Oracle® Communications

Cloud Native Core Policy User's Guide

Release 1.8.0

F34710-03

December 2020

Oracle Communications Cloud Native Core Policy User's Guide, Release 1.8.0

F34710-03

Contents

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 below 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.

What's New in This Guide

New/Updated Features in Release 1.8.0

- Updated the Managing Policy Tables section to support policy table enhancements.
- Added the Managing Retry Profiles section to support session retry functionality. This section also talks about DNS-SRV records.
- Updated the Bulk Export/Bulk Import section to support bulk import/export enhancements.
- Updated the Managing Subscriber Logging section
- Added the Support for Spending Limit Pending Counter section to support spending limit pending counter functionality
- Added the About Binding Service section. This section talks about the Binding Service.
- Updated the General Configurations section to add PRE related configurations
- Updated the Cloud Native Core Policy Metrics chapter to add metrics related to Binding Service and Diameter Gateway. And, few new metrics related to User Service has been added in this chapter.
- A new configuration parameter, **Enable Operator Specific Data Query**, has been added in the Configuring PCF Session Management Service section to support nudr to support operator specific data.

1
Introduction

This document provides information on how to configure the Cloud Native Core Policy services and managed objects using REST API.

Overview

Oracle Communications Cloud Native Core Policy (CNC Policy) solution provides a standard policy design experience and ultimately consistent end-user experience. The Converged policy solution supports both 4G and 5G networks. In addition, the overlap in functionality between PCF and PCRF (for example, need for a policy engine, policy design, Rx, similarity between Sy and Nchf_SpendingLimitControl, etc.), enables us to build micro-services that can be used to provide PCRF and PCF functionality. Even though it is a unified policy solution, you can still deploy the PCF and PCRF entirely independently.

The CNC Policy is a functional element for policy control decision and flows based charging control functionalities. The CNC Policy provides 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)
- Provide UE Route Selection Policies (URSP) rules to UE via AMF
- Accesses subscription information relevant for policy decisions in a Unified Data Repository (UDR)
- Provides network control regarding the service data flow detection, gating, QoS and flow based charging towards the Policy and Charging Enforcement Function (PCEF).
- Receives session and media related information from the AF and informs AF of traffic plane events.
- Provisions PCC Rules to the PCEF via the Gx reference point.

The CNC Policy supports the above functions through the following services:

- Session Management Service
- Access and Mobility Service
- Policy Authorization Service
- User Equipment (UE) Policy Service
- PCRF Core Service

Acronyms and Terminology

The following table provides information about the acronyms and the terminology used in the document.

Table 1-1 Acronyms and Terminology

Acronym	Definition
AMF	Access and Mobility Management Function
BSF	Binding Support Function
CHF	Charging Function
CM	Configuration Management
CUSTOMER_REPO	Docker registry address including the port number, if the docker registry has an associated port.
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.
MCC	Mobile Country code
METALLB_ADDRESS_POOL	Address pool which configured on metallb to provide external IPs .
MNC	Mobile Network code
NRF	Network Repository Function
PCF	Policy Control Function
CNPCRF	Cloud Native Policy and Charging Rules Function
SAN	Storage Area Network
SMF	Session Management Function
UDR	Unified Data Repository

References

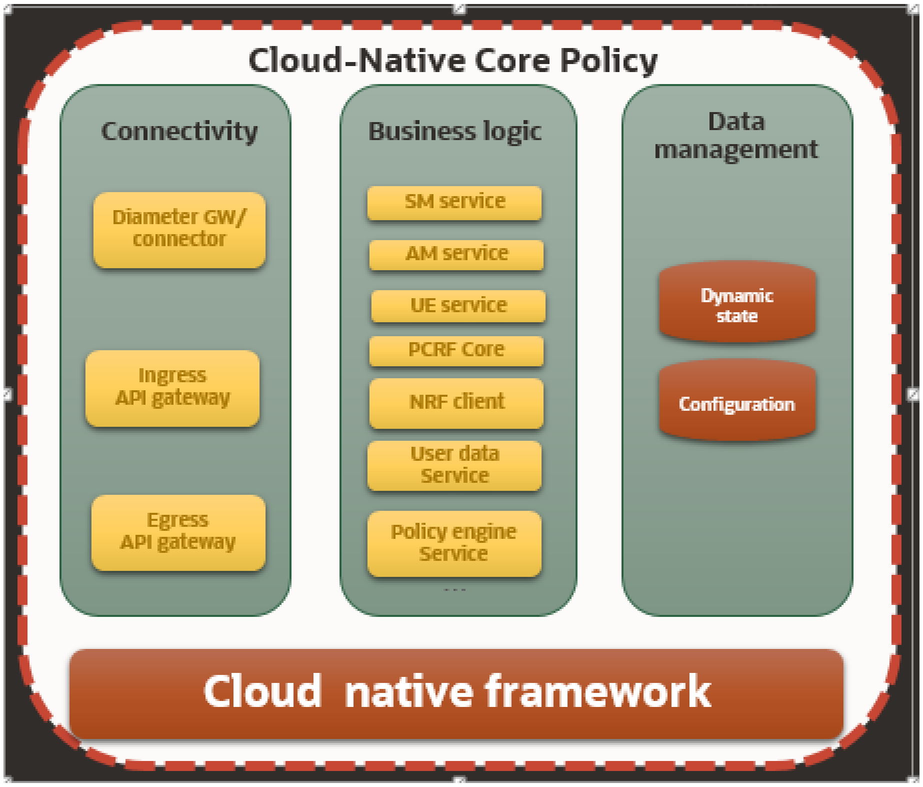
You can refer to the following documents for information.

- Oracle Communications Cloud Native Policy Control Function Installation Guide
- 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

2
Cloud Native Core Policy Architecture

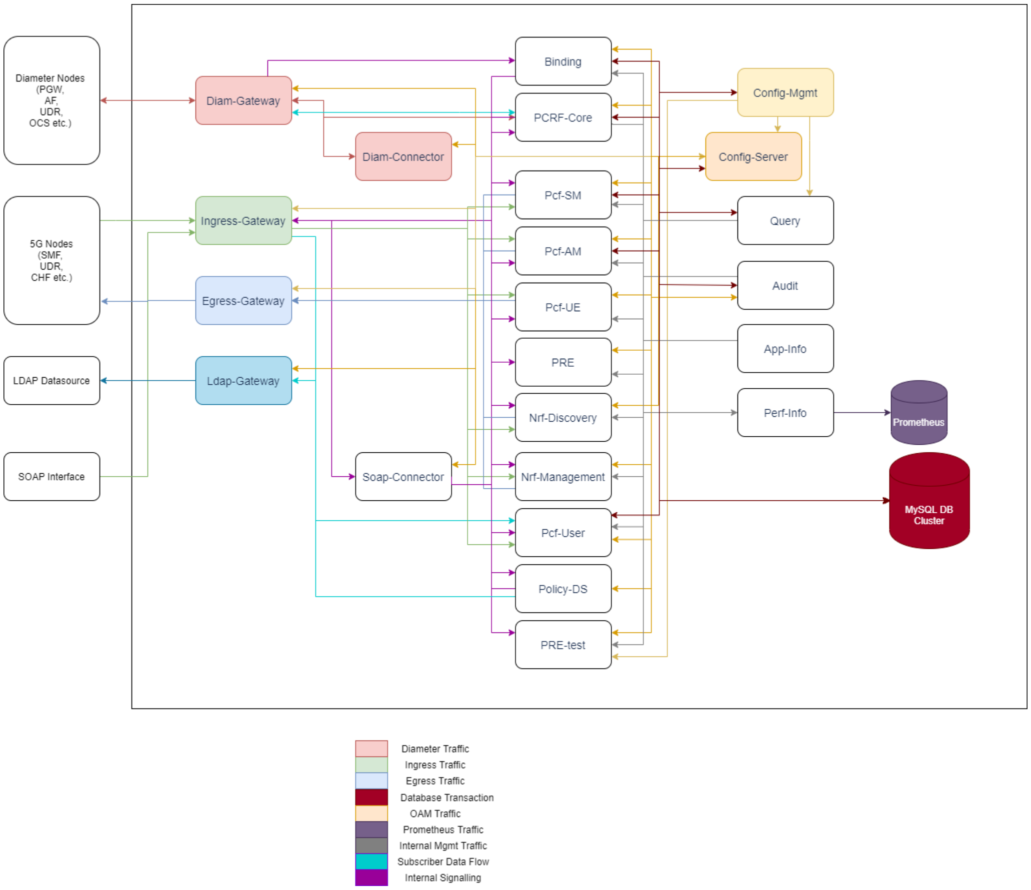
The Oracle Communications Cloud Native Core Policy is built as a cloud-native application composed of a collection of microservices running in a cloud-native environment. It separates processing/business logic and state concerns following the corresponding logical grouping of microservices/components:

- **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/PCF business logic, policy engine and various services that can be enabled based on deployment needs. These are stateless sets of components.
- **Data Management**: Data layer responsible for storing various types of persistent data. The PCF is built to be able to plug in different types of backend data layers that could be internal or external.



As a result, an actual policy function can be composed of the necessary micro-services to provide the desired service, For Example, PCF, PCF/PCRF, a subset of a PCF (For Example, one without usage monitoring, etc.).

Oracle Communication Cloud Native Core Policy solution takes the policy designing experience to the next level by providing ultimate flexibility, extensibility, modularization to rapidly and securely deploy new policies supporting different and 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 interworking and migration between 4G and 5G. Below is the Cloud Native Core Policy architecture diagram:



Components of the CNC Policy Architecture:

