause 4.11.1.4.1 of 3GPP TS 23.502 [3].
403 Forbidden	EBI_REJECTED_NO_N26	EPS Bearer ID allocation is rejected when the AMF is in a serving PLMN that does not support 5GS-EPS interworking procedures over the N26 interface.
403 Forbidden	SUPI_OR_PEI_UNKNOWN	The SUPI or PEI included in the message is unknown.
403 Forbidden	UE_IN_NON_ALLOWED_AREA	The UE is in a non-allowed area. Therefore, the N1/N2 message transfer cannot be completed because the request is not associated with a regulatory prioritized service.
403 Forbidden	UNSPECIFIED	The request is rejected for unspecified reasons.
403 Forbidden	SM_CONTEXT_RELOCATION_REQUIRED	The request is rejected because the SM context must be relocated to another SMF. For example, the AMF detects that I-SMF or V-SMF insertion, change, or removal is required, as specified in clause 4.23 of 3GPP TS 23.502 [3].
403 Forbidden	UE_WITHOUT_N1_LPP_SUPPORT	The UE does not support LPP in N1 mode. Therefore, the N1 LPP message cannot be sent to the UE.
404 Not Found	CONTEXT_NOT_FOUND	The requested UE context does not exist on the AMF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-1 (Cont.) Policy as a consumer of AMF - UE Policy.

Error Code-Message	Cause Code	Description
409 Conflict	HIGHER_PRIORITY_REQUEST_ONGOING	Paging-triggered N1/N2 transfer cannot be initiated because paging is already in progress for a higher-priority session.
409 Conflict	TEMPORARY_REJECT_REGISTRATION_ONGOING	N1/N2 message transfer to the UE or AN cannot be initiated, or EBI assignment fails, because a registration procedure is in progress.
409 Conflict	TEMPORARY_REJECT_HANDOVER_ONGOING	N1/N2 message transfer to the UE or AN cannot be initiated because an Xn or N2 handover procedure is in progress, or EBI assignment fails because an N2 handover procedure is in progress.
409 Conflict	UE_IN_CM_IDLE_STATE	N2 message transfer to the 5G-AN cannot be initiated because the UE is in the CM-IDLE state for the access network type associated with the PDU session.
409 Conflict	MAX_ACTIVE_SESSIONS_EXCEEDED	The RAT type is NB-IoT, and the UE already has two PDU sessions with active user plane resources.
409 Conflict	REJECTION_DUE_TO_PAGING_RESTRICTION	Paging Restrictions information restricts the N1N2MessageTransfer request from causing paging, as defined in 3GPP TS 23.501 [2], clause 5.38.5.
504 Gateway Timeout	UE_NOT_REACHABLE	The UE is not reachable for paging.

HTTP Error Codes supported by Policy for AM, SM, and UE Interfaces

Table C-2 HTTP Error codes and cause supported by Policy for AM, SM, and UE Interfaces for Notification

Error Code-Message	Cause Code	Description	Action
400 - Bad requests	INVALID_MSG_FORMAT	The HTTP request has an invalid format.	• POST retry with POST request • If retry is exhausted, then terminate the transaction.
400 - Bad requests	INVALID_QUERY_PARAM	The HTTP request contains an unsupported query parameter in the URI.	`invalidParams` attribute is included in the `ProblemDetails`data structure indicating unsupported.
400 - Bad requests	MANDATORY_IE_INCORRECT	A mandatory IE for an HTTP method received a semantically incorrect request.	• POST retry with POST request • If retry is exhausted, then terminate the transaction.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-2 (Cont.) HTTP Error codes and cause supported by Policy for AM, SM, and UE Interfaces for Notification

Error Code-Message	Cause Code	Description	Action
400 - Bad requests	MANDATORY_QUERY_PARAM_INCORRECT	A mandatory query parameter, or a conditional query parameter, but mandatory required for an HTTP method was received in the URI with semantically incorrect value.	
400 - Bad requests	OPTIONAL_QUERY_PARAM_INCORRECT	An optional query parameter for an HTTP method was received in the URI with asemantically incorrect value that prevents successful processing of the service request.	
400 - Bad requests	MANDATORY_QUERY_PARAM_MISSING	Query parameter which is defined as mandatory, or as conditional but mandatory required for a HTTP method is not included in the URI of the request.	
400 - Bad requests	MANDATORY_IE_MISSING	A mandatory IE for an HTTP method is not included in the request.	• POST retry with POST request • If retry is exhausted, then terminate the transaction.
400 - Bad requests	UNSPECIFIED_MSG_FAILURE	The request is rejected due to unspecified client error.	• POST retry with POST request • If retry is exhausted, then terminate the transaction.
400 - Bad requests	ERROR_REQUEST_PARAMETERS	The HTTP request is rejected because the set of information needed by the PCF for UE Policy selection is incomplete for the decision to be made.	• POST retry with POST request • If retry is exhausted, then terminate the transaction.
400 - Bad requests	OPTIONAL_IE_INCORRECT	An optional IE for a HTTP method was received with a semantically incorrect value that prevents successful processing of the service request.	
400 - Bad requests	USER_UNKNOWN	The HTTP request is rejected because either the end user specified in the request is unknown to the PCF or when a error occurs in PCF and the validate User flag is set as `true`.	

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-2 (Cont.) HTTP Error codes and cause supported by Policy for AM, SM, and UE Interfaces for Notification

Error Code-Message	Cause Code	Description	Action
401-Unauthorized	With header "WWW-Authenticate"	There will be a new function to enable retry for this error code.	• POST retry with POST request • If retry is exhausted, terminate the transaction
403-Forbidden	MODIFICATION_NOT_ALLOWED	The request is rejected because modification is not allowed.	• POST retry with POST request • If retry is exhausted, terminate the transaction
404 - Not Found	SUBSCRIPTION_NOT_FOUND	The request for modification or deletion of subscription is rejected because the subscription is not found in the NF.	• POST retry with POST request • If retry is exhausted, delete the session
404 - Not Found	RESOURCE_URI_STRUCTURE_NOT_FOUND	The request is rejected because a fixed part after the first variable part of an "apiSpecificResourceUriPart" is not found in the NF.	• POST retry with POST request • If retry is exhausted, delete the session
405 - Method Not Allowed	NA	If the NF supports the HTTP method for several resources in the API, but not for the target resource of a given HTTP request	• POST retry with POST request • If retry is exhausted, terminate the transaction
406 - Not Acceptable	NA	The server cannot generate a response in a format specified as acceptable by the client in the "Accept" headers.	• POST retry with POST request • If retry is exhausted, terminate the transaction
408 - Request Timeout	NA	The server did not receive a complete request from the client within the expected time frame.	• POST retry with POST request • If retry is exhausted, terminate the transaction
409 - Conflict	NA	The server did not receive a complete request from the client within the expected time frame.	• POST retry with POST request • If retry is exhausted, terminate the transaction
410 - Gone	NA	The server did not receive a complete request from the client within the expected time frame.	• POST retry with POST request • If retry is exhausted, terminate the transaction
411 - Length Required	INCORRECT_LENGTH	The request is rejected due to incorrect value of a Content-length header field.	• POST retry with POST request • If retry is exhausted, terminate the transaction

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-2 (Cont.) HTTP Error codes and cause supported by Policy for AM, SM, and UE Interfaces for Notification

Error Code-Message	Cause Code	Description	Action
412 - Precondition Failed	NA	One or more preconditions specified in the request headers were not met.	• POST retry with POST request • If retry is exhausted, terminate the transaction
413 - Payload Too Large	NA	The server refuses to process the request because the payload size exceeds its limitations.	• POST retry with POST request • If retry is exhausted, terminate the transaction
414 - URI Too Long	NA	The server cannot process the request because the provided URI exceeds its maximum length limit.	• POST retry with POST request • If retry is exhausted, terminate the transaction
415 - Unsupported Media Type	NA	The server cannot process the request due to an unsupported media type in the request payload.	• POST retry with POST request • If retry is exhausted, terminate the transaction
429 - Too Many Requests	NF_CONGESTION_RISK	The request is rejected due to excessive traffic which, if continued over time, may lead to (or may increase) an overload situation.	• POST retry with POST request • If retry is exhausted, terminate the transaction
500 -Internal Server Error	INSUFFICIENT_RESOURCES	The request is rejected due to insufficient resources.	• POST retry with POST request • If retry is exhausted, terminate the transaction
500 - Internal Server Error	UNSPECIFIED_NF_FAILURE	The request is rejected due to unspecified reason at the NF.	• POST retry with POST request • If retry is exhausted, terminate the transaction
500 - Internal Server Error	SYSTEM_FAILURE	The request is rejected due to generic error condition in the NF.	• POST retry with POST request • If retry is exhausted, terminate the transaction
500 -Internal Server Error	NF_FAILOVER	The request is rejected due to generic error condition in the NF.	• POST retry with POST request • If retry is exhausted, terminate the transaction
503 - Server temporarily unavailable	NF_CONGESTION	The NF experiences congestion and performs overload control, which does not allow the request to be processed.	• POST retry with POST request • If retry is exhausted, terminate the transaction

Copyright © 2019, 2026, Oracle and/or its affiliates.

Policy as a producer of Error to AM Interface

Table C-3 Policy as a producer of Error to AM Interface

Message	Cause Code	Description
400 - Bad request	MANDATORY_IE_INCORRECT	When the SUPI was incorrectly written into the request body and sent to Ingress.
400 - Bad request	MANDATORY_IE_MISSING	When a request is sent without a mandatory IE (SUPI) in the request body.
400 - Bad request	UNSPECIFIED_MSG_FAILURE	When there is malformed JSON object.
400 - Bad request	USER_UNKNOWN	A correct request is sent with a SUPI that is not registered in the UDR. The validate-user in the CNC Console of the UE Policy is activated.
400 - Bad request	ERROR_REQUEST_PARAMETERS	When there is malformed JSON object.
400 - Bad request	PENDING_TRANSACTION	In case of Pending transaction.
401 - Unauthorized	With header "WWW-Authenticate"	Supported by Gateway service.
403 - Forbidden	MODIFICATION_NOT_ALLOWED	Supported by Gateway service.
404 - Not Found	SUBSCRIPTION_NOT_FOUND	When UE-Delete is sent with a polAssoId that does not exist in the database.
404 - Not Found	RESOURCE_URI_STRUCTURE_NOT_FOUND	When resource URI structure is not found.
408 - Request Timeout	NA	Supported by Gateway service.
411 - Length Required	INCORRECT_LENGTH	Incorrect length.
429 - Too Many Requests	NF_CONGESTION_RISK	When there is congestion risk in the NF.
500 - Internal Server Error	UNSPECIFIED_NF_FAILURE	When an unexpected error occurs within the service.
503 - Service Unavailable	NF_CONGESTION	Supported by Gateway service.

Policy as a producer of Error to SM

Table C-4 Policy as a producer of Error to SM

Message	Cause Code	Description
400 - Bad request	MANDATORY_IE_MISSING	A request is sent without a mandatory IE (SUPI) in the request body.
400 - Bad request	UNSPECIFIED_MSG_FAILURE	malformed json object.
400 - Bad request	USER_UNKNOWN	A correct request is sent, with a SUPI that is not registered in the UDR. We activate the validate-user in the UE Policy GUI.
400 - Bad request	ERROR_INITIAL_PARAMETERS	A request is sent with an error in one or more of its parameters

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-4 (Cont.) Policy as a producer of Error to SM

Message	Cause Code	Description
400 - Bad request	PENDING_TRANSACTION	This error shall be used when the PendingTransaction feature is supported and the AMF receives an incoming request on a policy association while it has an ongoing transaction on the same policy association.
401- Unauthorized	With header "WWW-Authenticate"	Supported by Gateway service.
403 - Forbidden	MODIFICATION_NOT_ALLOWED	Supported by Gateway service.
403 - Forbidden	POLICY_CONTEXT_DENIED	When an error occurs in PRE service.
403 - Forbidden	LATE_OVERLAPPING_REQUEST	The request is rejected because it collides with an existing SM context or PDU session context with a more recent origination timestamp.
404 - Not Found	SUBSCRIPTION_NOT_FOUND	When UE-Delete is sent with a polAssoId that does not exist in the database.
404 - Not Found	RESOURCE_URI_STRUCTURE_NOT_FOUND	This error is being handled by IGW, never reaches the core service, send 404 Not Found without cause.
408 - Request Timeout	NA	Supported by Gateway service.
411 - Length Required	INCORRECT_LENGTH	The error cause will be changed to ERROR_REQUEST_PARAMETERS.
429 - Too Many Requests	NF_CONGESTION_RISK	This will be supported with IGW congestion control and load shedding profiles.
500 - Internal Server Error	UNSPECIFIED_NF_FAILURE	The request is rejected due to unspecified reason at the NF.
503 - Service Unavailable	NF_CONGESTION	Supported by Gateway service.