- Kubernetes cluster hosting Docker containers and Calico networking
- Standard CNE services to support operation of the PCF
- Cloud Native Core Policy Application Services
  - API GW (HTTP/2) – API Gateway service offers single entry to all HTTP/2 traffic to access policy services. The API gateway also plays a crucial role in traffic distribution, overload control and related ingress/egress services.
  - Diameter Gateway/Connector – Enables the policy solution functions as a diameter server and offers integration over Gx, Rx, Sh, Sy and other legacy diameter services. Diameter server is also implements routing, load balancing and overload control services. Diameter Gateway acts as a gateway for all diameter traffic to Policy Solution. It also performs Round Robin load balancing across its backend peers (diameter connector and PCRF-Core).
  - Ingress Gateway acts as a Gateway for all ingress HTTP traffic to Policy Solution.
  - Egress Gateway acts as a gateway for all egress 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 DS for processing.
  - NRF Client Service, along with application info and performance info services, integrates with external NRF for service registration, discovery, and service status/ load related information. NRF discovery helps in on-demand discovery of network functions. NRF management helps in autonomous discovery of network functions.
- Cloud Native Core Policy Business Logic
  - SM Service (includes PA Service) - Provides the SMF session and application/ flow based policies. The policy authorization service (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 N7 interface to trigger session management policies towards SMF function.
  - AM Service - Implements access management service-related policies over N15 interface towards the Access and Mobility Management Function (AMF).
  - PCRF Core Service – Implements the legacy handling of PCRF core business logic, interactions with other micro-services, and triggers for policy enforcement over the Gx interface. Policy and Charging Rules Function (PCRF) is a node which functions in real-time to determine policy rules in a multimedia network.
  - Binding Service - Stores binding information related to 4G/5G subscribers and aid Diameter Gateway in forwarding AF messages.
  - UE Policy Service - Provides UE policy, including Access Network Discovery and Selection Policy (ANDSP) and UE Route Selection Policy (URSP) via the AMF transparently to the UE.Implements UE management service-related policies over N15 interface towards the AMF.
  - User Service - This service is an evolution of the 4G UDR/SPR where the PCF is able to retrieve, update, subscribe, and get notified to changes. The service implements integration with all external data sources including 5G UDR, CHF, LDAP Server, 4G Sh and Sy interfaces. SM Service, AM Service and UE service talks to PCF-User service for UDR and CHF information.
  - Policy Data Service- Interfaces 4G/5G Signalling components with protocol specific connectors to have a unified datastructure which is understandable by both 4G and 5G Components.
  - Policy Engine – Implements the policy defined business logic to perform all network policy behaviors and actions. The policies can be configured using the config management service.
  - The PRE Test Engine runs the Policy Decision Engine for test messages. Test messaged can be triggered from the config management service.
  - Configuration Management - This service provides OAM interfaces (GUI and REST) 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 abstracts the database for storage and retrieval of policy configuration.
  - Query - The Query micro service processes session viewer queries triggered from configuration management service.
  - Audit - Audit micro service runs the Audit engine to detect and process stale session records.
  - App-Info - This micro service monitors application (micro-service) health and status.
  - Perf-Info - This micro service monitors application (micro-service) capacity and load status.

- Data Tier
  - Dynamic state – Store session information relevant for policy context.
  - Configuration store – Stores configuration related data

3 About Cloud Native Core Policy Services

About Session Management Service

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

Session Management Service supports the following:

- Enforcement control of policy decisions related to QoS, charging, gating, service flow detection, packet routing and forwarding, 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.

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

Table 3-1 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

Table 3-1 (Cont.) Session Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
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
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

About Access and Mobility Management Service

Oracle PCF implements access management service-related policies over N15 interface towards the Access and Mobility Management Function (AMF).

Access and Mobility Management Service supports the following:

- Enforcement control of policy decisions related to Radio Access Technology (RAT)/Frequency Selection Priority
- Enforcement of Service Area Restrictions is executed in the UE
- Enable location tracking for a UE to get periodic updates on subscriber current location

Oracle Communications PCF supports the following 3GPP defined services for Access and Mobility Management:

Table 3-2 Access and Mobility Management 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

Table 3-2 (Cont.) Access and Mobility Management Services

Service Operation Name	Description	Initiated By	Resource URI	HTTP Method
Npcf_AMPolicyControl_Update	Updates of 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
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

About Policy Authorization Service

Oracle Communications Policy Control Function (PCF) implements policy authorization service that authorizes an Application Function (AF) request over N5 interface.

Policy Authorization Service supports the following:

- Creates policies as requested by AF for the Protocol 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 3-3 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
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

About UE Management Service

Oracle PCF implements User Equipment (UE) management service-related policies over N15 interface towards the AMF.

UE Management Service supports the following:

- Transfer of UE Route Selection Policies (URSP) rules to UE
- Establish the UE Policy Association requested by the NF service consumer
- Define and deliver URSP message to UE via AMF using N1N2 message

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

Table 3-4 UE Management 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_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 a previously created subscription for N1 Message Transfer	AMF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages/subscriptions/{subscriptionId}	DELETE
N1N2MessageTransfer	Transfer an N1 message (NAS message) that is to be delivered to the UE	AMF	{apiRoot}/namf-comm/<apiVersion>/ue-contexts/{ueContextId}/n1-n2-messages	POST
N1MessageNotify	Indicate status of an N1 Message Transfer	PCF	{Notification URI}	POST

About PCRF Core Service

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 the PCEF to the PCRF.

PCRF Core Service supports the following:

- IP-CAN session Establishment, Modification and Termination Support
- Install/Modify/Remove Predefined PCC rules
- Install/Modify/Remove Dynamic PCC rules
- Gate function
- Charging-related Information Support
- Integration with AF (over Rx)
- Presence Area Reporting Support
- Time of the day procedures
- Sponsored Data Connectivity Support
- NSA related enhancements for QoS

About Binding Service

Binding service stores binding information related to 4G/5G subscribers and aid Diameter Gateway in forwarding Application Function (AF) requests. It also queries Network Repository Function (NRF) client for fetching 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 CNC Policy, Diameter Gateway should have a converged mode, where

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

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 will forward either to PCRF-Core or SM Service (via. Diameter Connector)

Configuration

In Helm Charts you need to configure **diamgateway.envGatewayMode** as **converged** in custom-values.yaml file, and the child helm files for Diameter-Gateway, Query-Service etc 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 Guide*.

Depending on the value of the following parameters, binding service or BSF is queried:

- **bindingEnable** in custom-values.yaml file
- **Binding Operation** in CNC Console GUI

Behaviour is as follows:

- When both the configuration variables are set to true, binding service is queried.

- When the **bindingEnable** parameter is set to true and the **Binding Operation** is configured to false, BSF is queried.
- When the **bindingEnable** parameter is set to false and the **Binding Operation** is configured to true, neither BSF nor binding service is queried.
- When both the configuration variables are set to false, neither BSF nor binding service is queried.

Binding Service Truth table when receiving AAR-I Following truth table will be considered by Binding Service for finding the context owner of a session.

Priority : Priority indicates that attributes if specified in the message will be 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 will be considered and corresponding context-owner information will be returned otherwise next attribute priority will be considered.

- IPv6
- IPv4 + APN/DNN+SNSSAI
- IPv4
- IMSI
- MSISDN

Table 3-5 Binding Service Truth table when receiving AAR-I

S.No.	Message	IPv6	IPv4	APN/DNN+SNSSAI	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+SNSSAI) + 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

Table 3-5   (Cont.) Binding Service Truth table when receiving AAR-I

S.No.	Message	IPv6	IPv4	APN/ DNN+SNSSAI	IP Domain ID	GPSI/ MSISDN	SUPI/ IMSI	Binding Lookup Query
	AAR - I		P			P	P	considered)
4	Gx-CCRI/SM Association	P	P	P		P	P	IPv4 + APN/ (DNN+SNSSAI) + 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			

Binding Service Truth table when receiving AAR-U

Table 3-6   Binding Service Truth table when receiving AAR-U

S.No.	Message	IPv6/IPv4	APN/ DNN+SNSAAI	Session ID	Binding Lookup Query
1	AAR-U	P	P	P	Session-ID
2	AAR-U	P	P	P	IP Address + APN/ DNN+SNSSAI (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:

1. IP-CAN-Session Not available, when there is no suitable binding found in the binding service
2. UNABLE-TO-COMPLY, when request times out at Diameter Gateway

4

Integrating Cloud Native Core Policy with Different Network Functions

You can integrate the Cloud Native Core Policy with NRF, UDR, and CHF Network Functions.

NRF Integration

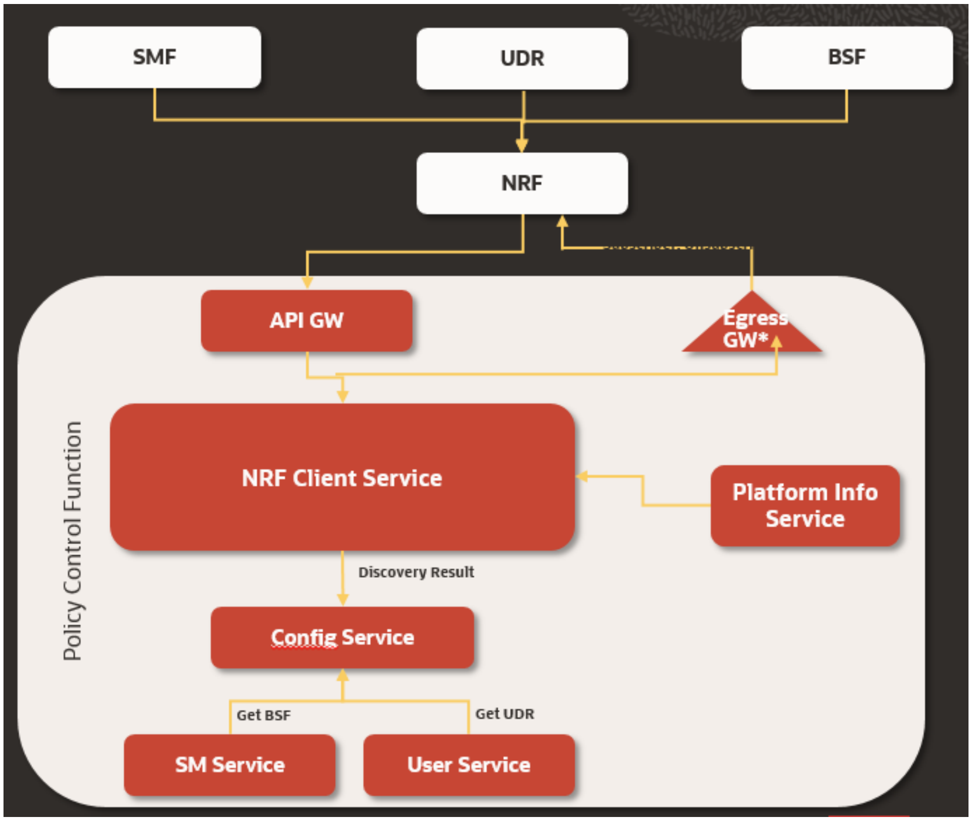
NRF Management (Client) service enables policy solution to integrate with NRF server for service registration, discovery, and service status/ load related information

Management Service support includes

- Register Service
- Deregister Service
- PCF heartbeat to NRF that includes load, priority and capacity information
- Knowledge to NRF of scaling change
- Subscribe/Un-subscribe

Discovery Service

- Used to discover UDR, BSF and CHF services
- Compliant with 29.510



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 Guide*.

1. Get a list of all the config maps in the PCF deployment namespace by entering this command:

   ```
   kubectl get cm -n pcf-namespace
   ```

   where, *pcf-namespace* is the PCF deployment namespace used by helm command.
2. Edit the application configuration map by entering this command:

   ```
   kubectl edit cm pcf-name-application-config -n pcf-namespace
   ```

   where, *pcf-name* is the release name used by 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.
3. Verify the NRF address (fqdn/IP) and the port number. NRF address is contained in the custom value yaml file. See attribute "configmapApplicationConfig" in the custom yaml file.

4. Check and add necessary NFs to "nrfClientSubscribeTypes". These NFs will be discovered and subscribed by PCF at the startup time. Leave this field empty if this onetime discovery and subscription for NFs is not required.
5. Check and edit, as necessary, the PCF Profile to be registered with the NRF. For example, if required enter the IP details of the PCF Services.
6. Save and exit the editor.

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 Sy, 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 (i.e., notifications of policy counter status changes).
  - Dynamic discovery of CHF from NRF
  - Support for policy counter retrieval, 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
- Usage Monitoring Data
- Policy Data Subscriptions
- Individual Policy Data Subscription
- Compliant with 29.519 V15.2.0

5 Configuring Cloud Native Core Policy

This section provides the information for configuring Oracle Communications Cloud Native Core Policy (CNC Policy) for various services.

CNC Policy offers the following interfaces to configure the CNC Policy solution:

- A web-browser based Graphical User Interface
- A REST API based Machine-to-Machine interface
- Kubernetes Configuration Maps (This configuration map is used to register PCF with NRF. For more information, see Integrating Cloud Native Core Policy with Different Network Functions

For more information on configurations using GUI, see Configuring Cloud Native Core Policy Using Cloud Native Core Console.

For REST API information, please refer *Oracle Communications Cloud Native Core Policy REST Specification Document*.

Configuring PCRF-Core Host in Config Map

To Configure PCRF-Core host in config map:

1. Edit the "ocpm-diam-gateway-config-peers" config map by executing the following command: `kubectl edit configmap ocpm-diam-gateway-config-peers -n <namespace>`
2. In the configmap, configure the pcrf-core host with the headless service name of pcrf-core.

   For Example,
   Configmap:

```
nodes:
      - name: 'pcrf-core'
        type: 'pcrf'
        responseOnly: true
        host: "ocpcrf-pcrf-core"
        port: 3868
        realm: ''
        identity: ''
```

   PCRF-Core Service Name:

```
NAME                      TYPE          CLUSTER-IP       EXTERNAL-
IP    PORT(S)
AGE
ocpcrf-pcrf-core                   ClusterIP
None            <none>        3868/TCP,5809/
TCP,9000/TCP                                    65m
```

```
ocpcrf-pcrf-core-service           NodePort
10.233.39.230   <none>        3868:31787/TCP,9080:31463/
TCP,5809:30513/TCP,9000:32401/TCP   65m
```

6
Configuring Cloud Native Core Policy Using Cloud Native Core Console

This chapter describes how to configure different services in Oracle Communications CNC Policy and how to create policies and manageable objects in CNC Policy using Oracle Communications Cloud Native Core Console.

Cloud Native Core Console Interface

This section provides an overview of the Oracle Communications Cloud Native Core (CNC) Console, which includes a interface to aid in creating policies and manageable objects in CNC Policy.

You use CNC Policy integrated with CNC Console only after logging successfully into the CNC Console application. To login successfully into the CNC Console, you need to make the following updates to the hosts file available at the **C:\Windows\System32\drivers\etc** location.

In the Windows system, user needs to open the **hosts** file in the notepad as an Administrator and append the following set of lines at the end:

Example:

```
10.75.212.88 cncc-iam-ingress-gateway.cncc.svc.cluster.local
```

```
10.75.212.88 cncc-core-ingress-gateway.cncc.svc.cluster.local
```

> **Note:**
>
> The IP Address in the above lines may change when deployment cluster changes.

Save and close the notepad.

> **Note:**
>
> Before logging into CNC Console, it is important to create a CNC user and password. Using this user details, you can login to the CNC Console application. For information on creating a CNC Console user and password, see *Oracle Communications Cloud Native Core Console Installation Guide*.

To login to CNC Console :

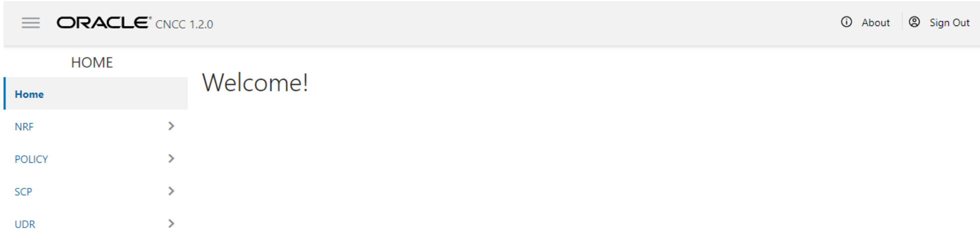
1. Open a web browser and enter the URL: http://*host name*:*port number* and press Enter.
   The login page opens.

where, *host name* is cncc-iam-ingress-ip and *port number* is cncc-iam-ingress-port

.

2. Enter your **Username**.
3. Enter your **Password**.
4. Click **Login**.
   Tha main page opens.

Figure 6-1 CNC Console Interface



This is the CNC Console Home Page from where you can navigate to different NF services. All the Policy related configurations are available in the left navigation menu under **Policy**.

Session Viewer

The Session Viewer displays detailed session information for a specific subscriber. Within the session viewer, you can enter query parameters to render session data for a specific subscriber. This section provides information about viewing the sessions.

To view the sessions:

1. From the navigation menu, under **Policy**, click **Session Viewer**. The Session Viewer page appears.
2. From the **Session Type** drop-down menu, select the service whose sessions you want to view. Possible values are:
   - SM Policy Association
   - AM Policy Association
   - PA Policy Association
   - PCRF-Core Session
   - Binding Session
3. a. From the **Identifier Type** drop-down menu, select the identifier type for the selected session type. Possible values for **SM Policy Association**, **AM Policy Association**, **PA Policy Association**, and**Binding Session** are:
      - SUPI
      - GPSI
      - IPV4

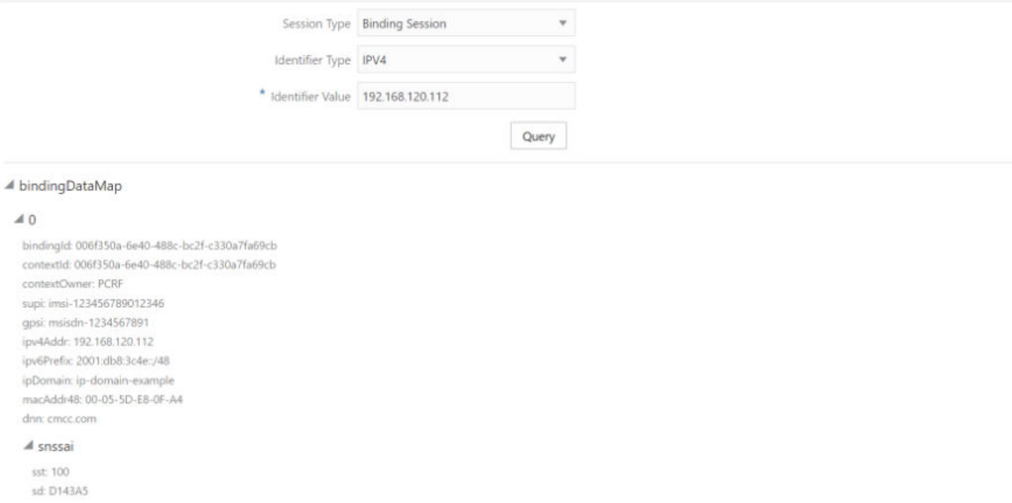
    - IPV6
    - POLICY_ASSOC_ID
    - MAC

    > **Note:**
    >
    > AM Policy Association and PA Policy Association fetches session data using **POLICY_ASSOC_ID** (Session ID) only.

  b. From the **Identifier Type** drop-down menu, select the identifier type for the selected session type. Possible values for **PCRF-Core Session** are:
    - DIAMETER_SESSION_ID
    - IMSI
    - MSISDN
    - IPV4
    - IPV6

4. Enter the value in the **Identifier Value** field for the selected identifier type.
5. Click **Query**. Information about the subscriber session(s) is displayed.

Following screen capture is an example of Query result:



Session Type: Binding Session

Identifier Type: IPV4

* Identifier Value: 192.168.120.112

bindingDataMap

0

bindingId: 006f350a-6e40-488c-bc2f-c330a7fa69cb
contextId: 006f350a-6e40-488c-bc2f-c330a7fa69cb
contextOwner: PCRF
supi: imsi-123456789012346
gpsi: msisdn-1234567891
ipv4Addr: 192.168.120.112
ipv6Prefix: 2001:db8:3c4e::/48
ipDomain: ip-domain-example
macAddr48: 00-05-5D-E8-0F-A4
dnn: cmcc.com

snssai

sst: 100
sd: D143A5

If session data is not available, the error is displayed along with No session found.

General Configurations

You can manage and view the General Configurations from this page.

To edit the General Configurations:

1. From the navigation menu, under **Policy**, click **General Configurations**.
   The General Configurations screen appears.
2. Click **Edit** to edit the general configurations.
3. Enter the following information:

- **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.
- **API Gateway Host**- The name of the API gateway host. This field is not used.
- **API Gateway Port**- The port number of the API gateway (if a port other than the default is being used). The default value is 80. This field is not used.
- **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

4. Click **Save**.

Service Configurations

You can tailor the Policy services as per network operator's requirements using the Service configuration pages. The configurations include setting up end point addresses, setting up log levels and other debug information like tracing etc. and customizing and/or optimizing NF interactions for example with UDR etc.

> **Note:**
>
> - The **NAS Message Maximum Packet Size** field is not supported in this release of PCF and will not take effect.
> - The **Validate User** and **Query User** fields must always be set to **false** in this release of PCF.

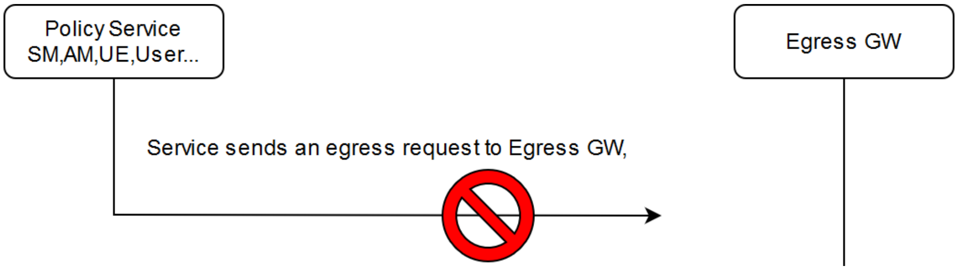
Managing Retry Profiles

This chapter describes how to create and manage retry profiles in the CNCPolicy system.

A retry profile specifies when and how the signaling message from one network function to another are retried and/or rerouted on failures. For example, if heartbeat messages that PCF send to NRF fail consistently, the PCF should choose a different (secondary/next priority) NRF that is available to send the subsequent heartbeat messages. Similar retry/reroute mechanisms are required for messages going towards UDR, CHF etc. Even the notifications to SMF may need to be retried and/or rerouted based on the configuration.