Table C-5 List of errors sent by SM service for AF 5G

Message	Cause Code	Description
500 Internal Server Error	PDU_SESSION_NOT_AVAILABLE	The PCRF rejects a new Rx session setup when it fails to associate the described service. IP flows within the session information received from the AF to an existing IP-CAN session.
400 Bad Request	ERROR_INITIAL_PARAMETERS	This error is used when the set of bearer/session information needed in the CRF for rule selection is incomplete or erroneous for the decision to be made. For example, QoS, AGW/SGSN address, RAT type, and TFT.
404 Not Found	APPLICATION_SESSION_CONTEXT_NOT_FOUND	The request contained an unknown Session-Id.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-5 (Cont.) List of errors sent by SM service for AF 5G

Message	Cause Code	Description
403 Forbidden	REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED	The PCRF rejects new or modified service information because the requested service, as described by the service information provided by the AF, is not consistent with either the related subscription information or operator defined policy rules.
403 Forbidden	UNAUTHORIZED_NON_EMERGENCY_SESSION	The PCRF rejects a new Rx session setup because the session binding function associated a non-Emergency IMS session to an IP-CAN session established to an Emergency APN.

Policy as a producer of Error to UE

Table C-6 Policy as a producer of Error to UE

Message	Cause Code	Description
400 - Bad request	MANDATORY_IE_INCORRECT	The SUPI was incorrectly written into the request body and sent to Ingress.
400 - Bad request	MANDATORY_IE_MISSING	A request is sent without a mandatory IE (SUPI) in the request body,the cases that are related to this cause will be handled asERROR_REQUEST_PARAMETERS.
400 - Bad request	UNSPECIFIED_MSG_FAILURE	When there is malformed JSON object.
400 - Bad request	USER_UNKNOWN	A correct request is sent, with a SUPI that is not registered in the UDR. We activate the validate-user in the UE Policy GUI.
400 - Bad request	ERROR_REQUEST_PARAMETERS	The HTTP request is rejected because the set of information needed by the PCF for UE Policy selection is incomplete or erroneous or not available for the decision to be made.
400 - Bad request	PENDING_TRANSACTION	This error shall be used when the Pending Transaction feature is supported and the AMF receives an incoming request on a policy association while it has an ongoing transaction on the same policy association.
401 - Unauthorized	With header "WWW-Authenticate"	Supported by Gateway service.
403 - Forbidden	MODIFICATION_NOT_ALLOWED	Supported by Gateway service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-6 (Cont.) Policy as a producer of Error to UE

Message	Cause Code	Description
404 - Not Found	SUBSCRIPTION_NOT_FOUND	When UE-Delete is sent with a polAssoId that does not exist in the database.
404 - Not Found	RESOURCE_URI_STRUCTURE_NOT_FOUND	This error is being handled by IGW, never reaches the core service, send 404 Not Found without cause.
408 - Request Timeout	NA	Request gets timed out.
411 - Length Required	INCORRECT_LENGTH	The error cause will be changed to ERROR_REQUEST_PARAMETERS.
429 - Too Many Requests	NF_CONGESTION_RISK	This will be supported with IGW congestion control and load shedding profiles.
500 - Internal Server Error	UNSPECIFIED_NF_FAILURE	The request is rejected due to unspecified reason at the NF.
503 - Service Unavailable	NF_CONGESTION	Supported by Gateway service.

HTTP Error Codes supported by Policy for CHF and UDR Interfaces

Table C-7 Error codes and cause supported by Policy for CHF Interface

Message	Cause Code	Description	Actions
400 - Bad Request	INVALID_API	The HTTP request contains an unsupported API name or API version in the URI.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	INVALID_MSG_FORMAT	The HTTP request has an invalid format.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-7 (Cont.) Error codes and cause supported by Policy for CHF Interface

Message	Cause Code	Description	Actions
400 - Bad Request	INVALID_QUERY_PARAM	The HTTP request contains an unsupported query parameter in the URI.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	MANDATORY_QUERY_PARAM_INCORRECT	A mandatory query parameter, or a conditional query parameter but mandatory required, for an HTTP method was received in the URI with semantically incorrect value.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	OPTIONAL_QUERY_PARAM_INCORRECT	A mandatory query parameter, or a conditional query parameter but mandatory required, for an HTTP method was received in the URI with semantically incorrect value.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	MANDATORY_QUERY_PARAM_MISSING	Query parameter which is defined as mandatory, or as conditional but mandatory required, for an HTTP method is not included in the URI of the request.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	MANDATORY_IE_INCORRECT	A mandatory IE or conditional IE but mandatory required, for an HTTP method was received with a semantically incorrect.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-7 (Cont.) Error codes and cause supported by Policy for CHF Interface

Message	Cause Code	Description	Actions
400 - Bad Request	OPTIONAL_IE_INCORRECT	-	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	MANDATORY_IE_MISSING	A mandatory query parameter is missing in the HTTP request.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	USER_UNKNOWN	The HTTP request is rejected because PCF received an unknown user.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	NO_AVAILABLE_POLICY_COUNTERS	Policy counters are not available.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.
400 - Bad Request	UNKNOWN_POLICY_COUNTERS	Policy counters are unknown.	• Session Retry using connector configuration with PUT and POST requests. • After the session retry is exhausted, final error code for PUT or POST failure will reach core service for Policy evaluation.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-7 (Cont.) Error codes and cause supported by Policy for CHF Interface

Message	Cause Code	Description	Actions
401 - Unauthorized	WWW-Authenticate	Unauthorized with Header "WWW-Authenticate"	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
403 - Forbidden	Modification_Not_Allowed	Request is forbidden.	• Retry with POST request • If retry is exhausted, delete the session
404 - Not Found	SUBSCRIPTION_NOT_FOUND	The request for modification or deletion of a subscription is rejected because the subscription is not found in the NF.	• Retry with POST request • If retry is exhausted, delete the session
404 - Not Found	RESOURCE_URI_STRUCTURE_NOT_FOUND	Resource URI structure is not found.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
405 - Method Not Allowed	NA	The HTTP request is rejected as the performed operation is not allowed.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
406 - Not acceptable	NA	The request is not acceptable.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
409 - Conflict	NA	The request is rejected due to schema errors and conflicts in versions.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-7 (Cont.) Error codes and cause supported by Policy for CHF Interface

Message	Cause Code	Description	Actions
410 - Gone	NA	This requested resource has been permanently deleted.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
411 - Length Required	NA	The HTTP request is rejected due to incorrect value of a Content-length header field.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
412 - Precondition Failed	NA	The request is rejected due to incorrect conditions in GET request.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
413 - Payload Too Large	NA	The payload is larger than the limit.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
414 - URI Too Long	NA	The request URI is longer than the limit.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
415 - Unsupported Media Type	NA	The HTTP request contains unsupported payload payload type.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-7 (Cont.) Error codes and cause supported by Policy for CHF Interface

Message	Cause Code	Description	Actions
429 - Too many requests	NA	The request is rejected due to excessive traffic, which if continued over time, may lead to (or may increase) an overload situation.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
500 - Internal Server Error	NA	The request is rejected due to generic error condition in the NF.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
501 - Not Implemented	NA	The service operation cannot be implemented due to invalid resource URI to be monitored.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
503 - Service Unavailable	NA	The NF experiences congestion and performs overload control, which does not allow the request to be processed.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.
504 - Gateway Timeout	NA	This error code is generated in case of timeout due to inactivity.	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, then terminate the transaction.

Table C-8 Error codes and cause supported by Policy for UDR Interface.

Error Code - Message	Cause Code	Description	Action
400 - Bad Request	INVALID_API	The HTTP request contains an unsupported API name or API version in the URI.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-8 (Cont.) Error codes and cause supported by Policy for UDR Interface.

Error Code - Message	Cause Code	Description	Action
400 - Bad Request	INVALID_MSG_FORMAT	The HTTP request has an invalid format.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
400 - Bad Request	INVALID_QUERY_PARAM	The HTTP request contains an unsupported query parameter in the URI.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
400 - Bad Request	MANDATORY_QUERY_PARAM_INCORRECT	A mandatory query parameter, or aconditional query parameter but mandatoryrequired, for an HTTP method was received in the URI with semantically incorrect value.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
400 - Bad Request	OPTIONAL_QUERY_PARAM_INCORRECT	A mandatory query parameter, or aconditional query parameter but mandatoryrequired, for an HTTP method was received in the URI with semantically incorrect value.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
400 - Bad Request	MANDATORY_QUERY_PARAM_MISSING	Query parameter which is defined asmandatory, or as conditional but mandatoryrequired, for an HTTP method is not included in the URI of the request.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
400 - Bad Request	MANDATORY_IE_INCORRECT	A mandatory IE or conditional IE butmandatory required, for an HTTP methodwas received with a semantically incorrect.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
400 - Bad Request	OPTIONAL_IE_INCORRECT	-	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-8 (Cont.) Error codes and cause supported by Policy for UDR Interface.

Error Code - Message	Cause Code	Description	Action
400 - Bad Request	MANDATORY_IE_MISSING	A mandatory query parameter is missing in theHTTP request.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
400 - Bad Request	USER_UNKNOWN	The HTTP request is rejected because PCF received an unknown user.	• Session Retry using connector configuration with PUT and POST requests. • If retry is exhausted, terminate the transaction.
401 - Unauthorized	WWW-Authenticate	Unauthorized with Header "WWW-Authenticate"	• Post Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, terminate the transaction
403- Forbidden	Modification_Not_Allowed	Request is forbidden.	Retry with POST request
404 - Not Found	SUBSCRIPTION_NOT_FOUND	The request for modification or deletion of a subscription is rejected because the subscription is not found in the NF.	• POST Retry with POST request (Session retry) • Put retry with POST (Revalidation/Reset context) • If retry is exhausted, delete the subscription
404 - Not Found	RESOURCE_URI_STRUCTURE_NOT_FOUND	Resource URI structure is not found.	• Retry with POST request • If retry is exhausted, terminate the transaction
404 - Not Found	USER_UNKNOWN	User is unknown.	• Retry with POST request • If retry is exhausted, terminate the transaction
405 - Method Not Allowed	NA	The HTTP request is rejected as the performed operation is not allowed.	• Retry with POST request • If retry is exhausted, terminate the transaction
406 - Not acceptable	NA	The request is not acceptable.	• Retry with POST request • If retry is exhausted, terminate the transaction
409 -Conflict	NA	The request is rejected due to schema errors and conflicts in versions.	

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-8 (Cont.) Error codes and cause supported by Policy for UDR Interface.

Error Code - Message	Cause Code	Description	Action
410 - Gone	NA	This requested resource has been permanently deleted.	• Retry with POST request • If retry is exhausted, terminate the transaction
411 - Length Required	NA	The HTTP request is rejected due to incorrect value of a Content-length header field.	• Retry with POST request • If retry is exhausted, terminate the transaction
412 - Precondition Failed	NA	The request is rejected due to incorrect conditions in GET request.	• Retry with POST request • If retry is exhausted, terminate the transaction
413 - Payload Too Large	NA	The payload is larger than the limit.	• Retry with POST request • If retry is exhausted, terminate the transaction
414 - URI Too Long	NA	The request URI is longer than the limit.	• Retry with POST request • If retry is exhausted, terminate the transaction
415 - Unsupported Media Type	NA	The HTTP request contains unsupported payload payload type.	• Retry with POST request • If retry is exhausted, terminate the transaction
429 - Too many requests	NA	The request is rejected due to excessive traffic, which if continued over time, may lead to (or may increase) an overload situation.	NA
500 - Internal Server Error	NA	The request is rejected due to generic error condition in the NF.	• Retry with POST request • If retry is exhausted, terminate the transaction
501 - Not Implemented	NA	The service operation cannot be implemented due to invalid resource URI to be monitored.	• Retry with POST request • If retry is exhausted, terminate the transaction
503 - Service Unavailable	NA	The NF experiences congestion and performs overload control, which does not allow the request to be processed.	• Retry with POST request • If retry is exhausted, terminate the transaction

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-8 (Cont.) Error codes and cause supported by Policy for UDR Interface.

Error Code - Message	Cause Code	Description	Action
504 - Gateway Timeout	NA	This error code is generated in case of timeout due to inactivity.	• Retry with POST request • If retry is exhausted, terminate the transaction

Policy as a producer of Error for Notification for CHF Interface

Table C-9 Policy as a producer of Error for Notification for CHF Interface

Error Code - Message	Cause Code	Scenario
400 - Bad Request	MANDATORY_IE_MISSING	When SUPI is not present in the request body for update or terminate notification.
400 - Bad Request	INVALID_MESSAGE_FORMAT	When the request body does not adhere to update or terminate notification structure.
400 - Bad Request	invalid_API	The HTTP request contains an unsupported API name or API version in the URI.
404 - Not Found	RESOURCE_URI_STRUCTURE_NOT_FOUND	The notification URI is incorrect.
404 - Not Found	SUBSCRIPTION_NOT_FOUND	When the spendinglimit resource is not found in DB.
504 - Gateway Timeout	GATEWAY_TIMEOUT	This error code is generated in case of timeout due to inactivity.