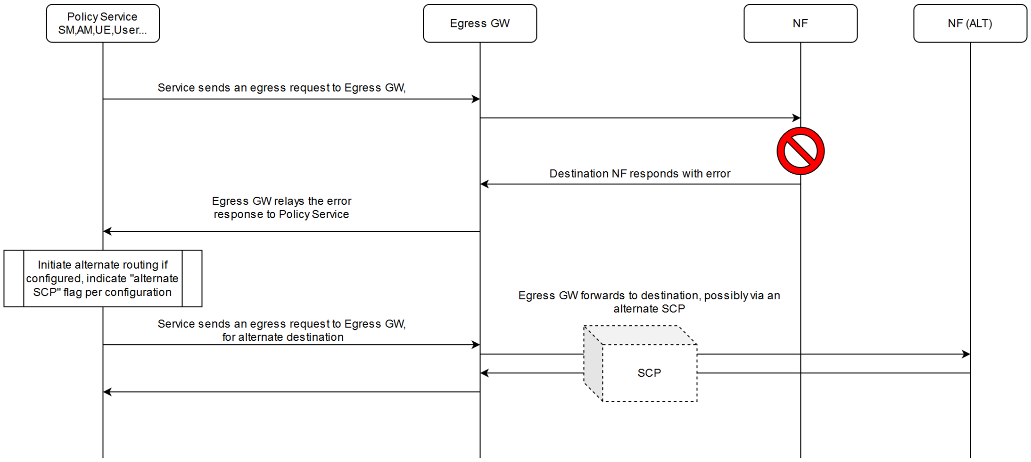
Retry: Retry is initiated when the Policy Control Function (PCF) microservices initiates an egress request but, it fails to reach the egress gateway. The reason can be connection failure or Aspen Service Mesh failure. Session retry enables alternate recovery mechanisms to mitigate impact of any unavailable 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.

Below screen capture shows a scenario when the Policy Control Function (PCF) microservices initiates an egress request but, it fails to reach the egress gateway.



Alternate routing: Alternate routing is initiated when egress gateway fails to reach external network function (NF) or external NFs fail with an error code, or external NFs do not respond. Alternate destination can be chosen by using static configuration or by using DNS-SRV records. For more information on DNS-SRV records, see Configurable Parameters for DNS-SRV section in the *Oracle Communications Cloud Native Core Policy Installation Guide*.

Below screen capture shows a scenario when egress gateway reaches the NF, but NF responds with an error code.


Policy Service
SM,AM,UE,User...
Egress GW
NF
NF (ALT)
Service sends an egress request to Egress GW,
Destination NF responds with error
Egress GW relays the error
response to Policy Service
Initiate alternate routing if
configured, indicate "alternate
SCP" flag per configuration
Egress GW forwards to destination, possibly via an
alternate SCP
Service sends an egress request to Egress GW,
for alternate destination
SCP

You can create and manage Retry Profiles from the **Retry Profile** screen. The page displays the list of defined retry profiles. You can add, import, export or refresh the Retry Profiles from this page.

To configure the retry profile:

1. From the navigation menu, click **Policy**, and then **Service Configurations**, and then **Common Data**, and then **Retry Profiles**.
   The **Retry Profile** page opens, displaying the list of defined retry profiles. You can add or import new retry profile from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Retry Profile** page opens.
3. Enter the unique **Name** for the retry profile. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
4. Enable or disable the **Retry on Internal Send Failure**. On enabling, **Retry Settings** group is effective.
5. Enable or disable the **Enable Alternate Routing**. On enabling, **Alternate Routing Settings** group is effective.
6. Expand the **Retry Settings group** group to enter the **Maximum Number Of Retries**.
   The maximum number of retry attempts during a retry cycle in the range from 1 to 10.
7. Expand the **Alternate Routing Settings** group to enter the following information:
   - **Maximum Number Of Alternate Routing Attempts** - The maximum number of alternate routing attempts during a alternate routing cycle in the range from 1 to 10.
   - **Error Codes List** - The error codes received from the destination network function. Error Codes can be any HTTP error code.
   - **Use Alternate SCP for Alternate Routing** - If enabled, PCF egress gateway tries to chose alternate SCP to reach the alternate destination.
   - **Enable Fallback to Higher Priority Destination** - If enabled, higher priority destination that had been failed will be reused after the retry interval.
   - **Retry After Interval (in milliseconds)** - The length of time to wait, in milliseconds, after a reported failure before falling back. Enter a value from 1 to 1440 milliseconds.
8. Click **Save**
   The retry profile is defined in the Policy database and can now be used in a policy.

   The retry profile gets listed on the **Retry Profile** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the retry profile.

Configuring PCF Session Management Service

Perform the following steps to configure the PCF Session Management Service:

1. From the navigation menu, under **Policy**, click **Service Configurations**, and then click **PCF Session Management**.
   The PCF Session Management service screen appears.

2. Click **Edit** to configure the PCF Session Management service.
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:

Field Name	Description
System	
Log Level	Indicates the log level of PCF Session Management (SM) service. **Default Value**: WARN **Allowed Values**: DEBUG, INFO, WARN, ERROR
Component Tracing	Determines if component tracing is enabled. Component tracing is used to evaluate system process latency in detail level. **Default Value**: FALSE
Server Root URL	Specifies the callback URI for notifications to be received by the user.
FQDN	This is 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**: pcf-smservice.oracle.com **Note** : If we have multiple PCF, Diameter identity and FQDN must be unique.
Diameter Realm	This is 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	This is 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**: pcf-smservice.oracle.com **Note** : If we have multiple PCF, Diameter identity and FQDN must be unique.
Snssai	Used to register Binding data to BSF by PCF. AF/BSF may use this SNSSAI to discover proper PCF. **Default Value**: 0,000000
Enable Metrics	This determines if system metrics is enabled. This will take priority on global metrics configuration. **Default Value**: True
Override Supported Features	**Default Value**: PRA PRA is only supported in this release.

Field Name	Description
SMF Terminate Uri Segment	Segment in the URI to identify the SM Session TERMINATE operation. **Default Value**: terminate
SMF Update Uri Segment	Segment in the URI to identify the SM Session UPDATE operation. To be configured when the SMF uses anything other than the segment string mentioned in the standards. **Default Value**: update
Process 400 as 200	**Default Value**: False
Enable Custom Json	This determines if custom JSON is enabled. **Default Value**: False
SMF Notification Retry Profile	Defines the retry profile configuration for session management. See Managing Retry Profilesfor configuring retry profile.
User	
Validate User	When this option is enabled, and the subscriber is not found in the UDR, or PCF is not able to query an available/ eligible UDR, PCF shall fail the SM Association creation request with a 400 USER_UNKNOWN error. When this option is disabled, and the subscriber is not found in the UDR, or PCF is not able to query an available/ eligible UDR, PCF shall not fail the SM Association creation request, but continue policy processing. **Default Value**: FALSE
Query User	Determines if user query from UDR is enabled. When this option is enabled, PCF shall query 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 PCF User 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. **Default Value**: TRUE

Field Name	Description
Query User On Update	Determines if user query from UDR on update is enabled. When this option is enabled, PCF shall query the UDR about the subscriber present in the SM Association **update** request by sending a GET request for “sm-data” resource on the nudr-dr service. **Note:** The PCF User 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. **Default Value** : FALSE
Query User On Delete	Determines if user query from UDR on delete is enabled. When this option is enabled, PCF shall query the UDR about the subscriber present in the SM Association **delete** request by sending a GET request for “sm-data” resource on the nudr-dr service. **Note:** The PCF User 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. **Default Value** : FALSE

Field Name	Description
Query User On Reauth	Determines if user query from UDR on reauth is enabled. When this option is enabled, PCF shall query the UDR about the subscriber, when it receives a Reauthorization request (like an Rx or Policy Authorization request) by sending a GET request for “sm-data” resource on the nudr-dr service. **Note:** The PCF User 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. **Default Value** : FALSE
Subscribe to Notify	When this flag is enabled, PCF shall subscribe with the UDR to get notified on changes in subscriber profile. **Default Value**: TRUE
Ignore Subs Notification Check	**Default Value**: FALSE
Enable CHF Query All	When this option is enabled, PCF shall fetch the status of Policy Counters (Spending Limit Status Information) and subscribe with the CHF to get notified on change in status by sending a POST request to the nchf-spendinglimitcontrol service. **Default Value**: FALSE
Include Snssai in user query	**Default Value**: true
Include Dnn in user query	**Default Value**: true
Enable Operator Specific Data Query	When this option is set to true, PCF interacts with UDR for OperatorSpecificData in SM service. **Default Value**: false
Policy	
Evaluate	This determines if policy evaluate is enabled. **Default Value**: TRUE
Policy Control Request Trigger	
Default Policy Control Request Triggers	**Values**: PLMN_CH, UE_IP_CH, DEF_QOS_CH, and AC_TY_CH
Binding Configuration	
Binding Operation	Determines if binding operation (register and deregister) to the BSF is enabled. **Default Value**: TRUE

Field Name	Description
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
BSF Retry Profile	Defines the retry profile configuration for Binding service. See Managing Retry Profilesfor configuring retry profile.
QOS	
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_
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 will be 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 will be 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 will be 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 will be applied if no default Qos is requested by UE. **Default Value**: 1
Rule	
Install Default Pcc Rule	**Default Value** : IF_NO_RULE
Default PCC Rule Profile	
Rule Id Prefix	**Default Value** : 0_
Default Pcc Rule 5qi	This is the 5Qi of default pcc rule. **Default Value**: 9

Field Name	Description
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
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
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	**Default Value**: FALSE
Set PacketFilterUsage to true for Preliminary Service Info	**Default Value**: FALSE
Charging	
Charging Data Id Prefix	**Default Value**: chgdata_
Primary CHF Address	Address of the primary CHF
Secondary CHF Address	Address 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.
Traffic Control	
Traffic Control Id Prefix	**Default Value**: tcdata_
IMS Emergency Session	

Field Name	Description
Emergency DNNs	
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
Audit	
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 will notify to Session Management (SM) service in one second. **Default Value**: 50
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 Passes Interval (in minutes)	Defines the time when next audit for the SM service table will begin after delta time if auditing this table has been finished before this specified time. **Default Value**: 330

4. Click **Save**.

Configuring PCF Access and Mobility Service

You can configure the PCF access and mobility service from this page.

To configure the PCF Access and Mobility Service:

1. From the navigation menu, click **Policy**, and then **Service Configurations**, and then **PCF Access and Mobility**.
   The PCF Access and Mobility Service screen appears.
2. Click **Edit** to edit the PCF access and mobility service configurations.
3. Check the default configuration for all the fields in all groups and edit as necessary.

The following table describes the input fields available under each group:

Field Name	Description
System	
Root Log Level	**Default Value**: WARN
AMF Notification Retry Profile	Defines the retry profile configuration for Access and Mobility service. See Managing Retry Profiles for configuring retry profile.
Log Level	
Use Policy Service	**Default Value**: true
Use User Service	**Default Value**: true
Subscribe	**Default Value**: true
Enable HTTP2.0	**Default Value**: false
Validate User	Determines if user validate is enabled. HTTP 400 with cause USER_UNK NOWN returns, if this is enabled and user not found in UDR. **Default Value**: false
App	
Default Service Area Restriction	
Default Rfsp	
Default Triggers	

4. Click **Save**.

Configuring PCF Policy Authorization Service

You can configure the PCF policy authorization service from this page.

To configure the PCF Policy Authorization Service:

1. From the navigation menu, click **Policy**, and then **Service Configurations**, and then **PCF Policy Authorization**.
   The PCF Policy Authorization Service screen appears.
2. Click **Edit** to edit the PCF policy authorization service configurations.
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:

Field Name	Description
System	
Af Direct Reply	**Default Value**: true
Override Supported Features	
AF Terminate Uri Segment	**Default Value**: termination
AF Subscriber Notify Segment	**Default Value**: termination

Field Name	Description
Rx Resource Allocation Partial Failure Report Prefence	After PCF triggers a notification to Diameter Connector, the connector generates a RAR message. The partial failed specific action in the RAR message will depend 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 below mentioned three options. Once the value is defined in this field, the connector will use 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. See Managing Retry Profiles for configuring retry profile.
IMS Emergency Session	
Emergency Service URNs	
Reservation Priority Types	**Default Value**: PRIO_6

4. Click **Save**.

Configuring PCF UE Policy Service

You can configure the PCF UE policy service from this page.

To configure the PCF UE Policy Service:

1. From the navigation menu, click **Policy**, and then **Service Configurations**, and then **PCF UE Policy**.
   The PCF UE Policy Service screen appears.
2. Click **Edit** to edit the PCF UE policy service configurations.
3. In the **Notification URI Root** field, enter the callback URI for notifications to be received by the PCF UE Policy service (For example, while creating a subscription for the NAS Message Transfer with the AMF)
4. 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:

Field Name	Description
System	

Field Name	Description
Log Level	**Default Value**: WARN
Notification URI Root	
AMF	
Enable HTTP/1.1	**Default Value**: false
NAS Message Maximum Packet Size (bytes)	enter a range in [0-65535] number
User	
Validate User	**Default Value**: false
Query User	**Default Value**: false

5. Click **Save**.

Configuring PCF User Connector Service

You can configure the PCF user connector service from this page.

To configure the PCF User Connector Service:

1. From the navigation menu, click **Policy**, and then **Service Configurations**, and then **PCF User Connector**.
   The PCF User Connector Service screen appears.
2. Click **Edit** to edit the PCF user connector service configurations.
3. In the **Server Root URL** field, enter the callback URI for notifications to be received by the User service (For example, while creating a subscription for the user with the UDR)
4. 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:

Field Name	Description
System	
Log Level	**Default Value**: WARN
Server Root URL	
Common	
Resource Get Subscribe	**Default Value**: false
Request Timeout	**Default Value**: 1000
DB	
Keys Precedence	
User Index Keys	
Indexing	
Index By Msisdn	**Default Value**: true
Index By Extid	**Default Value**: true
Index By Imsi	**Default Value**: true
Index By Nai	**Default Value**: true
UDR	

Field Name	Description
Base Uri	**Default Value**: /nudr-dr/v1
Supported Features	**Default Value**: f
AM Data Uri	**Default Value**: /policy-data/ues/{ueId}/am-data
UE Policy Set Uri	**Default Value**: /policy-data/ues/{ueId}/ue-policy-set
SM Data Uri	**Default Value**: /policy-data/ues/{ueId}/sm-data
Usage Mon Uri	**Default Value**: /policy-data/ues/{ueId}/sm-data/{usageMonId}
Subs To Notify Uri	**Default Value**: /policy-data/subs-to-notify
Subs To Notify Subs Id 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".
Request Timeout	**Default Value**: 1000
Explode Snssai	**Default Value**: false
Enable HTTP1.1	**Default Value**: false
Enable Discovery On Demand	**Default Value**: false
Retry Profile	Defines the retry profile configuration for UDR. See Managing Retry Profiles for configuring retry profile.
CHF	
Retry Profile	Defines the retry profile configuration for CHF. See Managing Retry Profiles for configuring retry profile.

5. Click **Save**.

Configuring PCRF Core Settings

You can configure the PCRF core settings from this page.

To configure the PCRF Core Settings:

1. From the navigation menu, click **Policy**, and then **Service Configurations**, and then **PCRF Core**, and then **Settings**.
   The PCRF Core Settings screen appears.
2. Click **Edit** to edit the PCRF Core settings configuration. This enables the **Add** button in **Advanced Settings** group.
3. Click **Add**. The **Add Advanced Settings** window opens.
4. Enter the values in **Key** and **Value** fields.
5. Click **Save**.

Configuring Logs

This chapter describes how to configure log level for PCRF Core service through Cloud Native Core Console.

> **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.

To configure the log level:

1. From the navigation menu, click **Policy**, and then **Service Configurations**, and then **PCRF Core**, and then **Logs**.
   The **Logs** page opens. You can add or edit the log level and package log level for PCRF Core service from this page.
2. Click **Edit**.
3. From the **Root Log Level** drop-down menu, select the PCRF Core's root log level. Possible values are:
   - Trace
   - Debug
   - Information
   - Warn
   - Error
   - Fatal

   > **Note:**
   >
   > The value for the **Root Log Level** field will be set only when the package log level is not configured.
4. Expand the **Package Log Level** group to enter the package log level information:
   a. Click **Add**.
   The **Add Package Log Level** page opens.
   b. Enter the value in the **Package** field. The value of **Package** field is dependent on the package's name in the application. Before you set the value of **Package** field, you need to know what package is existed in that application. Possible values are:
      - ocpm
      - camiant
      - msc
      - customerspecific
      - Trace-Logging
      - Alarm-Logging
      - SyslogLogger
      - Subscriber-Logging

c. From the **Log Level** drop-down menu, select the log level for the package. Possible values are:
   - Trace
   - Debug
   - Information
   - Warn
   - Error
   - Fatal

d. Click **Save**.
   The Package log level information is saved.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the package log level information.

5. Click **Save**.
   The log level information for the PCRF Core is saved.

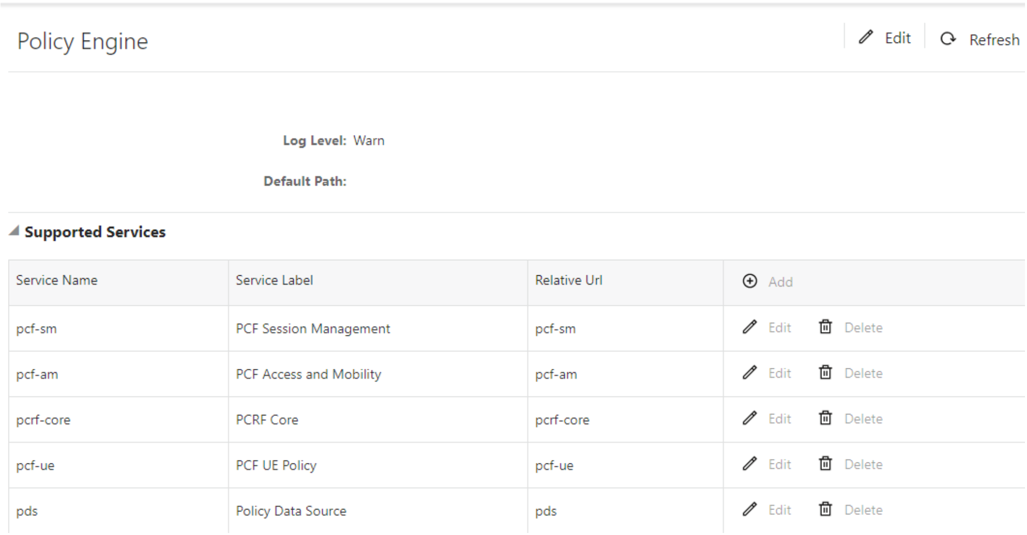
Policy Engine

You can view the Policy Engine services on this page. List of the services displayed on this page is based on your deployment.

> **Note:**
>
> Services should not be added or edited on this page.

To view the Policy Engine page: From the navigation menu, under **Policy**, then **Service Configurations**, and then click **Policy Engine**. The Policy Engine page appears.

Below is a screen capture of Policy Engine page.



Log Level: Warn

Default Path:

Supported Services

Service Name	Service Label	Relative Url	Add
pcf-sm	PCF Session Management	pcf-sm	Edit Delete
pcf-am	PCF Access and Mobility	pcf-am	Edit Delete
pcrf-core	PCRF Core	pcrf-core	Edit Delete
pcf-ue	PCF UE Policy	pcf-ue	Edit Delete
pds	Policy Data Source	pds	Edit Delete

Configuring Audit Service

Oracle Communications Cloud Native Core Policy (OCCNCP) signalling services (SM service, AM service, UE service, Binding Management service etc.) are stateless in nature, thereby offloading session state to a centralized database (DB) tier, in this case, it is Oracle MySQL. As the session processing micro-services and the DB tier are different components that communicate over a network there are chances for certain transactions to fail on the transit, for example, in overload situations and/or as a result of code bugs. The OCCNCP solution requires a database audit mechanism to monitor records getting stale and to clean them up so that the database memory does not eventually grow indefinitely. The audit mechanism also notifies the owner services about stale records so that they can trigger signalling messages in certain cases to ensure that the sessions detected as stale by the Audit service is actually released by other consumer NFs. Additionally in certain cases, releasing a session when found to be stale in a NF may require to release associated sessions in the same and/or other NFs. For Example, deleting a stale SM association may require to delete the associated PA sessions.

You can configure the audit service from this page.

To configure the Audit Service:

1. From the navigation menu, under **Policy**, then under **Service Configurations**, click **Audit**.
   The Audit screen appears.
2. Click **Edit** to edit the session management service configurations.
3. Check the default configuration for the fields available and edit as necessary.
   The following table describes the input fields displayed under **System** group:

Field Name	Description
System	

Field Name	Description
Log Level	Indicates the log level of Audit service. **Default Value**: Warn **Allowed Values**: Debug, Information, Warn, Error
Audit Enabled	Determines if auditing is enabled for all the registered services. **Default Value**: FALSE
Audit Rate (records per second)	Defines the number of records audited per second.

4. Click **Save**.

Logging in Audit Service

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 DELETE action)
- Number of notifications sent (for NOTIFY action)
- Time taken to complete the audit pass
- Any exceptions occurred

Sample of Audit Report

```
Audit Report {
"database" : "pcf_smservice_161",
"table" : "SmPolicyAssociation",
"staleRecords" : 18869,
"recordsDeleted" : 0,
"timeToCompletePass" : 20,
"recordsEnqueuedForNotification" : 18869,
"exceptions" : [ ]
}
```

Policy Data Configurations

This chapter describes how to create manageable objects in CNC Policy function.