Policy as a producer of Error for Notification for UDR Interface

Table C-10 Policy as a producer of Error for Notification for UDR Interface

Error Code - Message	Cause Code	Scenario
400 - Bad Request	INVALID_MESSAGE_FORMAT	When the request body does not adhere to update or terminate notification structure.
404 - Not Found	SUBSCRIPTION_NOT_FOUND	When the PolicyDataChangeNotification resource is not found in DB.
501 - Not Implemented	UNSUPPORTED_MONITORED_URI	When the PolicyDataChangeNotification received have resource other than smPolicyData,operatorSpecificData, amPolicyData, and UePolicySet.

HTTP Error Codes supported by Policy for NRF Interface

HTTP Error codes supported by Policy for NRF Interface:

Copyright © 2019, 2026, Oracle and/or its affiliates.

Error Code - Message	Description	Action
400 - Bad Request	The Request contains invalid values.	**Autonomous mode:** The NF retries primary NRF configurable N times, if fails NF retries secondary NRF configurable M times. NF continues switching back and forth between primary and secondary NRF until success registration. The time interval between one attempt and another is configurable. **On demand mode:** NF retries non primary NRF, if Primary NRF fails. If non primary NRF fails, NF continues with call flow and shall not be able to deregister in NRF.
403 - Forbidden	Request is forbidden.	**Autonomous mode:** The NF retries primary NRF configurable N times, if fails NF retries secondary NRF configurable M times. NF continues switching back and forth between primary and secondary NRF until success registration. The time interval between one attempt and another is configurable. **On demand mode:** NF retries non primary NRF, if Primary NRF fails. If non primary NRF fails, NF continues with call flow and shall not be able to deregister in NRF.
404- Not Found	The request for modification or deletion of a subscription is rejected because the subscription is not found in the NF.	**Autonomous mode:** The NF retries primary NRF configurable N times, if fails NF retries secondary NRF configurable M times. NF continues switching back and forth between primary and secondary NRF until success registration. The time interval between one attempt and another is configurable. **On demand mode:** NF retries non primary NRF, if Primary NRF fails. If non primary NRF fails, NF continues with call flow and shall not be able to deregister in NRF.
405 - Method Not Allowed	The request method is not GET, PUT, PATCH or DELETE.	**Autonomous mode:** The NF retries primary NRF configurable N times, if fails NF retries secondary NRF configurable M times. NF continues switching back and forth between primary and secondary NRF until success registration. The time interval between one attempt and another is configurable. **On demand mode:** NF retries non primary NRF, if Primary NRF fails. If non primary NRF fails, NF continues with call flow and shall not be able to deregister in NRF.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Error Code - Message	Description	Action
411 - Length Required	The request is rejected due to incorrect value of a Content-length header field, or the header doesn't exist.	**Autonomous mode:** The NF retries primary NRF configurable N times, if fails NF retries secondary NRF configurable M times. NF continues switching back and forth between primary and secondary NRF until success registration. The time interval between one attempt and another is configurable. **On demand mode:** NF retries non primary NRF, if Primary NRF fails. If non primary NRF fails, NF continues with call flow and shall not be able to deregister in NRF.
500 - Internal Server Error	Internal error occurred in NRF.	**Autonomous mode:** The NF retries primary NRF configurable N times, if fails NF retries secondary NRF configurable M times. NF continues switching back and forth between primary and secondary NRF until success registration. The time interval between one attempt and another is configurable. **On demand mode:** NF retries non primary NRF, if Primary NRF fails. If non primary NRF fails, NF continues with call flow and shall not be able to deregister in NRF.
503 - Service Unavailable	Rejecting traffic for overload control.	**Autonomous mode:** The NF retries primary NRF configurable N times, if fails NF retries secondary NRF configurable M times. NF continues switching back and forth between primary and secondary NRF until success registration. The time interval between one attempt and another is configurable. **On demand mode:** NF retries non primary NRF, if Primary NRF fails. If non primary NRF fails, NF continues with call flow and shall not be able to deregister in NRF.

Table C-11 Policy as a producer of Error for Notification for NRF Interface

Message	Cause Code	Scenario
400 - Bad Request	INVALID_MSG_FORMAT	NRF terminates the notification transaction.
400 - Bad Request	MANDATORY_IE_INCORRECT	NRF terminates the notification transaction.
400 - Bad Request	OPTIONAL_IE_INCORRECT	NRF terminates the notification transaction.
400 - Bad Request	MANDATORY_IE_MISSING	NRF terminates the notification transaction.
400 - Bad Request	UNSPECIFIED_MSG_FAILURE	NRF terminates the notification transaction.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-11 (Cont.) Policy as a producer of Error for Notification for NRF Interface

Message	Cause Code	Scenario
429 - Too Many Requests	NF_CONGESTION_RISK	NRF terminates the notification transaction.
500 - Internal Server Error	SYSTEM_FAILURE	NRF terminates the notification transaction.
503 - Service Unavailable	NA	NRF terminates the notification transaction.

Table C-12 Error Codes and Cause Supported by Policy for PCRF Core

Message	Cause Code	Description
3001	DIAMETER_COMMAND_UNSUPPORTED	The Request contained a Command-Code that the receiver did not recognize or support. This must be used when a Diameter node receives an experimental command that it does not understand.
3004	DIAMETER_TOO_BUSY	When returned, a Diameter node must attempt to send the message to an alternate peer. This error must only be used when a specific server is requested, and it cannot provide the requested service.
3005	DIAMETER_LOOP_DETECTED	An agent detected a loop while trying to get the message to the intended recipient. The message can be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem.
5003	DIAMETER_AUTHORIZATION_REJECTED	A request was received for which the user can not be authorized. This error can occur if the service requested is not permitted to the user.
5005	DIAMETER_MISSING_AVP	The request did not contain an AVP that is required by the Command Code definition. If this value is sent in the Result-Code AVP, a `Failed-AVP` must be included in the message. The `Failed-AVP` must contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP should be of correct minimum length and contain zeroes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-12 (Cont.) Error Codes and Cause Supported by Policy for PCRF Core

Message	Cause Code	Description
5001	DIAMETER_AVP_UNSUPPORTED	The peer received a message that contained an AVP that is not recognized or supported and was marked with the Mandatory bit. A Diameter message with this error must contain one or more `Failed-AVP` containing the AVPs that caused the failure.
5009	DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	A message was received that included an AVP that appeared more often than permitted in the message definition. The `Failed-AVP` must be included and contain a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences.
5014	DIAMETER_INVALID_AVP_LENGTH	The request contained an AVP with an invalid length. A Diameter message indicating this error must include the offending AVPs within a `Failed-AVP`.
5004	DIAMETER_INVALID_AVP_VALUE	The request contained an AVP with an invalid value in its data portion. A Diameter message indicating this error must include the offending AVPs within a `Failed-AVP`.
3009	DIAMETER_INVALID_AVP_BITS	A request was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the AVP's definition.
3008	DIAMETER_INVALID_HDR_BITS	A request was received whose bits in the Diameter header were either set to an invalid combination, or to a value that is inconsistent with the command code's definition.
3002	DIAMETER_UNABLE_TO_DELIVER	This error is given when Diameter can not deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request, or because Destination-Host AVP was given without the associated Destination-Realm AVP.
5012	DIAMETER_UNABLE_TO_COMPLY	This error is returned when a request is rejected for unspecified reasons.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-12 (Cont.) Error Codes and Cause Supported by Policy for PCRF Core

Message	Cause Code	Description
5002	DIAMETER_UNKNOWN_SESSION_ID	The request contained an unknown Session-Id.

Table C-13 List of errors sent by Diameter Connector for AF

Message	Cause Code	Description
5063	REQUESTED_SERVICE_NOT_AUTHORIZED	The PCRF rejects new or modified service information because the requested service, as described by the service information provided by the AF, is not consistent with either the related subscription information or operator defined policy rules.
5065	IP_CAN_SESSION_NOT_AVAILABLE	The PCRF rejects a new Rx session setup when it fails to associate the described service IP flows within the session information received from the AF to an existing IP-CAN session.
5002	DIAMETER_UNKNOWN_SESSION_ID	The request contained an unknown Session-Id.
5012	DIAMETER_UNABLE_TO_COMPLY	This error is returned when a request is rejected for unspecified reasons.
3004	DIAMETER_TOO_BUSY	When returned, a Diameter node must attempt to send the message to an alternate peer. This error must only be used when a specific server is requested, and it cannot provide the requested service.

Table C-14 List of errors sent by Diameter Connector for Sy

Message	Cause Code	Description
5002	DIAMETER_UNKNOWN_SESSION_ID	The request contained an unknown Session-Id.
5012	DIAMETER_UNABLE_TO_COMPLY	This error is returned when a request is rejected for unspecified reasons.
3004	DIAMETER_TOO_BUSY	When returned, a Diameter node must attempt to send the message to an alternate peer. This error must only be used when a specific server is requested, and it cannot provide the requested service.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-15 List of errors sent by Diameter Gateway for AF

Message	Cause Code	Description
3002	DIAMETER_UNABLE_TO_DELIVER	This error is given when Diameter can not deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request, or because Destination-Host AVP was given without the associated Destination-Realm AVP.
5065	IP_CAN_SESSION_NOT_AVAILABLE	Context owner not found after binding service query for session-id.
3004	DIAMETER_TOO_BUSY	Error 5xx response received from binding service query for session-id.
5012	DIAMETER_UNABLE_TO_COMPLY	Error response received from binding service query for session-id.

Table C-16 List of errors sent by DIAM-STACK (Diameter Gateway, Diameter Connector)

Message	Cause Code	Description
3001	DIAMETER_COMMAND_UNSUPPORTED	The request contained a Command-Code that the receiver did not recognize or support. This must be used when a Diameter node receives an experimental command that it does not understand.
3005	DIAMETER_LOOP_DETECTED	An agent detected a loop while trying to get the message to the intended recipient. The message can be sent to an alternate peer, if one is available, but the peer reporting the error has identified a configuration problem.
5005	DIAMETER_MISSING_AVP	The request did not contain an AVP that is required by the Command-Code definition. If this value is sent in the Result-Code AVP, a `Failed-AVP` must be included in the message. The `Failed-AVP` must contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP must be of correct minimum length and contain zeroes.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-16 (Cont.) List of errors sent by DIAM-STACK (Diameter Gateway, Diameter Connector)

Message	Cause Code	Description
5001	DIAMETER_AVP_UNSUPPORTED	The peer received a message that contained an AVP that is not recognized or supported and was marked with the Mandatory bit. A Diameter message with this error must contain one or more `Failed-AVP` containing the AVPs that caused the failure.
5009	DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	A message was received that included an AVP that appeared more often than permitted in the message definition. The `Failed-AVP` must be included and contain a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences.
5014	DIAMETER_INVALID_AVP_LENGTH	The request contained an AVP with an invalid length. A Diameter message indicating this error must include the offending AVPs within a `Failed-AVP`.
5004	DIAMETER_INVALID_AVP_VALUE	The request contained an AVP with an invalid value in its data portion. A Diameter message indicating this error must include the offending AVPs within a `Failed-AVP`.
3009	DIAMETER_INVALID_AVP_BITS	A request was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the AVP's definition.
3008	DIAMETER_INVALID_HDR_BITS	A request was received whose bits in the Diameter header were either set to an invalid combination, or to a value that is inconsistent with the command code's definition.
3002	DIAMETER_UNABLE_TO_DELIVER	This error is given when Diameter can not deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request, or because Destination-Host AVP was given without the associated Destination-Realm AVP.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-16 (Cont.) List of errors sent by DIAM-STACK (Diameter Gateway, Diameter Connector)

Message	Cause Code	Description
5012	DIAMETER_UNABLE_TO_COMPLY	This error is returned when a request is rejected for unspecified reasons.

Table C-17 List of errors sent by PCRF Core for AF

Message	Cause Code	Description
5063	REQUESTED_SERVICE_NOT_AUTHORIZED	The PCRF rejects a new Rx session setup because the session binding function associated a non-Emergency IMS session to an IP-CAN session established to an Emergency APN.
5012	DIAMETER_UNABLE_TO_COMPLY	This error is returned when a request is rejected for unspecified reasons.
5065	IP_CAN_SESSION_NOT_AVAILABLE	The PCRF rejects a new Rx session setup when it fails to associate the described service IP flows within the session information received from the AF to an existing IP-CAN session.
5066	UNAUTHORIZED_NON_EMERGENCY_SESSION	The PCRF rejects a new Rx session setup because the session binding function associated a non-Emergency IMS session to an IP-CAN session established to an Emergency APN.
5454	DIAMETER_ERROR_TIMED_OUT_REQUEST	PCRF to indicate the incoming request is known to have already timed out at the originating entity.
5068	TEMPORARY_NETWORK_FAILURE	The PCRF rejects new or modified service information because there is a temporary failure in the access network such as the SGW has failed.
5003	DIAMETER_AUTHORIZATION_REJECTED	A request was received for which the user could not be authorized. This error could occur if the service requested is not permitted to the user.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-18 List of errors sent by PCRF Core for Gx

Message	Cause Code	Description
5453	DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST	To indicate that the incoming request collides with an existing session, which has a more recent time stamp than the time stamp of the new request.
5030	DIAMETER_USER_UNKNOWN	The specified end user is unknown in the credit-control server.
5454	DIAMETER_ERROR_TIMED_OUT_REQUEST	PCRF to indicate the incoming request is known to have already timed out at the originating entity.
5002	DIAMETER_UNKNOWN_SESSION_ID	The request contained an unknown Session-Id.
5003	DIAMETER_AUTHORIZATION_REJECTED	A request was received for which the user could not be authorized. This error could occur if the service requested is not permitted to the user.
5012	DIAMETER_UNABLE_TO_COMPLY	This error is returned when a request is rejected for unspecified reasons.
4144	DIAMETER_PENDING_TRANSACTION	A race condition detected, this is 3GPP specific result code

Table C-19 List of errors sent by PCRF Core for Sd

Message	Cause Code	Description
5012	DIAMETER_UNABLE_TO_COMPLY	This error is returned when a request is rejected for unspecified reasons.
5003	DIAMETER_AUTHORIZATION_REJECTED	A request was received for which the user could not be authorized. This error could occur if the service requested is not permitted to the user.