Common

You can configure the common services from this page. To configure the common service, click **Policy**, and then **Policy Data Configurations**, and then **Common**.

The Common configuration includes:

- Policy Table
- Dropdown Blocks
- PCF Presence Reporting Area

- Policy Counter ID
- Match List
- Subscriber Logging
- Custom Attributes

Managing Policy Tables

This chapter describes how to create, modify, delete, and view policy tables, which are independent objects that you can use to capture differences in policy structures.

You can manage multiple policies with small differences by abstracting the differences into tables. The process of modifying the policies, or creating new, similar policies, then becomes a matter of modifying the policy table, which is simpler and less prone to error.

About Policy Tables

In practical use, many policies are very similar, having only small differences between them. A policy table abstracts the differences between related policies. Using a policy table instead of creating many similar policies makes the tasks of adding new policies, modifying existing sets of policies, and checking consistency among related policies simpler and less prone to error

> **Note:**
>
> Policy Table is only supported for the Session Managment service.

Policy tables resemble database tables and contain the following elements:

- Table name
- 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 will be of the same data type as the column. Every table must have atleast 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.

Creating a Policy Table

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 a policy table:

1. From the **Policy Management** section of the navigation pane, select **Policy Table**.

   The **Policy Tables** page opens.

2. Click **Create** .

   The Create Policy Table page opens.

3. Enter information as appropriate:

   a. **Name** (required) — The unique name you assign to the policy table.

      The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underscore (_). The maximum length is 32 characters.

   b. **Description** — Free-form text that identifies the policy table. The maximum length is 255 characters.

   c. Click **Save**.

      The Policy Table is created and listed under the SM service related policy tables.

      > **Note:**
      >
      > You can create maximum 20 tables per service type.

4. To add a column, click **Open**, then click **Create Column**.

   The Create Policy Table Column page opens.

   > **Note:**
   >
   > You must define at least one key column. You can define maximum five key columns in a policy table.

   Enter the following information:

   - **Name** (required) — The name you assign to the column. 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** (required) — The data type of cells in the column. You can select the required data type from the drop-down.
   - **Key** — If this is a key column, enable the switch.

     > **Note:**
     >
     > The first column is always the **Key** cloumn by default and you will not be able to change it.

   - Click **Save**.

   The column is created.

> **Note:**
>
> You can create maximum 10 columns in a policy table.

> **Note:**
>
> Note the following tips while adding a new column in a policy table, when the policy table contains the rows:
>
> - Add/Modify/Delete operations are allowed on the non-key columns only while the policy table contain row(s).
> - **Key** switch will be in disabled mode while adding a column when the policy table contain 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.
> - A warning is issued to update the policies manually, if the column is deleted.

5. (Optional) You can create rows as follows:
   a. Click **Create Row**. The Create Policy Table Row page opens.
   b. You can enter the value for the cell. The data in the cell must match the data type of the column.
   c. Enter the value and click **OK**. You can also enter a comma-separated list of values.

   The row is created and appears below the previous row.

   > **Note:**
   >
   > You can create maximum 100 rows in a policy table.

   > **Note:**
   >
   > Make sure that the key column 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.

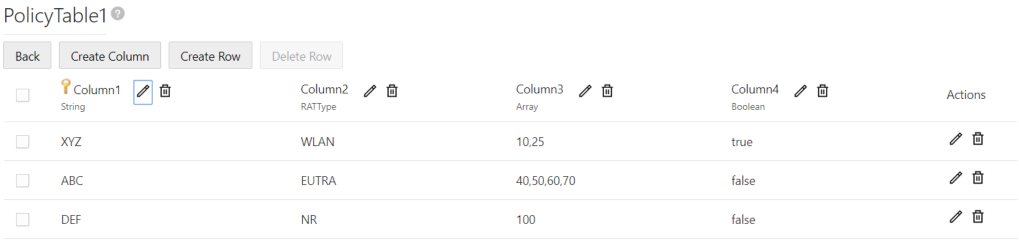
6. Click **Save**.

   The policy table is created and is displayed on the Policy Tables page.

Note:

One or more wildcarded values in the key column cell are compared to the values in the policy context data. If there is any match, the row is matched. The asterisk (*) character represents any number of characters, and the question mark (?) character represents any single character.

Policy table is updated with columns and rows. You can now use the table in a policy. Below screenshot is a sample policy table, PolicyTable1, with four columns and three rows:



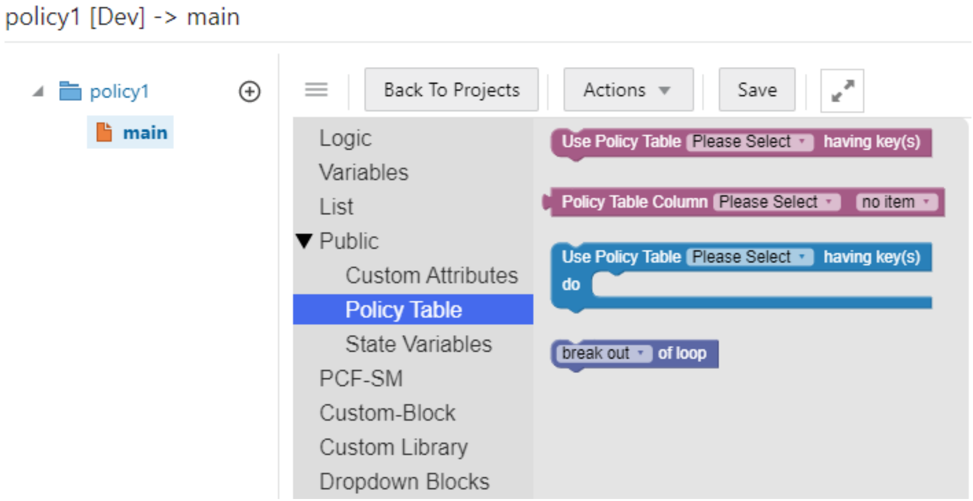
□	Column1 String	Column2 RATType	Column3 Array	Column4 Boolean	Actions
□	XYZ	WLAN	10,25	true	
□	ABC	EUTRA	40,50,60,70	false	
□	DEF	NR	100	false	

Associating a Policy Table with a Policy

To associate a policy table with a new or existing policy, the policy table must already be created.

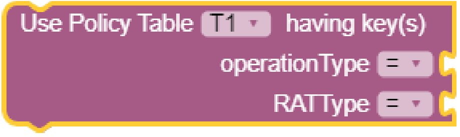
To associate a policy table with a policy rule:

1. From the navigation menu, under **Policy Management**, click **Policy Projects**. The Policy Projects page displays all the created policies.
2. Select the policy.
3. Click **Open** for the selected policy. The policy page is displayed. You can access Policy Table blocks under the **Public** category. The following screen capture shows an example of the **SM Policies** policy page with Policy Table blocks:



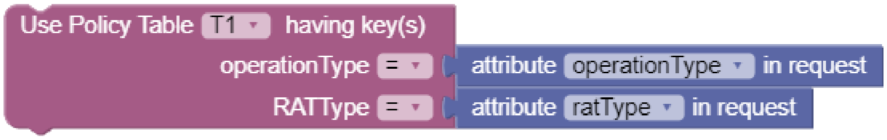
4. In the first block, select the policy table from the **Policy Table** drop-down and the corresponding key columns are displayed in the **key(s)**. The following screen

capture shows an example in which Policy Table **T1** has been selected and the **OperationType** and **RatType** are the corresponding key columns in the table **T1**.



Use Policy Table T1 ▾ having key(s)
operationType = ▾
RATType = ▾

5. Select the operator from the operator drop-down 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**.

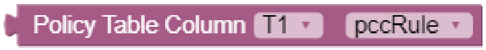


Use Policy Table T1 ▾ having key(s)
operationType = ▾ attribute operationType ▾ in request
RATType = ▾ attribute ratType ▾ in request

If all the values associated with the key columns match its column data from policy table based on the operator used ("="), then it will return the complete row data.

> **Note:**
>
> This block can return only single row.

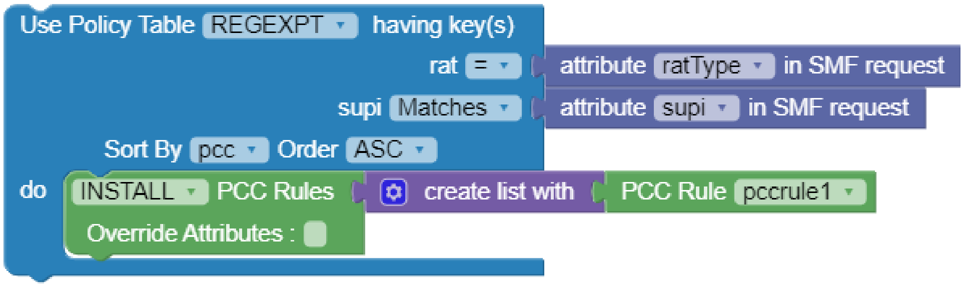
6. In the second block, select the policy table from the **Policy Table Column** drop-down and the corresponding non-key columns are displayed in the **no item**drop-down. The following screen capture shows an example in which policy table **T1** is selected and the non-key column, **pccRule** is displayed in the drop-down.



Policy Table Column T1 ▾ pccRule ▾

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 and the corresponding key and non-key columns are displayed in the **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**. 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 **PCF-SM** topics. The following screen capture shows an example of associating policy conditions with the columns, **rat** and **supi**.


Use Policy Table REGEXPT having key(s)
rat = attribute ratType in SMF request
supi Matches attribute supi in SMF request
Sort By pcc Order ASC
do INSTALL PCC Rules create list with PCC Rule pccrule1
Override Attributes :

If all the values associated with the columns match its column data from policy table based on the operator used ("=") and Matches, then it will return the complete row data.

> **Note:**
>
> This block can return multiple rows.

> **Note:**
>
> For this block, "=", "!=", Matches, and Ignore opearotrs are supported.

8. Click **Save**.

The selected policy tables are associated with this policy rule.

Modifying a Policy Table

To modify a policy table:

1. From the **Policy Management** section of the navigation pane, select **Policy Table**.

   The **Policy Tables** page opens, displaying information about the policy table.
2. Click **Edit** next to the policy table you want to edit.

   The table fields become editable.
3. Make required changes and click **Save**.

The policy table content is modified.

Deleting a Policy Table

To delete a policy table:

1. From the **Policy Management** section of the navigation pane, select **Policy Table** .

   The **Policy Tables** page opens, displaying information about the policy table.
2. Click **Delete** next to the policy table you want to delete.

   A confirmation message appears.
3. Click **OK**.

The policy table is deleted.

Dropdown Blocks

To create the Dropdown blocks from this page:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then click **Dropdown Blocks**.
   The **Dropdown Blocks** screen appears with the listing of all the dropdown blocks created. You can create or import new dropdown blocks from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Dropdown Block** screen appears.
3. On the **Create Dropdown Block** screen, enter values for the input fields.
   The following table describes the fields:

Field Name	Description
Attribute Name	Name of the attribute
Description	Description of the attribute
Type	Select one of the values: static or dynamic

4. In the **Block Options** group, click **Add** to add the field details:
   a. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Label Name	Name of the block
Value	Specify the value

      > **Note:**
      >
      > Click **Remove** to cancel the changes.

   b. Click **Save**.
5. Click **Save**.
   The value gets listed on the **Dropdown Blocks** screen.

   > **Note:**
   >
   > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Dropdown Blocks

To import the dropdown blocks:

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**.

PCF Presence Reporting Area

You can manage, view, import, export and create the PCF Presence Reporting Area using this screen.

To configure the service:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **PCF Presence Reporting Area**.
   The **PCF Presence Reporting Area** screen appears with the listing of all the available reports. You can create or import new reports from this page.

   > **Note:**
   >
   > Click Export to download the available reports to your system.

2. Click **Add**.
   The **Create PCF Presence Reporting Area** screen appears.
3. Enter values for the input fields common to all the groups available on the screen. .
   The following table describes the fields:

Field Name	Description
Name	The unique name assigned to the PRA.
Pra Id	The unique identifying number of the PRA list. The ID must be numeric value between 0 and 16777125. This field is present if the Area of Interest subscribed or reported is a Presence Reporting Area.

4. Expand the **Tracking Area List** group.
   The expanded window displays the available tracking area lists. To create new lists:
   a. Click **Add**.
      The **Add Tracking Area List** window appears on the screen.
   b. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Mnc	Defines the Mobile Network Code. Two to three digit number.

Field Name	Description
Mcc	Defines the Mobile Country Code. Three digit number.
Tac	28-bit string identifying an E-UTRAN Cell Id as specified, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the Cell Id shall appear first in the string, and the character representing the 4 least significant bit of the Cell Id shall appear last in the string. Pattern: '^[A-Fa-f0-9]{7}$' Example: An E-UTRAN Cell Id 0x5BD6007 shall be encoded as "5BD6007".

> **Note:**
>
> Click **Cancel** to cancel the changes.

c. Click **Save**.
The value gets listed in the **Tracking Area List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

5. Expand the **Ecgi List** group.
The expanded window displays the available Eutra Cell Ids. To create new Ids:

   a. Click **Add**.
   The **Add Ecgi List** window appears on the screen.

   b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Mnc	Defines the Mobile Network Code of the PLMN. Two to three digit number.
Mcc	Defines the Mobile Country Code of the PLMN. Three digit number.

Field Name	Description
Eutra Cell Id	28-bit string identifying an E-UTRA Cell Id as specified in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the Cell Id shall appear first in the string, and the character representing the 4 least significant bit of the Cell Id shall appear last in the string. Pattern: '^[A-Fa-f0-9]{7}$' Example: An E-UTRA Cell Id 0x5BD6007 shall be encoded as "5BD6007".

> **Note:**
>
> Click **Cancel** to cancel the changes.

c. Click **Save**.
The value gets listed in the **Ecgi List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

6. Expand the **Ncgi List** group.
   The expanded window displays the available Nr Cell Ids. To create new Ids:

   a. Click **Add**.
   The **Add Ncgi List** window appears on the screen.

   b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Mnc	Defines the Mobile Network Code of the PLMN. Two to three digit number.
Mcc	Defines the Mobile Country Code of the PLMN. Three digit number.

Field Name	Description
Nr Cell Id	36-bit string identifying an NR Cell Id as specified in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the Cell Id shall appear first in the string, and the character representing the 4 least significant bit of the Cell Id shall appear last in the string. Pattern: '^[A-Fa-f0-9]{9}$' Example: An NR Cell Id 0x225BD6007 shall be encoded as "225BD6007".

Note:

Click **Cancel** to cancel the changes.

c. Click **Save**.
The value gets listed in the **Ncgi List**.

Note:

Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

7. Expand the **Global Ran NodeId List** group.
The expanded window displays the available **N3 Iwf Ids**. To create new Ids:

a. Click **Add** displayed in the window.
The **Add Global Ran NodeId List** window appears on the screen.

b. Enter the applicable values in the input fields available on the window.
The following table describes the fields:

Field Name	Description
Plmn Id	
Mnc	Defines the Mobile Network Code of the PLMN. Two to three digit number.
Mcc	Defines the Mobile Country Code of the PLMN. Three digit number.
N3 Iwf Id	This field is included if the RAN node belongs to non 3GPP access (i.e a N3IWF). If included, this field contains the FQDN of the N3IWF.
gNb Id	

Field Name	Description
Bit Length	Unsigned integer representing the bit length of the gNB ID within the range 22 to 32
gNb Value	This represents the identifier of the gNB. The string shall be formatted with following pattern: '^[A-Fa-f0-9]{6,8}$' The value of the gNB ID shall be encoded in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the gNB ID shall appear first in the string, and the character representing the 4 least significant bit of the gNB ID shall appear last in the string. Examples: "382A3F47" indicates a gNB ID with value 0x382A3F47
Nge Nb Id	This field is included if the RAN Node Id represents a NG-eNB. When present, this field contains the identifier of an NG-eNB.

> **Note:**
>
> Click **Cancel** to cancel the changes.

c. Click **Save**.
The value gets listed under **Global Ran NodeId List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

8. Click **Save**.
The Pra details are listed on the **PCF Presence Reporting Area** screen.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

Importing the PCF Presence Reports

To import the reports:

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** button.

Configuring Policy Counter Id

You can create and manage Policy Counter Ids from the Policy Counter Id screen. The page provides information about the existing Policy Counter Ids. You can create or refresh the Policy Counter Ids from this page.

To configure the service:

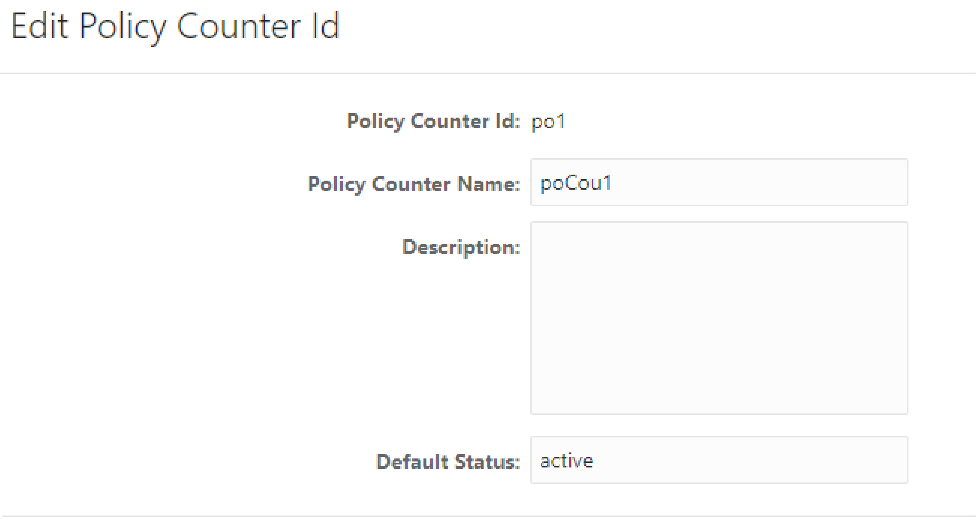
1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Policy Counter Id**.
   The **Policy Counter Id** screen appears with the listing of all the available rules. You can create or import new data from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Policy Counter Id** screen appears.
3. On the **Create Policy Counter Id** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Policy Counter Id	Policy Counter Id's Name.
Name	
Description	Policy Counter Id's description.
Default Status	

Below screen capture shows a sample of Policy Counter Id:



Edit Policy Counter Id

Policy Counter Id:	po1
Policy Counter Name:	poCou1
Description:	
Default Status:	active

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Policy Counter Id** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Policy Counter Id Data

To import the Policy Counter Ids:

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**.

Configuring Match Lists

In a wireless network, a match list is a set of defined values that can represent, for example, IDs or Internet addresses. Match lists provide whitelist and blacklist functions in policy rules. Match lists support wildcard matching.

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. A match list can function as a whitelist (listing items to be included) or a blacklist (listing items to be excluded). By using a match list, you can, for example, apply a policy to all subscribers in a set of LACs, or block access to a list of Internet addresses known to be high risk. Match lists support wildcards. Using wildcards, a range of values can be specified compactly.

Creating a Match List

To create a match list:

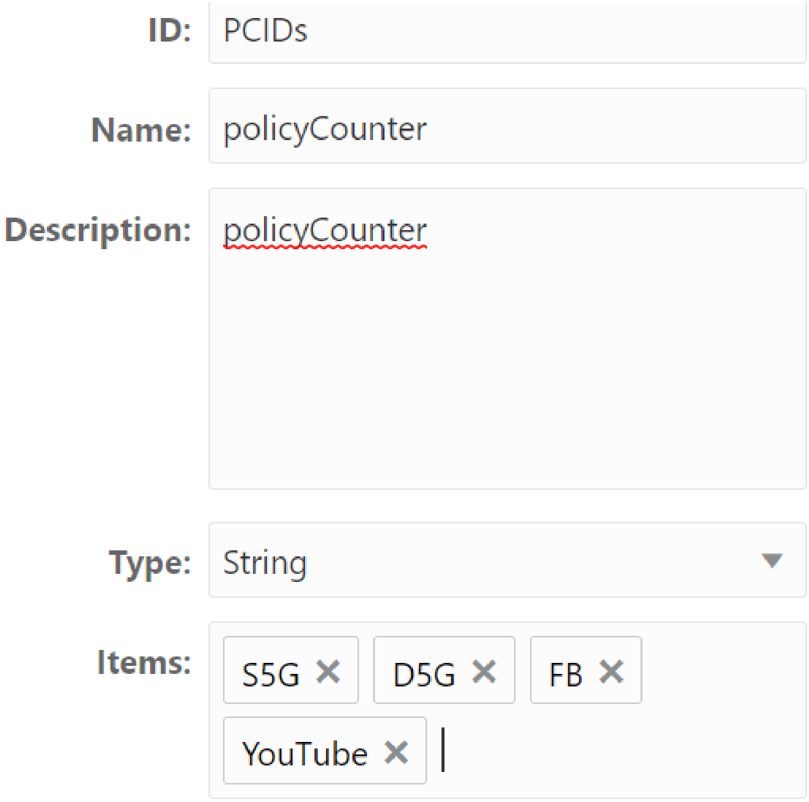
1. From the navigation pane, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Match List**.
   The **Match List** page opens in the work area.
2. Click **Create**.
   The Create Match List page opens.
3. Enter the following information:
   - **ID**: The ID assigned 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.
- **Items**:

4. Click **Save**.

The match list is defined in the database and can now be used in a policy.