Table C-20 List of errors that Diameter Connector for Sd for 5G

Code	Status Code	Description
408	Request Timeout	This error is returned when Diameter Connector detects a timeout while forwarding Sd:TSR/ Sd:RAR message.
400	Bad Request	This error is returned when Diameter Connector detects that Sd session Id value is null or empty.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-20 (Cont.) List of errors that Diameter Connector for Sd for 5G

Code	Status Code	Description
503	Service Unavailable	This error is returned when Diameter Connector detects that Sd session Id is set as deferred result when Timeout is triggered for Sd:TSR/Sd:RAR message.

Table C-21 List of errors produced by LDAP-GATEWAY as a producer

Code	Status Code	Comments
400	Bad request	This error code indicates that the server cannot process the request sent by the client.
404	Not Found	This error code indicates that there is a mistyped URL and cannot be found.
414	URI Too Long	This error code indicates that URI provided in the client's request is longer than the server is willing to interpret.
500	Internal Servicer Error	This error code indicates that the server encountered an unexpected condition that prevented it from fulfilling your request.
503	Service Unavailable	This error code indicates that the server is temporarily unable to handle the request.

Table C-22 List of errors produced by LDAP-GATEWAY as a consumer

Code	Status Code	Comments
408	Request Timeout	This error code indicates that the server did not receive a complete request from the client within the time it was prepared to wait

Table C-23 List of errors produced by SOAP Connector as a consumer

Code	Status Code	Comments
500	Internal Servicer Error	This error code indicates that the server encountered an unexpected condition that prevented it from fulfilling your request.
503	Service Unavailabl.	This error code indicates that the server is currently unable to handle the request due to a temporary overload or scheduled maintenance.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table C-24 List of errors produced by Usage Monitor as a producer

Code	Status Code	Comments
400	Bad request	This error code indicates that the server cannot process the request sent by the client.
500	Internal Server Error	This error code indicates that the server encountered an unexpected condition that prevented it from fulfilling your request.
504	Gateway Timeout	Gateway Timeout Dependency failure for e.g. Unable to reach PRE

Table C-25 List of errors produced by Usage Monitor as a consumer

Code	Status Code	Comments
500	Internal Servicer Error	This error code indicates that the server encountered an unexpected condition that prevented it from fulfilling your request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

D
Error Code Dictionary

Table D-1 Error Code Dictionary for SM

App Error ID	Description	Cause	Action
EC-OPCF-SM-REQVLD-EI-05-02-400-00009-05-01	SM Create request from SMF to PCF failed at SM Service. **HTTP Status:** 400 - BAD_REQUEST. **Cause:** OPTIONAL_IE_INCORRECT. **Error Category:** Request validation (REQVLD)	SM Create request has optional parameters in invalid format.	If sending SM Create with optional parameters, then those parameters should be in a valid format.
EC-OPCF-SM-INTRNL-EI-05-02-500-00039-05-01	SM Create request from SMF to PCF failed at SM Service **HTTP Status:** 500 - INTERNAL_SERVER_ERROR **Cause:** UNSPECIFIED_NF_FAILURE **Error Category:** Internal (INTRNL)	The request is rejected due to unspecified reasons at the NF.	Refer My Oracle Support for the guidance.
EC-OPCF-SM-REQVLD-EI-05-02-400-00048-05-01	SM Create request from SMF to PCF failed at SM Service **HTTP Status:** 400 - BAD_REQUEST **Cause:**ERROR_INITIAL_PARAMETERS **Error Category:** Request validation (REQVLD)	SM Create requests have empty or invalid mandatory request elements	Send create request with all required and valid parameters
EC-OPCF-SM-REQVLD-EI-05-02-400-00010-05-01	SM Create request from SMF to PCF failed SM Service **HTTP Status:** 400 - BAD_REQUEST **Cause:** MANDATORY_IE_MISSING **Error Category:** Request validation (REQVLD)	SM Create request does not have mandatory elements	Send create request with all required parameters

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-1 (Cont.) Error Code Dictionary for SM

App Error ID	Description	Cause	Action
EC-OPCF-SM-REQVLD-EI-05-02-400-00011-05-01	SM Create request from SMF to PCF failed at SM Service **HTTP Status:** 400 - BAD_REQUEST **Cause:** UNSPECIFIED_MSG_FAILURE **Error Category:** Request validation (REQVLD)	SM Create request has an invalid JSON body	Send create request with valid JSON
EC-OPCF-SM-REQVLD-EI-05-02-411-00046-05-01	SM Create request from SMF to PCF failed at SM Service **HTTP Status:** 411 - LENGTH_REQUIRED **Cause:** INCORRECT_LENGTH **Error Category:** Request validation (REQVLD)	Server (that is, PCF, specifically SM Services) rejects the request with incorrect Content-Length header.	Send create request with valid JSON and content-length
EC-OPCF-SM-REQVLD-EI-05-02-400-00001-05-01	SM Create request from SMF to PCF failed at SM Service **HTTP Status:** 400 - BAD_REQUEST **Cause:** USER_UNKNOWN **Error Category:** Request validation (REQVLD)	SM Create request has SUPI not registered with UDR and validate-user configuration is enabled in SM Policy GUI.	send request with a SUPI that is registered in the UDR or disable validate-user in the SM
EC-OPCF-SM-SIG-EI-05-02-403-00022-05-01	SM Create request from SMF to PCF failed at SM Service **HTTP Status:** 403 - FORBIDDEN **Cause:** POLICY_CONTEXT_DENIED **Error Category:** Signaling operations errors (SIG)	PCF-SM Policy evaluation returns mandatory action "Reject"SM Create request has an invalid content length for the request body	check policy created, the criteria not matching for the accepting policy. correct policy/send correct request to evaluate it to "Accept"

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-1 (Cont.) Error Code Dictionary for SM

App Error ID	Description	Cause	Action
EC-OPCF-SM-SIG-EI-05-04-404-00025-05-01	SM Delete request from SMF to PCF failed at SM Service **HTTP Status:** 404 - NOT_FOUND **Cause:** SUBSCRIPTION_NOT_FOUND **Error Category:** Signaling operations errors (SIG)	SMF sends a Delete request with an association ID which is not associated with any existing SM session.	send a Delete request with a valid association ID which is associated with the existing SM session.
EC-OPCF-SM-SIG-EI-05-02-403-00023-05-01	SM Create request from SMF to PCF failed at SM Service **HTTP Status:** 403 - FORBIDDEN **Cause:** LATE_OVERLAPPING_REQUEST **Error Category:** Signaling operations errors (SIG)	On SMF create Collision detected with older timestamp, request rejected	Refer My Oracle Support for the guidance.
EC-OPCF-SM-SIG-EI-05-03-400-00019-05-01	SM Update request from SMF to PCF failed at SM Service **HTTP Status:** 400 - BAD_REQUEST **Cause:** PENDING_TRANSACTION **Error Category:** Signaling operations errors (SIG)	The error occurs when concurrent request arrives and Lock is already acquired by ongoing transaction in SM.	Refer My Oracle Support for the guidance.
EC-OPCF-SM-INTRNL-EI-05-02-504-00069-05-01	SM request from SMF to PCF failed at SM Service HTTP Status: 504 - GATEWAY_TIMEOUT Cause: TIMED_OUT_REQUEST Error Category: Internal (INTRNL)	The request has timed out and was rejected.	Verify network connectivity, retry the request, and adjust the timeout value if needed.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-1 (Cont.) Error Code Dictionary for SM

App Error ID	Description	Cause	Action
EC-OPCF-SM-REQVLD-EI-05-02-400-00008-05-01	SM Create request from SMF to PCF failed at SM Service HTTP Status: 400 - BAD_REQUEST Cause: MANDATORY_IE_INCORRECT Error Category: Request validation (REQVLD)	SM Create request does not have mandatory parameters as expected	Send create request with all required parameters in valid format
EC-OPCF-SM-REQVLD-EI-05-02-400-00009-05-01	SM Create request from SMF to PCF failed at SM Service. HTTP Status: 400 - BAD_REQUEST Cause: OPTIONAL_IE_INCORRECT. Error Category: Request validation (REQVLD)	SM Create request has optional parameters but in invalid format.	If sending SM Create with optional parameters then those parameters should be in valid format.

Table D-2 Error Code Dictionary for AM

App Error Id	Description	Cause	Action
EC-OPCF-AM-REQVLD-EI-05-02-400-00010-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 400 BAD_REQUEST Cause - MANDATORY_IE_MISSING Error Category**:** Request Validation (REQVLD)	A mandatory Information element is missing in request.	Send the Create request with required parameters in the request body.
EC-OPCF-AM-REQVLD-EI-05-02-400-00011-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 400 BAD_REQUEST Cause - UNSPECIFIED_MSG_FAILURE Error Category**:** Request Validation (REQVLD)	The request is rejected due to unspecified client error.	Make sure the request body is in right Json format.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-2 (Cont.) Error Code Dictionary for AM

App Error Id	Description	Cause	Action
EC-OPCF-AM-REQVLD-EI-05-03-400-00011-06-01	The AM-Update request from AMF to PCF failed at AM Service with HttpStatus - 400 BAD_REQUEST Cause - UNSPECIFIED_MSG_FAILURE Error Category: Request Validation (REQVLD)	The request is rejected due to unspecified client error.	Make sure the request body is in right Json format.
EC-OPCF-AM-REQVLD-EI-05-02-400-00048-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 400 BAD_REQUEST Cause - ERROR_INITIAL_PARAMETERS Error Category: Request Validation (REQVLD)	A request is sent with an error in one or more of its parameters.	Send the Create request with right values for the mandatory parameters.
EC-OPCF-AM-REQVLD-EI-05-02-411-00046-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 411 Length Required Cause - INCORRECT_LENGTH Error Category: Request Validation (REQVLD)	The request is rejected because the length of a provided value does not meet the expected or required criteria.	Make sure that the length of the input matches the required specifications.
EC-OPCF-AM-REQVLD-EI-05-03-411-00046-06-01	The AM-Update request from AMF to PCF failed at AM Service with HttpStatus - 411 Length Required Cause - INCORRECT_LENGTH Error Category: Request Validation (REQVLD)	The request is rejected because the length of a provided value does not meet the expected or required criteria.	Make sure that the length of the input matches the required specifications.
EC-OPCF-AM-REQVLD-EI-05-02-400-00018-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 400 BAD_REQUEST Cause - ERROR_REQUEST_PARAMETERS Error Category: Request Validation (REQVLD)	The Create request is rejected because the information set required by the PCF for AM Policy selection is incomplete, preventing a decision from being made.	Make sure the required parameters are in expected format.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-2 (Cont.) Error Code Dictionary for AM

App Error Id	Description	Cause	Action
EC-OPCF-AM-REQVLD-EI-05-02-400-00001-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 400 BAD_REQUEST Cause - USER_UNKNOWN Error Category: Request Validation (REQVLD)	When validate user is enabled and Create request is sent for a SUPI that is not registered in the UDR.	Send the Create request with right/registered Supi.
EC-OPCF-AM-SIG-EI-05-03-404-00025-06-01	The AM-Update request from AMF to PCF failed at AM Service with HttpStatus - 404 Not Found Cause - SUBSCRIPTION_NOT_FOUND Error Category: Signaling (SIG)	When AM-Update is sent with a polAssoId that is not associated with any existing AM session.	Send the Update request with right/ registered Supi.
EC-OPCF-AM-SIG-EI-05-04-404-00025-06-01	The AM-Terminate request from AMF to PCF failed at AM Service with HttpStatus - 404 Not Found Cause - SUBSCRIPTION_NOT_FOUND Error Category: Signaling (SIG)	When AM-Delete is sent with a polAssoId that is not associated with any existing AM session.	Send the Delete request with right/registered polAssoId.
EC-OPCF-AM-INTRNL-EI-05-02-500-00039-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 500 Internal Server Error Cause - UNSPECIFIED_NF_FAILURE Error Category: Internal (INTRNL)	The request is rejected due to unspecified reason at the NF.	Refer My Oracle Support for the guidance.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-2 (Cont.) Error Code Dictionary for AM

App Error Id	Description	Cause	Action
EC-OPCF-AM-INTRNL-EI-05-03-500-00039-06-01	The AM-Update request from AMF to PCF failed at AM Service with HttpStatus - 500 Internal Server Error Cause - UNSPECIFIED_NF_FAILURE Error Category: Internal (INTRNL)	The request is rejected due to unspecified reason at the NF.	Refer My Oracle Support for the guidance.
EC-OPCF-AM-INTRNL-EI-05-04-500-00039-06-01	The AM-Terminate request from AMF to PCF failed at AM Service with HttpStatus - 500 Internal Server Error Cause - UNSPECIFIED_NF_FAILURE Error Category: Internal (INTRNL)	The request is rejected due to unspecified reason at the NF.	Refer My Oracle Support for the guidance.
EC-OPCF-AM-SIG-EI-05-02-403-00022-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 403 Forbidden Cause - POLICY_CONTEXT_DENIED Error Category: Signaling (SIG)	AM Create request is rejected by PRE	Check and update PRE policy accordingly
EC-OPCF-AM-SIG-EI-05-03-403-00022-06-01	The AM-Update request from AMF to PCF failed at AM Service with HttpStatus - 403 Forbidden Cause - POLICY_CONTEXT_DENIED Error Category: Signaling (SIG)	AM Update request is rejected by PRE	Check and update PRE policy accordingly

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-2 (Cont.) Error Code Dictionary for AM

App Error Id	Description	Cause	Action
EC-OPCF-AM-SIG-EI-05-04-403-00022-06-01	The AM-Terminate request from AMF to PCF failed at AM Service with HttpStatus - 403 Forbidden Cause - POLICY_CONTEXT_DENIED Error Category: Signaling (SIG)	AM Terminate request is rejected by PRE	Check and update PRE policy accordingly
EC-OPCF-AM-SIG-EI-05-02-403-00023-06-01	The AM-Create request from AMF to PCF failed at AM Service with HttpStatus - 403 Forbidden Cause - LATE_OVERLAPPING_REQUEST Error Category: Signaling (SIG)	The request is rejected because it collides with an existing AM context or PDU session context with a more recent origination timestamp.	Refer My Oracle Support for the guidance.
EC-OPCF-AM-SIG-EI-05-03-400-00019-06-01	The AM-Update request from AMF to PCF failed at AM Service HttpStatus - 400 Bad Request Cause - PENDING_TRANSACTION Error Category: Signaling (SIG)	This error shall be used when the PendingTransaction feature is supported and the PCF receives an incoming request on a policy association while it has an ongoing transaction on the same policy association.	Refer My Oracle Support for the guidance.
EC-OPCF-AM-INTRNL-EI-05-02-504-00069-06-01	AM request from AMF to PCF failed at AM Service HTTP Status: 504 - GATEWAY_TIMEOUT Cause: TIMED_OUT_REQUEST Error Category: Internal (INTRNL)	The request has timed out and was rejected.	Refer My Oracle Support for the guidance.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-3 Error Code Dictionary for UE

App Error Id	Description	Cause	Action
EC-OPCF-UE-REQVLD-EI-05-02-400-00010-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 400 - BAD_REQUEST **Cause:** MANDATORY_IE_MISSING **Error Category:** Request Validation (REQVLD)	UE Create request does not have mandatory information elements	Send create request with all required parameters
EC-OPCF-UE-REQVLD-EI-05-02-400-00011-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status**: 400 - BAD_REQUEST **Cause:** UNSPECIFIED_MSG_FAILURE **Error Category:** Request Validation (REQVLD)	UE Create request have invalid JSON body	Send create request with valid JSON body
EC-OPCF-UE-REQVLD-EI-05-02-400-00001-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 400 - BAD_REQUEST **Cause:** USER_UNKNOWN **Error Category:** Request Validation (REQVLD)	UE Create request have unregistered SUPI. **Configuration:** Validate user flag is enabled	Send create request with a registered SUPI
EC-OPCF-UE-REQVLD-EI-05-02-400-00018-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 400 - BAD_REQUEST **Cause:** ERROR_REQUEST_PARAMETERS **Error Category:** Request Validation (REQVLD)	UE Create request have empty mandatory information elements	Send create request with all required and valid parameters

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-3 (Cont.) Error Code Dictionary for UE

App Error Id	Description	Cause	Action
EC-OPCF-UE-SIG-EI-05-02-400-00019-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 400 - BAD_REQUEST **Cause:** PENDING_TRANSACTION **Error Category:** **Signaling (SIG)**	UE Create request cannot be processed because of the pending transaction of same policy association in request.	Wait for the current transaction to complete, then retry the UE Create request.
EC-OPCF-UE-SIG-EI-05-02-403-00022-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 403 - FORBIDDEN **Cause:** POLICY_CONTEXT_DENIED **Error Category:** Signaling (SIG)	UE Create request rejected by PRE	Check and update PRE policy accordingly if needed
EC-OPCF-UE-SIG-EI-05-02-403-00023-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 403 - FORBIDDEN **Cause:** LATE_OVERLAPPING_REQUEST **Error Category:** Signaling (SIG)	UE Create request rejected because it collides with an existing UE context or PDU session context with more recent origination timestamp.	Wait for sometime and resend UE create request
EC-OPCF-UE-REQVLD-EI-05-02-411-00046-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 411 - LENGTH REQUIRED **Cause:** INCORRECT_LENGTH **Error Category:** Request Validation (REQVLD)	Server (*i.e. PCF, specifically UE Services*) rejects the request with incorrect Content-Length header	Check if Content-Length header is present in request headers and has a valid value which matches to the request body size.
EC-OPCF-UE-INTRNL-EI-05-02-500-00039-06-01	UE Create request from AMF to PCF failed at UE Service. **HTTP Status:** 500 INTERNAL SERVER ERROR **Cause:** UNSPECIFIED_NF_FAILURE **Error Category:** Internal (INTRNL)	UE Create request failed with unexpected internal service error.	Refer My Oracle Support for the guidance.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-3 (Cont.) Error Code Dictionary for UE

App Error Id	Description	Cause	Action
EC-OPCF-UE-REQVLD-EI-05-03-400-00011-06-01	UE Update request from AMF to PCF failed at UE Service. **HTTP Status**: 400 - BAD_REQUEST **Cause:** UNSPECIFIED_MSG_FAILURE **Error Category:** Request Validation (REQVLD)	UE Update request have invalid JSON body	Send update request with valid JSON body
EC-OPCF-UE-SIG-EI-05-03-403-00022-06-01	UE Update request from AMF to PCF failed at UE Service. **HTTP Status:** 403 - FORBIDDEN **Cause:** POLICY_CONTEXT_DENIED **Error Category:** Signaling (SIG)	UE Update request rejected by PRE	Check and update PRE policy accordingly if needed
EC-OPCF-UE-SIG-EI-05-03-403-00023-06-01	UE Update request from AMF to PCF failed at UE Service. **HTTP Status:** 403 - FORBIDDEN **Cause:** LATE_OVERLAPPING_REQUEST **Error Category:** Signaling (SIG)	UE Update request rejected because it collides with an existing UE context or PDU session context with more recent origination timestamp.	Refer My Oracle Support for the guidance.
EC-OPCF-UE-SIG-EI-05-03-404-00025-06-01	UE Update request from AMF to PCF failed at UE Service. **HTTP Status:** 404 - NOT FOUND **Cause:** SUBSCRIPTION_NOT_FOUND **Error Category:** Signaling (SIG)	UE Update request failed because of unregistered association ID in URL.	Send update request with a registered association ID
EC-OPCF-UE-REQVLD-EI-05-03-411-00046-06-01	UE Update request from AMF to PCF failed at UE Service. **HTTP Status:** 411 - LENGTH REQUIRED **Cause:** INCORRECT_LENGTH **Error Category:** Request Validation (REQVLD)	Server (*i.e. PCF, specifically UE Services*) rejects the request with incorrect Content-Length header	Check if Content-Length header is present in request headers and has a valid value which matches to the request body size.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-3 (Cont.) Error Code Dictionary for UE

App Error Id	Description	Cause	Action
EC-OPCF-UE-INTRNL-EI-05-03-500-00039-06-01	UE Update request from AMF to PCF failed at UE Service. **HTTP Status:** 500 INTERNAL SERVER ERROR **Cause:** UNSPECIFIED_NF_FAILURE **Error Category:** Internal (INTRNL)	UE Update request failed with unexpected internal service error.	Contact My Oracle Support for the guidance.
EC-OPCF-UE-SIG-EI-05-04-404-00025-06-01	UE Delete request from AMF to PCF failed at UE Service. **HTTP Status:** 404 - NOT FOUND **Cause:** SUBSCRIPTION_NOT_FOUND **Error Category:** Signaling (SIG)	UE Delete request failed because of unregistered association ID in URL.	Send update request with a registered association ID
EC-OPCF-UE-INTRNL-EI-05-04-500-00039-06-01	UE Delete request from AMF to PCF failed at UE Service. **HTTP Status:** 500 INTERNAL SERVER ERROR **Cause:** UNSPECIFIED_NF_FAILURE **Error Category:** Internal (INTRNL)	UE Update request failed with unexpected internal service error.	Refer My Oracle Support for the guidance.
EC-OPCF-UE-SIG-EI-05-08-404-00025-06-01	UE N1 notification or failure notification request from AMF to PCF failed at UE Service. **HTTP Status:** 404 NOT FOUND **Cause:** SUBSCRIPTION_NOT_FOUND **Error Category:** Signaling (SIG)	UE N1 notification or failure notification failed due to subscription not found	Send notification request with a registered association ID.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-3 (Cont.) Error Code Dictionary for UE

App Error Id	Description	Cause	Action
EC-OPCF-UE-INTRNL-EI-05-08-404-00000-06-01	UE N1 notification request from AMF to PCF failed at UE Service. **HTTP Status:** 404 NOT FOUND **Cause:** PTI does not match **Error Category:** Internal (INTRNL)	UE N1 notification or failure notification failed due to PTI mismatch in the association	Send notification request with a right PTI for the association.
EC-OPCF-UE-INTRNL-EI-05-08-500-00039-06-01	UE N1 notification or failure notification request from AMF to PCF failed at UE Service. **HTTP Status:** 500 INTERNAL SERVER ERROR **Cause:** UNSPECIFIED_NF_FAILURE **Error Category:** Internal (INTRNL)	Any exception during request validation	Send the right notification body
EC-OPCF-UE-INTRNL-EI-05-08-500-00000-06-01	UE N1 notification or failure notification request from AMF to PCF failed at UE Service. **HTTP Status:** 500 INTERNAL SERVER ERROR **Cause:** Null or Exception in processing notification request **Error Category:** Internal (INTRNL)	1. Timeout exception Cause: null 2. Any other internal exception in processing notification Cause: Exception in processing notification request	Please contact My Oracle Support for any guidance
EC-OPCF-UE-INTRNL-EI-05-08-403-00000-06-01	UE N1 notification request from AMF to PCF failed at UE Service. **HTTP Status:** 403 Forbidden **Cause:** Exception in decoding N1 NAS Message **Error Category:** Internal (INTRNL)	N1 notification with incorrect NAS data.	Send the right NAS message from AMF

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-3 (Cont.) Error Code Dictionary for UE

App Error Id	Description	Cause	Action
EC-OPCF-UE-INTRNL-EI-05-02-504-00069-06-01	UE request from AMF to PCF failed at UE Service HTTP Status: 504 - GATEWAY_TIMEOUT Cause: TIMED_OUT_REQUEST Error Category: Internal (INTRNL)	The request has timed out and was rejected.	Verify network connectivity, retry the request, and adjust the timeout value if needed.

Table D-4 Error Code Dictionary for UDR Connector

App Error Id	Description	Cause	Action
EC-OPCF-UDR_C-REQVLD-EI-05-08-400-00003-03-01	The UDR notification request from UDR to PCF failed at UDR-Connector with httpStatus- 400 BAD_REQUEST cause-INVALID_MSG_FORMAT Note: Applies for UM notification as well	1. Incorrect JSON format 2. Empty Notification Body i.e., []	1. Verify UDR to send the content with right JSON format 2. Verify UDR to send the notification with notification data
EC-OPCF-UDR_C-REQVLD-EI-05-08-400-00011-03-01	The UDR notification request from UDR to PCF failed at UDR-Connector with httpStatus- 400 BAD_REQUEST cause-UNSPECIFIED_MSG_FAILURE Note: Applies for UM notification as well	1. Null notification body i.e., no content in the body	1. Verify UDR to send the notification with content
EC-OPCF-UDR_C-REQVLD-EI-05-08-501-00043-03-01	The UDR notification request from UDR to PCF failed at UDR-Connector with httpStatus- 501 Not Implemented cause-UNSUPPORTED_MONITORED_URI Note: Applies for UM notification as well	1. When notification body doesn't contain at least one of the data source notification data among the below a. smPolicyData b. amPolicyData c. uePolicySet d. delResources	1. Verify UDR to send the notification with at least one of the listed data Source information

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-4 (Cont.) Error Code Dictionary for UDR Connector

App Error Id	Description	Cause	Action
EC-OPCF-UDR_C-EI-05-08-404-00025-03-01	The UDR notification request from UDR to PCF failed at UDR-Connector with httpStatus- 404 Not Found cause-SUBSCRIPTION_NOT_FOUND Note: Applies for UM notification as well	1. When the notification received user session is not present in Policy-ds 2. Session for the user is found but subscription information is missing.	Refer My Oracle Support for the guidance.
EC-OPCF-UDR_C-INTRNL-EI-05-08-504-00069-03-01	Request from UDR to PCF failed HTTP Status: 504 - GATEWAY_TIMEOUT Cause: TIMED_OUT_REQUEST Error Category: Internal (INTRNL)	The request has timed out and was rejected.	Verify network connectivity, retry the request, and adjust the timeout value if needed

Table D-5 Error Code Dictionary for CHF Connector

App Error Id	Description	Cause	Action
EC-OPCF-CHF_C-REQVLD-EI-05-08-400-00003-04-01	The NOTIFY-POST request from CHF to PCF failed with status code 400 and cause 'INVALID_MSG_FORMAT'	The request body JSON need to follow a certain format	Send the POST request in the correct format.
EC-OPCF-CHF_C-REQVLD-EI-05-08-400-00010-04-01	The NOTIFY-POST request from CHF to PCF failed with status code 400 and cause 'MANDATORY_IE_MISSING'	SUPI is a mandatory parameter for the POST request	Send the POST request with the SUPI information present in the body.
EC-OPCF-CHF_C-REQVLD-EI-05-08-400-00011-04-01	The NOTIFY-POST request from CHF to PCF failed with status code 400 and cause 'UNSPECIFIED_MSG_FAILURE'	The request body JSON needs to follow a certain format	Send the POST request in the correct format.
EC-OPCF-CHF_C-SIG-EI-05-08-404-00025-04-01	The NOTIFY-POST request from CHF to PCF failed with status code 404 and cause 'SUBSCRIPTION_NOT_FOUND'	The user session is not present in PolicyDS or the session for the user is found but the subscription information is missing.	Refer My Oracle Support for the guidance.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-5 (Cont.) Error Code Dictionary for CHF Connector

App Error Id	Description	Cause	Action
EC-OPCF-CHF_C-INTRNL-EI-05-08-500-00000-04-01	The NOTIFY-POST request from CHF to PCF failed with status code 500 and cause 'UNKNOWN'	PDS responded back with status code 500	Refer My Oracle Support for the guidance.
EC-OPCF-CHF_C-INTRNL-EI-05-08-503-00000-04-01	The NOTIFY-POST request from CHF to PCF failed with status code 503 and cause 'UNKNOWN'	Required service is unavailable	Check whether all services are up and running
EC-OPCF-CHF_C-REQVLD-EI-05-11-400-00003-04-01	The TERMINATE-POST request from CHF to PCF failed with status code 400 and cause 'INVALID_MSG_FORMAT'	The request body JSON need to follow a certain format	Send the POST request in the correct format.
EC-OPCF-CHF_C-REQVLD-EI-05-04-400-00011-04-01	The TERMINATE-POST request from CHF to PCF failed with status code 400 and cause 'UNSPECIFIED_MSG_FAILURE'	The request body JSON needs to follow a certain format	Send the POST request in the correct format.
EC-OPCF-CHF_C-SIG-EI-05-08-404-00025-04-01	The TERMINATE-POST request from CHF to PCF failed with status code 404 and cause 'SUBSCRIPTION_NOT_FOUND'	The user session is not present in PolicyDS or the session for the user is found but the subscription information is missing.	Refer My Oracle Support for the guidance.
EC-OPCF-CHF_C-INTRNL-EI-05-08-500-00000-04-01	The TERMINATE-POST request from CHF to PCF failed with status code 500 and cause 'UNKNOWN'	PDS responded back with status code 500	Refer My Oracle Support for the guidance.
EC-OPCF-CHF_C-INTRNL-EI-05-08-503-00000-04-01	The TERMINATE-POST request from CHF to PCF failed with status code 503 and cause 'UNKNOWN'	Required service is unavailable	Check whether all services are up and running
EC-OPCF-CHF_C-INTRNL-EI-05-08-504-00069-04-01	Request from CHF to PCF failed HTTP Status: 504 - GATEWAY_TIMEOUT Cause: TIMED_OUT_REQUEST Error Category: Internal (INTRNL)	The request has timed out and was rejected.	Verify network connectivity, retry the request, and adjust the timeout value if needed

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-6 Error Code Dictionary for Binding

App Error Id	Description	Cause	Action
EC-OPCF-BINDING-REQVLD-EI-05-19-500-00011-02-01	BSF Audit request from BSF to PCF failed at Binding Service with HttpStatus - 500 Internal Server Error Cause - UNSPECIFIED_MSG_FAILURE Error Category: Request Validation (REQVLD)	The request is rejected due to unspecified client error.	Make sure the request body is in right Json format.
EC-OPCF-BINDING-REQVLD-EI-05-19-500-00046-02-01	BSF Audit request from BSF to PCF failed at Binding Service with HttpStatus - 500 Internal Server Error Cause - INCORRECT_LENGTH Error Category: Request Validation (REQVLD)	The request has an invalid content length for the request body	Check if Content-Length header is present in request headers and has a valid value which matches to the request body size.
EC-OPCF-BINDING-SIG-EI-05-19-404-00053-02-01	BSF Audit request from BSF to PCF failed at Binding Service with HttpStatus - 404 Not Found Cause - CONTEXT_NOT_FOUND Error Category: Signaling (SIG)	BSF Audit request is sent with a context id that is not associated with any existing Binding session.	Send the request with registered context id.
EC-OPCF-BINDING-INTRNL-EI-05-19-500-00000-02-01	BSF Audit request from BSF to PCF failed at Binding Service with HttpStatus - 500 Internal Server Error Cause - UNKNOWN Error Category: Internal (INTRNL)	The request is rejected due to unknown error.	Refer My Oracle Support for the guidance.

Table D-7 Error Code Dictionary for Egress Gateway

App Error Id	Description	Cause	Action
OPCF-EGW-E001 **Error Type**: CONNECTION_TIMEOUT	This error code indicates that Egress Gateway is unable to establish the connection with peer NF in the configured connectionTimeout period.	The server is down, or it takes too long to respond.	Increase the timeout value or check if the server is up and running.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-7 (Cont.) Error Code Dictionary for Egress Gateway

App Error Id	Description	Cause	Action
OPCF-EGW-E002 **Error Type**: REQUEST_TIMEOUT	This error code indicates that request processing time is more than the configured request timeout at Egress Gateway.	A successful TCP connection was established, but no response was received within the expected time frame.	To resolve this issue, increase the request timeout setting on the Egress Gateway or optimize the back-end services to handle the request faster.
OPCF-EGW-E003 **Error Type**: UNKNOWN_HOST_EXCEPTION	This error code indicates that Egress Gateway is unable to resolve the peer NF service host name.	The error message indicates that Egress Gateway is unable to resolve the configured back-end service hostname. This could be due to several reasons, such as incorrect DNS settings, network issues, or misconfigured hostnames.	Ensure that the hostname provided in the configuration file matches the actual hostname of the back-end service. If required, update the DNS records or configure Gateway Services to use Alternative Routing Service.
OPCF-EGW-E004 **Error Type**: CONNECT_EXCEPTION	This error code indicates that Egress Gateway is unable to establish the connection with peer NF service.	Peer or NF service is refused due to incorrect network configuration and inactive service.	Verify peer or NF service availability, network routing, and ensure that the correct IP address and port are being used.
OPCF-EGW-E005 **Error Type**: INVALID_HTTP_REQUEST_EXCEPTION	This error code indicates an exception occurred because HTTP1.1 is disabled, but the oc-http-version header has a value http1.	The enableOutgoingHttp1 parameter of Egress Gateway is set to false.	Set the enableOutgoingHTTP1 parameter in Egress Gateway config to true.
OPCF-EGW-E006 **Error Type**: CLOSED_CHANNEL_EXCEPTION	This error code indicates that a closed channel exception has occurred as the incoming TCP connection was abruptly terminated before Egress Gateway sent the response.	Unexpected behavior is observed within the network.	Capture network traces to identify the cause why the connection was terminated abruptly.
OPCF-EGW-E007 **Error Type**: SSL_HANDSHAKE_EXCEPTION	This error code indicates the SSL handshake exception occurred in Egress Gateway.	Incorrect certificates are used to establish the connection. Use of incorrect certificates or cipher suites mismatch or TLS version incompatibility.	Check certificates, Cipher suites, and TLS version match between the client and server.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-7 (Cont.) Error Code Dictionary for Egress Gateway

App Error Id	Description	Cause	Action
OPCF-EGW-E051 **Error Type**: REJECTED_EXECUTION_EXCEPTION	This error code indicates that RejectedExecutionException has occurred at Egress Gateway as the number of incoming requests is more than queueCapacity configured in applicationThreadPoolConfig.	Value set for the applicationThreadPoolConfig configuration in Egress Gateway is low for incoming traffic.	Increase the value of applicationThreadPoolConfig in Egress Gateway Configuration or reduce the number of requests to Egress Gateway for incoming traffic.
OPCF-EGW-E052 **Error Type**: NOT_FOUND_EXCEPTION	This error code indicates that Egress Gateway received a request path with an endpoint that is not implemented in the peer NF service.	URI of the request has not been configured in the routesConfig for Egress Gateway.	Configure the required URI in routesConfig or correct the URI of the request.
OPCF-EGW-E054 **Error Type**: INTERNAL_ERROR	This error code indicates that some unknown internal error occurred in Egress Gateway while processing the request.	NA	NA
OPCF-EGW-E102 **Error Type**: LATE_ARRIVAL_EXCEPTION	This error code indicates that late arrival exception has occurred at Egress Gateway as the request has already expired as part of the SbiTimer feature.	• Timezone mismatch or 12H/24H time format mismatch is leading to some time in the past in SBI Timer header for SBI Timer feature. • Header of MaxRspTime might have been configured with the wrong value. • The calculated request timeout value based on SBI Timer Headers is less than the configured requiredTime value at the route level.	Ensure that the timestamp and maximum response time attached in the header are of the correct time with respect to the time zone and not a time in the past. Verify if the requiredTime is accommodating to the calculated timeout value from SBI Timer header values.
OPCF-EGW-E112 **Error Type**: NOTIFICATION_RATE_LIMIT	This error code indicates that requests are being rejected after exceeding the bucketCapacity when the notificationRateLimit feature is enabled.	Request count is higher than the configured bucketCapacity at notificationRateLimit in Egress Gateway configurations.	Either increase the bucketCapacity or reduce the number of requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-7 (Cont.) Error Code Dictionary for Egress Gateway

App Error Id	Description	Cause	Action
OPCF-EGW-E122 **Error Type**: RETRY_AFTER_ERROR	This error code indicates that the retry-after feature is enabled and producer FQDN is blocklisted, therefore the request cannot be fulfilled.	The RetryAfter feature is enabled, and the blackListPeriod is completed for the peer. But when the peer is accessed when it is blocklisted, this error is displayed.	If not the intended behavior, disable the RetryAfter feature.
OPCF-EGW-E127 **Error Type**: GRACEFUL_SHUTDOWN	This error code indicates that the service shutdown is in progress.	During the processing of requests, if the IP changes and DNS refresh occurs.	Wait for the IP reset and DNS refresh to complete. After establishing connection to the service, try sending the request again.
OPCF-EGW-E132 **Error Type**: VIRTUAL_HOST_RESOLUTION_ERROR	This error code indicates that the DNS resolution of virtual FQDN failed.	The vFQDN provided for the virtual host cannot be resolved by the DNS servers.	• Verify that the vFQDN is correctly spelled and formatted. • Ensure that the DNS server is operational. • Confirm that the FQDN exists in the DNS records.
OPCF-EGW-E152 **Error Type**: INVALID_OAUTH_TOKEN_REQUEST	This error code indicates the exception occurred because of a bad AccessToken request received.	The OAuth token received might be of the incorrect format or value.	Check the correct format or value on the basis of the configurations at Egress Gateway.
OPCF-EGW-E153 **Error Type**: OAUTH_INTERNAL_ERROR	This error code indicates that Egress Gateway is unable to send an AccessToken request to NRF.	InternalServerError because of error while processing or sending a request to NRF.	NA
OPCF-EGW-E154 **Error Type**: OAUTH_TOKEN_RETRIEVAL_FAILURE	This error code indicates an error in retrieving a token from NRF.	Error while retrieving the token from a response received from NRF.	NA
OPCF-EGW-E155 **Error Type**: OAUTH_NRF_RESPONSE_FAILURE	This error code indicates response failure from NRF (invalid/bad response) while trying to fetch OAuth token.	Error while processing the response received from NRF.	NA
OPCF-EGW-E172 **Error Type**: EGRESS_RATE_LIMITING	This error code indicates that requests are being rejected after exceeding the bucketCapacity when the egressRateLimiting feature is enabled.	The number of requests is exceeding the bucket size set in the configurations for Egress Gateway.	Edit the bucket size in Egress Gateway configurations, or reduce the rate of requests.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-7 (Cont.) Error Code Dictionary for Egress Gateway

App Error Id	Description	Cause	Action
OPCF-EGW-E182 **Error Type**: EGW_CUSTOM_EXCEPTION	This error code indicates that custom exception occurred in some feature at Egress Gateway because some conditions failed to fulfill at runtime, such as SbiRouting, SeppProxyFilter, PeerBlackListHelper, EgressGatewayFilter, and so on.	NA	Identify the error from the response received, and verify with the respective documentaiton.
OPCF-EGW-E183 **Error Type**: RESPONSE_STATUS_EXCEPTION	This error code indicates that ResponseStatusException was created by Spring boot as Egress Gateway exception handler was unable to handle an exception.	NA	NA
OPCF-EGW-E192 **Error Type**: PARTIAL_SHUTDOWN	This error code indicates that requests are being discarded partially at Egress Gateway when the control shutdown feature is enabled.	Behavior is observed when ControlledShutdown is enabled.	Disable the ControlledShutdown configuration.
OPCF-EGW-E193 **Error Type**: COMPLETE_SHUTDOWN	This error code indicates that requests are being discarded completely at Egress Gateway when the control shutdown feature is enabled.	Behavior is observed when ControlledShutdown is enabled.	Disable the ControlledShutdown configuration.
OPCF-EGW-E202 **Error Type**: INVALID_ROUTE_EXCEPTION	This error code indicates that an invalid route exception has occurred as invalidRouteFilter was configured in routesConfiguration.	Invalid route exception filter is enabled at the route level in routesConfig.	If this is unexpected behavior, check if the expected path was supposed to be marked as an invalid route.
OPCF-EGW-E206 **Error Type**: IP_TYPE_MISMATCH_EXCEPTION	This error code indicates that there is a mismatch in the configured EgressRoutingMode IP type and the DNS resolved IP type.	The type of IP resolved by DNS is different from the IP type configured at Egress Gateway.	Verify if Gateway Services is deployed in a dual stack IP setup.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-8 App Error Code Dictionary for Ingress Gateway

Application Error Code ID	Description	Cause	Action
OPCF-IGW-E001 **Error Type**: CONNECTION_TIMEOUT	This error code indicates that Ingress Gateway is unable to establish connection with the back-end service in the configured connectionTimeout period.	The server is down, or it takes too long to respond.	Increase the timeout value or check if the server is up and running.
OPCF-IGW-E002 **Error Type**: REQUEST_TIMEOUT	This error code indicates that request processing time is more than the configured request timeout at Ingress Gateway.	A successful TCP connection was established, but no response was received within the expected time frame.	To resolve this issue, increase the request timeout setting on the Ingress Gateway or optimize the back-end services to handle the request faster.
OPCF-IGW-E003 **Error Type**: UNKNOWN_HOST_EXCEPTION	This error code indicates that Ingress Gateway is unable to resolve the configured back-end service host name.	The error message indicates that the Ingress Gateway is unable to resolve the configured back-end service hostname. This occurs due to several reasons, such as incorrect DNS settings, network issues, or misconfigured hostnames.	Check if the FQDN of the back-end service is correctly resolved from the Ingress Gateway. If required, update the DNS records or configure Ingress Gateway to use alternative routing servers. Additionally, ensure that the hostname provided in the configuration file matches the actual hostname of the back-end service.
OPCF-IGW-E004 **Error Type**: CONNECT_EXCEPTION	This error code indicates that Ingress Gateway is unable to establish the connection with the back-end service.	Peer or NF service is refused due to incorrect network configuration and inactive service.	Verify peer or NF service availability, network routing, and ensure that the correct IP address and port are being used.
OPCF-IGW-E005 **Error Type**: BLACKLIST_IP_EXCEPTION	This error code indicates that Blocklist IP exception has occurred while establishing a new connection with the blocklisted IP at Ingress Gateway. IP is blocklisted if the TCP connection to this IP has failed more than 10 times	Gateway Services is unable to establish TCP connection for more than 10 times.	Verify why the IP is not accepting TCP connecitons.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-8 (Cont.) App Error Code Dictionary for Ingress Gateway

Application Error Code ID	Description	Cause	Action
OPCF-IGW-E006 **Error Type**: CLOSED_CHANNEL_EXCEPTION	This error code indicates that closed channel exception has occurred because the incoming TCP connection was abruptly terminated before Ingress Gateway sent back the response.	Unexpected behavior is observed within the network.	Capture network traces to identify the cause why the connection was terminated abruptly.
OPCF-IGW-E051 **Error Type**: REJECTED_EXECUTION_EXCEPTION	This error code indicates that RejectedExecutionException has occurred at Ingress Gateway as the number of incoming requests is more than the queueCapacity configured in applicationThreadPoolConfig.	Value set for the applicationThreadPoolConfig configuration in Ingress Gateway is low for incoming traffic.	Increase the value of applicationThreadPoolConfig in Ingress Gateway Configuration or reduce the number of requests to Ingress Gateway for incoming traffic.
OPCF-IGW-E052 **Error Type**: NOT_FOUND_EXCEPTION	This error code indicates that Ingress Gateway received the request path with no endpoint implemented in the back-end service.	URI of the Request has not been configured in the routesConfig for Ingress Gateway.	Configure the required URI in routesConfig or correct the URI of the request.
OPCF-IGW-E053 **Error Type**: SOCKET_EXCEPTION	This error indicates that SocketException has occurred as Ingress Gateway was unable to create a TCP connection.	Due to network connectivity issues, network restrictions, or misconfigured endpoints.	Verify if there are any network policies blocking the communication between the Ingress Gateway and the back-end service. Ensure that the endpoint URL provided in the configuration file is correct and reachable from Ingress Gateway.
OPCF-IGW-E054 **Error Type**: INTERNAL_ERROR	This error code indicates some unknown internal error occurred at Ingress Gateway while processing the request.	Internal errors occur when there is an issue with improper configurations and mismatches in Helm charts and versions.	Identify the cause from the error message sent back in the response and refer to the documentation for the specific feature that is being used and verify all the configurations. Helm charts and respective versions can be checked.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-8 (Cont.) App Error Code Dictionary for Ingress Gateway

Application Error Code ID	Description	Cause	Action
OPCF-IGW-E102 **Error Type**: LATE_ARRIVAL_EXCEPTION	This error code indicates that late arrival exception occurred at Ingress Gateway as the request has already expired as part of the SbiTimer feature.	• Timezone mismatch (or) 12H/24H time format mismatch leading to some time in the past in SBI Timer • Header for SBI Timer Feature (or) Header of MaxRspTime might have been configured with the wrong value • The calculated request timeout value based on SBI Timer Headers is less than the configured required Time value at route level	Ensure that the timestamp and maximum response time attached in the header are of the correct time with respect to the time zone and not a time in the past. Verify if the requiredTime is accommodating to the calculated timeout value from SBI Timer header values.
OPCF-IGW-E112 **Error Type**: USERAGENT_VALIDATION_FAILURE_EXCEPTION	This error code indicates validation of the User-Agent header failure at Ingress Gateway.	The NF configured in the User-Agent header of the request does not match with the configured NFs in Ingress Gateway.	Either verify if the request has the correct NF value configured, or if the intended NF has been added into the list of acceptable NFs at Ingress Gateway.
OPCF-IGW-E122 **Error Type**: GRACEFUL_SHUTDOWN	This error code indicates that requests received at ingress-gateway were rejected gracefully during the ingress-gateway shutdown.	This indicates that the service or pod is shutting down, and the responses include error response.	Redeploy Ingress Gateway or prevent shutdown.
OPCF-IGW-E132 **Error Type**: GLOBAL_RATELIMIT	This error code indicates requests are being rejected after exceeding the burstCapacity when the global ratelimit feature is enabled.	Number of requests is exceeding the bucket size set in the configurations for Ingress Gateway, which is calculated on the basis of maxTokenRequest and burstCapacity.	Modify the globalIngressRateLimiting parameter of Gateway Services configurations to accommodate incoming requests.
OPCF-IGW-E152 **Error Type**: RSS_BASED_RATELIMIT	This error code indicates that requests are being rejected after exceeding the burstCapacity when the rss ratelimit feature is enabled.	When egressrateLimitingConfigMap is configured with burstCapacity and ratelimiting enabled, this exception is thrown when the requests count exceeds this burstCapacity and it is also based on the MNC and MCC values.	If this is an unexpected behavior, change the values or attributes in egressrateLimitingConfigMap.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-8 (Cont.) App Error Code Dictionary for Ingress Gateway

Application Error Code ID	Description	Cause	Action
OPCF-IGW-E162 **Error Type**: XFCC_HEADER_VALIDATION_FAILURE	This error code indicates that validation of the XFCC header failed at Ingress Gateway.	Indicates that the XFCC header in the request is in the correct format but is not validated as it is the wrong value for the request.	Verify if the right value is updated in the XFCC header based on the Ingress Gateway deployment configuration.
OPCF-IGW-E163 **Error Type**: XFCC_HEADER_NOT_PRESENT_OR_EMPTY	This error code indicates that a request received at Ingress Gateway has no XFCC header or an empty XFCC header.	XFCC Header is not present	Include the XFCC Header in the Request.
OPCF-IGW-E164 **Error Type**: XFCC_MATCHCERTCOUNT_GREATER_THAN_CERTS_IN_HEADER	This error code indicates that the XFCC header validation failed due to XFCC certificate count mismatch in Ingress Gateway.	Ingress Gateway configuration requires more certs than the number of certs sent in the request.	Check the number of certificates in the request sent and attach the certificates matching the configuration set for Ingress Gateway.
OPCF-IGW-E165 **Error Type**: XFCC_HEADER_INVALID	This error code indicates that an invalid XFCC header is received at Ingress Gateway.	XFCC Header present in the request is not of the right format.	Fix the XFCC Header of the request and send.
OPCF-IGW-E171 **Error Type**: OAUTH_TOKEN_VALIDATION_FAILURE	This error code indicates that validation of the OAuth token failed at Ingress Gateway.	The OAuth token passed with the request is enclosed with values that are incorrect with respect to the configuration present at Gateway Services.	Verify and include the OAuth token with the correct set of values related to the deployed Ingress Gateway config.
OPCF-IGW-E172 **Error Type**: OAUTH_CERT_EXPIRED	This error code indicates that the OAuth cert that has expired is received at Ingress Gateway.	Indicates that all the attributes are present and in the correct format, but the token has expired with respect to Ingress Gateway configuration.	Attach an OAuth token in the request, which has not expired.
OPCF-IGW-E173 **Error Type**: OAUTH_MISMATCH_IN_KID	This error code indicates that OAuth mismatch occurred in KID at Ingress Gateway.	Incorrect issuer and incorrect KID value is included in the request.	Check the issuer attribute and KID value passed in the request.
OPCF-IGW-E173 **Error Type**: OAUTH_MISMATCH_IN_ALGORITHM_FOR_KID	This error code indicates that the algorithm used while generating the token does not match the configured algorithm when the oauthValidationMode is "KID_ONLY".	The algorithm used while generating the token does not match the configured algorithm.	Check the issuer attribute and KID value passed in the request.
OPCF-IGW-E174 **Error Type**: OAUTH_PRODUCER_SCOPE_NOT_PRESENT	This error code indicates that producer scope is absent in the OAuth token received at Ingress Gateway.	Producer scope is absent in the token of the request.	Check for the producer scope value in the token used in the request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-8 (Cont.) App Error Code Dictionary for Ingress Gateway

Application Error Code ID	Description	Cause	Action
OPCF-IGW-E175 **Error Type**: OAUTH_PRODUCER_SCOPE_MISMATCH	This error code indicates that the producer scope present in the OAuth token mismatches with the producer scope configured at Ingress Gateway.	The producer scope sent through the token either has a wrong format, has been used incorrectly, or an incorrect value is present.	Verify the producer scope attribute of the token sent through the request.
OPCF-IGW-E176 **Error Type**: OAUTH_MISMATCH_IN_NRF_INSTANCEID	This error code indicates that the NRF instance ID present in the OAuth token mismatches with the NRF instance ID configured at Ingress Gateway.	A wrong issuer attribute is passed along with the access token.	Check the issue attribute attached along with the request.
OPCF-IGW-E176 **Error Type**: OAUTH_MISMATCH_IN_ALGORITHM	This error code indicates that the algorithm used while generating the token does not match the configured algorithm when the oauthValidationMode is "KID_PREFERRED" or "INSTANCEID_ONLY".	The algorithm used while generating the token does not match the configured algorithm.	Correct the algorithm used.
OPCF-IGW-E177 **Error Type**: OAUTH_PRODUCER_PLMNID_MISMATCH	This error code indicates that the received OAuth token mismatches with the producer PLMN configured at Ingress Gateway.	The configured PLMN ID in Ingress Gateway is not matching with the PLMN ID received through the OAuth token.	Correct the PLMN ID in the configuration for Ingress Gateway or correct the ID in the OAuth token.
OPCF-IGW-E178 **Error Type**: OAUTH_AUDIENCE_NOT_PRESENT_OR_INVALID	This error code indicates that the received OAuth token does not contain an audience or an invalid audience at Ingress Gateway.	The token is passed with the Audience parameter containing only correct nfType but in a different case. An Audience parameter with missing or wrong values for NfType and NfInstanceId can also raise this error.	Verify and include the correct NfType or NfInstanceID in the request.
OPCF-IGW-E179 **Error Type**: OAUTH_TOKEN_INVALID	This error code indicates that an invalid OAuth token is received at Ingress Gateway.	Indicates that the OAuth token received at Ingress Gateway is not valid, that is, not in the correct format.	Verify if the OAuth token is in the right format and configured with the right set of values with respect to the configuration at Gateway Services.
OPCF-IGW-E180 **Error Type**: OAUTH_TOKEN_ABSENCE	This error code indicates that a request was received at Ingress Gateway with no OAuth token or an empty OAuth token.	The OAuth Token is missing in the request.	Include the OAuth token in the request.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-8 (Cont.) App Error Code Dictionary for Ingress Gateway

Application Error Code ID	Description	Cause	Action
OPCF-IGW- E182 **Error Type**: IGW_OVERLOAD_CONTROL_EXCEPTION	This error code indicates that overload control exception occurred at Ingress Gateway.	Occurs when the OverloadControl feature is enabled and configured at the requests per second being sent.	Modify the configuration for acceptable requests per second.
OPCF-IGW-E183 **Error Type**: RESPONSE_STATUS_EXCEPTION	This error code indicates that ResponseStatusException was created by Spring boot as Ingress Gateway exception handler was unable to handle an exception.	NA	NA
OPCF-IGW-E184 **Error Type**: NO_RESOURCE_FOUND_EXCEPTION	This error code indicates that no route is configured for the requested URI.	The invalid request URI or missing route configuration for the required route.	Update the request URI or routesConfiguration.
OPCF-IGW-E191 **Error Type**: CCA_HEADER_VALIDATION_FAILURE	This error code indicates that validation of the CCA header failed at Ingress Gateway.	The CCA header sent through the request failed while validation.	Include the correct value for the CCA header in the request.
OPCF-IGW-E192 **Error Type**: PARTIAL_SHUTDOWN	This error code indicates that requests are being discarded partially at Ingress Gateway when the control shutdown feature is enabled.	This behavior is observed when ControlledShutdown is enabled.	Disable ControlledShutdown.
OPCF-IGW-E193 **Error Type**: COMPLETE_SHUTDOWN	This error code indicates that requests are being discarded at Ingress Gateway when the control shutdown feature is enabled.	This behavior is observed when ControlledShutdown is enabled.	Disable ControlledShutdown.
OPCF-IGW-E201 **Error Type**: IGW_OVERLOAD_CONTROL_PERCENTAGE_DISCARD	This error code indicates that requests are being rejected when the load level matches the configured percentage in the discard policy mapping of the overload control feature.	The number of requests has reached the configured percentage for OverloadControl. When this value is reached, the respective Error Code is displayed.	Change the percentage value to accommodate more requests and not to display the error code.
OPCF-IGW-E202 **Error Type**: IGW_OVERLOAD_CONTROL_PRIORITY_DISCARD	This error code indicates that requests with the sbi-priority header with value greater than the configured value of the discarded load level match the discard policy mapping of the overload control feature.	The number of requests has reached the configured priority for OverloadControl. When this value is reached, the respective Error Code is displayed.	Change the priority value to accommodate more requests and not to display the error code.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-8 (Cont.) App Error Code Dictionary for Ingress Gateway

Application Error Code ID	Description	Cause	Action
OPCF-IGW-E211 **Error Type**: IGW_ROUTE_RATELIMITER_PRIORITY_DISCARD	This error code indicates that requests are being rejected when the priority level matches with the configured priority in the discard policy mapping of the route-level ratelimiting feature.	Request is rejected because the priority level set in the SBI header is greater than the configured priority in the route-level rate limiting and discard policy mapping.	Increase the Priority in discard policy mapping for route-level rate limiting, so requests with higher priority are accepted.
OPCF-IGW-E220 **Error Type**: IGW_PLMN_EGRESS_RATELIMIT	This error code indicates that requests are being rejected after exceeding the burstCapacity when the PLMN Egress Rate Limit feature is enabled.	When egressrateLimitingConfigMap is configured with burstCapacity and ratelimiting enabled, this exception is thrown when the requests count exceeds this burstCapacity and it is also based on the MNC and MCC values.	If this is an unexpected behavior, change the values or attributes in egressrateLimitingConfigMap.
OPCF-IGW-E221 **Error Type**: INVALID_ROUTE_EXCEPTION	This error code indicates that an invalid route exception has occurred as invalidRouteFilter was configured in the routesConfiguration.	Invalid Route Exception is a filter enabled at the route-level in routesConfig.	If this is an unexpected behavior, check the path if that is the expected path that was supposed to be marked as an invalid route.
OPCF-IGW-E223 **Error Type**: OAUTH_ALGORITHM_INVALID	This error code indicates that the algorithm used while generating the token is invalid.	The algorithm used while generating the token is invalid.	Provide a valid algorithm while generating the token.

Table D-9 Error Code Dictionary for NRF Client

App Error Id	Description	Cause	Action
OPCF-NCMGMT-E502	NRF client generates 400 Error code with cause "BAD REQUEST" and "OPCF-NCMGMT-E502" as App Error ID.	UDR SUSPENSION status change notification is with wrong version as "apiVersionInUri": "v1.0".	Send UDR SUSPENSION status change notification with wrong version as "apiVersionInUri": "v1.0".
OPCF-NCMGMT-E033	NRF client generates 400 Error code with cause "BAD REQUEST" and "OPCF-NCMGMT-E033" as App Error ID.	UDR SUSPENSION status change notification without any event as "event": "" .	Send UDR SUSPENSION status change notification without any event as "event": "" .

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-10 Error Cause Diameter Connector to SM service

Diameter Error Name	Diameter Result Code	Response Body 'Cause' from Diameter Connector to SM
DIAMETER_UNABLE_TO_COMPLY	5012	An internal failure occurred.
DIAMETER_UNKNOWN_SESSION_ID	5002	A request is received with unknown session ID.
DIAMETER_UNABLE_TO_DELIVER	3002	Request did not delivered to the destination.
DIAMETER_TOO_BUSY	3004	An upstream peer is either in congestion or too busy to handle a request.
DIAMETER_MISSING_AVP	5005	The request did not contain an AVP that is required by the Command Code definition.
DIAMETER_COMMAND_UNSUPPORTED	3001	The Request contained a Command-Code that the receiver did not recognize or support.
DIAMETER_LOOP_DETECTED	3005	An agent detected a loop while trying to get the message to the intended recipient.
DIAMETER_UNSUPPORTED_VERSION	5011	A request was received, whose version number is unsupported.
DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	5009	A message was received that included an AVP that appeared more often than permitted in the message definition.
DIAMETER_AVP_UNSUPPORTED	5001	The peer received a message that contained an AVP that is not recognized or supported and was marked with the Mandatory bit.
DIAMETER_INVALID_AVP_VALUE	5004	The request contained an AVP with an invalid value in its data portion.
DIAMETER_INVALID_AVP_LENGTH	5014	The request contained an AVP with an invalid length.
DIAMETER_INVALID_HDR_BITS	3008	A request was received whose bits in the Diameter header were either set to an invalid combination, or to a value that is inconsistent with the command code definition.
DIAMETER_INVALID_AVP_BITS	3009	A request was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the AVP definition.

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-11 Diameter Result Codes from TDF toward SM service

Diameter Result Code	HTTP Response Code	Diameter Connector Response Body
DIAMETER_SUCCESS	200	No response body
DIAMETER_MISSING_AVP / DIAMETER_UNABLE_TO_COMPLY / DIAMETER_UNABLE_TO_DELIVER / DIAMETER_TOO_BUSY / DIAMETER_LOOP_DETECTED/ DIAMETER_APPLICATION_UNSUPPORTED	500	{ "type": null, "title": "INTERNAL_SERVER_ERROR", "status": 500, "detail": "Error Occurred", "instance": null, "cause": "<Mapping of Diameter Result Code with Cause is provided in below table>", "invalidParams": null }
DIAMETER_UNKNOWN_SESSION_ID	404	{ "type": null, "title": "NOT_FOUND", "status": 404, "detail": "Session Does not Exist", "instance": null, "cause": "A request is received with unknown session ID.", "invalidParams": null }

Table D-12 HTTP Result Codes from SM service toward TDF

HTTP Response Code	Diameter Result Code
204/200	DIAMETER_SUCCESS
500	DIAMETER_UNABLE_TO_COMPLY
503	DIAMETER_UNABLE_TO_COMPLY
400	DIAMETER_UNABLE_TO_COMPLY

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-12 (Cont.) HTTP Result Codes from SM service toward TDF

HTTP Response Code	Diameter Result Code
404	DIAMETER_UNKNOWN_SESSION_ID

Table D-13 Cause Codes

Error Cause	Code
UNKNOWN	00000
USER_UNKNOWN	00001
INVALID_API	00002
INVALID_MSG_FORMAT	00003
INVALID_QUERY_PARAM	00004
MANDATORY_QUERY_PARAM_INCORRECT	00005
OPTIONAL_QUERY_PARAM_INCORRECT	00006
MANDATORY_QUERY_PARAM_MISSING	00007
MANDATORY_IE_INCORRECT	00008
OPTIONAL_IE_INCORRECT	00009
MANDATORY_IE_MISSING	00010
UNSPECIFIED_MSG_FAILURE	00011
PCC_RULE_EVENT	00012
UE_STATUS_SUSPEND	00013
RULE_TEMPORARY_ERROR	00014
PCC_QOS_FLOW_EVENT	00015
NO_AVAILABLE_POLICY_COUNTERS	00016
UNKNOWN_POLICY_COUNTERS	00017
ERROR_REQUEST_PARAMETERS	00018
PENDING_TRANSACTION	00019
ERROR_TRIGGER_EVENT	00020
WWW_AUTHENTICATE	00021
POLICY_CONTEXT_DENIED	00022
LATE_OVERLAPPING_REQUEST	00023
UPDATE_NOT_ALLOWED	00024
SUBSCRIPTION_NOT_FOUND	00025
USER_NOT_FOUND	00026
DATA_NOT_FOUND	00027
RESOURCE_URI_STRUCTURE_NOT_FOUND	00028
METHOD_NOT_ALLOWED	00029
NOT_ACCEPTABLE	00030
CONFLICT	00031
GONE	00032
LENGTH_REQUIRED	00033
PRECONDITION_FAILED	00034
PAYLOAD_TOO_LARGE	00035
URI_TOO_LONG	00036

Copyright © 2019, 2026, Oracle and/or its affiliates.

Table D-13 (Cont.) Cause Codes

Error Cause	Code
UNSUPPORTED_MEDIA_TYPE	00037
INSUFFICIENT_RESOURCES	00038
UNSPECIFIED_NF_FAILURE	00039
SYSTEM_FAILURE	00040
NF_FAILOVER	00041
DATABASE_INCONSISTENCY	00042
UNSUPPORTED_MONITORED_URI	00043
NF_CONGESTION	00044
NF_CONGESTION_RISK	00045
INCORRECT_LENGTH	00046
GATEWAY_TIMEOUT	00047
ERROR_INITIAL_PARAMETERS	00048
BULWARK_SERVICE_ERROR	00049
OPTIONAL_IE_MISSING	00050
INVALID_MESSAGE_FORMAT	00051
APP_IN_CONGESTION_STATE	00052
CONTEXT_NOT_FOUND	00053
BULWARK_ALREADY_LOCKED	00054
BULWARK_SERVICE_UNREACHABLE	00055
INTERNAL_SERVER_ERROR	00056
BAD_REQUEST	00057
UNAUTHORIZED	00058
FORBIDDEN	00059
NOT_FOUND	00060
REQUEST_TIMEOUT	00061
TOO_MANY_REQUESTS	00062
ERROR_4XX	00063
SERVICE_UNAVAILABLE	00064
ERROR_5XX	00065
BINDING_SERVICE_ERROR	00066
INSUFFICIENT_RESOURCES_SLICE	00067
REQUESTED_SERVICE_TEMPORARILY_NOT_AUTHORIZED	00068
TIMED_OUT_REQUEST	00069

Copyright © 2019, 2026, Oracle and/or its affiliates.