Below screen capture shows an example of Match List:



ID: PCIDs

Name: policyCounter

Description: policyCounter

Type: String

Items: S5G ✕ D5G ✕ FB ✕ YouTube ✕

Modifying a Match List

To modify a match list:

1. From the navigation pane, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Match List**.
   The **Match List** page opens in the work area, displaying the list of defined match lists.
2. Select the match list you want to modify.
3. Click **Edit**.
   The Edit Match List page opens.
4. Modify match list information as required.
5. Click **Save**.
   The match list is modified.

Deleting a Match List

To delete a match list:

1. From the navigation pane, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Match List**.
   The **Match List** page opens in the work area, displaying the list of defined match lists.
2. Select the match list you want to delete.
3. Click **Delete**.
   A confirmation message displays.
4. Click **OK**.
   The match list is deleted.

Importing the Match Lists

To import the match lists:

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**.

Exporting the Match Lists

You can export the match lists by clicking **Export All**. The Match Lists will be downloaded in a local machine.

Managing Subscriber Logging

Subscriber logging lets you to define a list of the subscribers (identifier) that you are interested to troubleshoot and network fuction trace all the logs related to the subscribers separately to view. This allows you to use this functionality to troubleshoot problematic subscribers in production without having to enable logs/traces that can impact all subscribers. Using the subscriber logging, you can capture and monitor subscriber logs for UDR/CHF notifications and associated call flow in Session Management (SM) and egress gateway.

To enable the subscriber activity logging functionality, set the **Enable Subscriber Activity Logging** parameter as **true** in the **General Configurations** screen. By default, this functionality is disabled. General Configurations screen can be accessed via the left navigation menu under **Policy**.

> **Note:**
>
> This functionality is only supported by Session Management (SM) Associations in this release.

You can configure the list of subscribers using the **Subscriber Logging** screen.

> **Note:**
>
> The maximum number of subscribers that can be configured is 100.

> **Note:**
>
> You can not modified subscriber information once it is entered. If you need to modify the subscriber information, delete the subscriber information and add it again .

To configure a list of subscribers for logging:

1. From the navigation menu, under **Policy**, then under **Policy Data Configurations**, and then under **Common**, click **Subscriber Logging**.
   The Subscriber Logging screen appears with the listing of subscribers. You can create or import subscribers from this page.

   > **Note:**
   >
   > Click Export to download the available listing on your syatem.

2. Click **Add** to add the subscriber item to the list..
   The **Create Subscriber Logging** screen appears.
3. From the **Identifier Type** drop-down, select the subscriber identifier type.
   Supported subscriber identifier type are:
   - GPSI
   - SUPI
   - IPV4
   - IPV6
4. Enter the subscriber identier value in the **Identifier Value** field for the selected identifier type.
5. Select **Enable** to enable/disable the subscriber logging functionality for the selected subscriber.
6. Click **Save**.

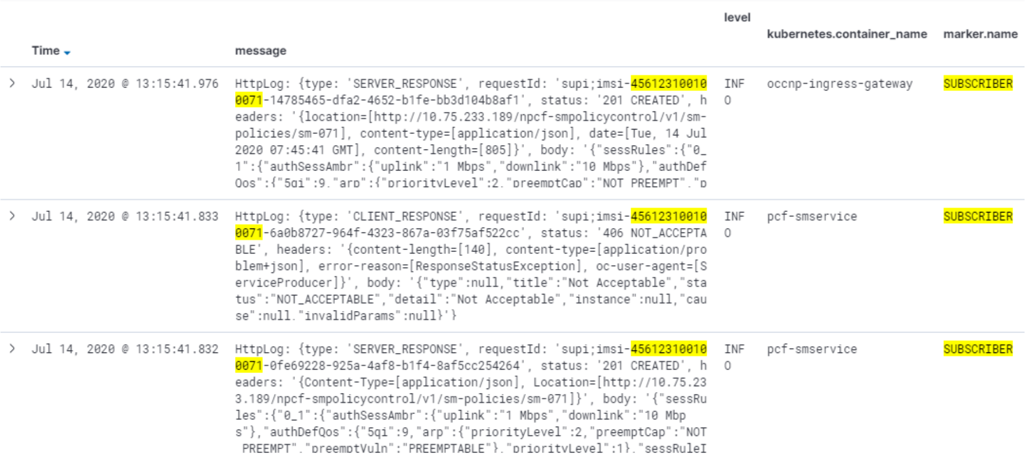
> **Note:**
>
> Use pencil icon or trash can icon available in the next column to update or delete the subscriber listing.

When the subscriber logging has been enabled, the trace log (displayed in the kibana dashboard) for that specified subscriber IDs has the following information:

- Subscriber Identification including associated IP Address information

- Message, Container name, Level
- Policy related information (applied for the subscriber session)
- Date and Timestamps for all messages logged

Below screen capture is a log sample (kibana dashboard) with filter "marker.name:SUBSCRIBER" and fields: message, level, kubernetes.container_name, and marker.name.



Time	message	level	kubernetes.container_name	marker.name
Jul 14, 2020 @ 13:15:41.976	HttpLog: {type: 'SERVER_RESPONSE', requestId: 'supi;imsi-456123100100071-14785465-dfa2-4652-b1fe-bb3d104b8af1', status: '201 CREATED', headers: '{location=[http://10.75.233.189/npcf-smpolicycontrol/v1/sm-policies/sm-071], content-type=[application/json], date=[Tue, 14 Jul 2020 07:45:41 GMT], content-length=[805]}', body: '{"sessRules":{"0_1":{"authSessAmbr":{"uplink":"1 Mbps","downlink":"10 Mbps"},"authDefQos":{"5qi":9,"arp":{"priorityLevel":2,"preemptCap":"NOT PREEMPT","p	INFO	occnp-ingress-gateway	SUBSCRIBER
Jul 14, 2020 @ 13:15:41.833	HttpLog: {type: 'CLIENT_RESPONSE', requestId: 'supi;imsi-456123100100071-6a0b8727-964f-4323-867a-03f75af522cc', status: '406 NOT_ACCEPTABLE', headers: '{content-length=[140], content-type=[application/problem+json], error-reason=[ResponseStatusException], oc-user-agent=[ServiceProducer]}', body: '{"type":null,"title":"Not Acceptable","status":"NOT_ACCEPTABLE","detail":"Not Acceptable","instance":null,"cause":null,"invalidParams":null}'}	INFO	pcf-smservice	SUBSCRIBER
Jul 14, 2020 @ 13:15:41.832	HttpLog: {type: 'SERVER_RESPONSE', requestId: 'supi;imsi-456123100100071-0fe69228-925a-4af8-b1f4-8af5cc254264', status: '201 CREATED', headers: '{Content-Type=[application/json], Location=[http://10.75.233.189/npcf-smpolicycontrol/v1/sm-policies/sm-071]}', body: '{"sessRules":{"0_1":{"authSessAmbr":{"uplink":"1 Mbps","downlink":"10 Mbps"},"authDefQos":{"5qi":9,"arp":{"priorityLevel":2,"preemptCap":"NOT PREEMPT","preemptVuln":"PREEMPTABLE"},"priorityLevel":1},"sessRuleI	INFO	pcf-smservice	SUBSCRIBER

Custom Attributes

Custom attributes lets you to accept the vendor's data that is in custom format, not in the standard format. This data can then be used to construct conditions and actions.

Configuring Custom Schema

This section describes how to import the custom schema in the Policy User Interface (UI). Custom attributes lets you to accept the vendor's data that is in custom format, not in the standard format. This data can then be used to construct conditions and actions .

> **Note:**
>
> Custom schema yaml file should follow Open API standards.

To import a custom schema file:

1. Create a custom schema yaml file. Below is a sample yaml file:

```
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:
  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
```

2. Save the yaml file on your system.
3. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Custom Attributes**, and then **Custom Schema**. The **Custom Schema** screen appears with the listing of custom schema.

   > **Note:**
   >
   > Click Export to downlaod the available listing on your system.

4. Click **Import** to import the custom schema yaml file.
   The **File Upload** window opens.
5. Click **Drop Files here or click to upload**. Locate the yaml file to be imported.
6. Click **Import**. After the import is complete, the schemas are listed on the Custom Schema page.

You can use this custom schema in creating policy conditions and actions by using blockly interface under the **Custom Attributes** section in the **Public** section.

Custom AVP

About Custom AVP

An attribute-value pair (AVP) is used to encapsulate protocol-specific information with usage monitoring supported by the MPE device. 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 third-party AVPs.

> **Note:**
>
> The Diameter messages listed are examples only. There are many messages associated with Diameter.

You can 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.

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 ]
[ 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 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 an MPE or MRA device, the definition must include the AVP name, code, vendor ID, data type, and an optional AVP flag.

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

Configuring Custom AVP

To create a custom AVP:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Custom Attributes**, and then **Custom AVP**.
   The Custom AVP screen appears.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The Create Custom AVP page opens.
3. Enter information as appropriate:
   a. **AVP Name** (required) — The name you assign to the AVP.
      The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_). The maximum length is 255 characters.
   b. **Description** — Free-form text that identifies the AVP. Enter up to 250 characters.
   c. **AVP Code** (required) — A unique numeric value assigned to the new AVP.
   d. **Vendor** — Select a vendor from the vendor list. To add a vendor to the list, see Custom Vendor.
   e. **Mandatory Flag** (optional) —
   f. **Protect Flag** (optional) — When checked, specifies the protected AVP values.
   g. **May Encrypt Flag** — The AVP is encrypted if the checkbox is specified.

h. **Vendor Specific Flag** — The AVP is vendor specific if the checkbox is specified.

> **Note:**
>
> This box is checked automatically if the value of the vendor ID is not 0.

i. **AVP Type** (required) — Select the data type from the list:

- **address**
- **enumerated**
- **float32**
- **float64**
- **grouped**
- **id**
- **int32**
- **int64**
- **ipFilterRule**
- **octetString**
- **time**
- **uint32**
- **uint64**
- **uri**
- **utf8String**

j. **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**
- **Codec-Data:10415**
- **Cost-Information**
- **Default-EPS-Bearer-Qos:10415**
- **E2E-Sequence**
- **Envelope:10415**
- **Event-Report-Indication:10415**
- **Explicit-Route-Record:21274**
- **Explicit-Route:21274**
- **Failed-AVP**
- **Final-Unit-Indication**
- **Flow-Description-Info:5535**
- **Flow-Description:10415**
- **Flow-Grouping:10415**
- **Flow-Info:5535**
- **Flow-Information:10415**
- **Flow:10415**
- **G-S-U-Pool-Reference**
- **Granted-Qos:5535**
- **Granted-Service-Unit**
- **Juniper-Discovery-Descriptor:2636**
- **Juniper-Provisioning-Descriptor:2636**
- **LI-Indicator-Gx:12951**
- **LI-TargetMFAddr:12951**
- **Media-Component-Description:10415**
- **Media-Sub-Component:10415**
- **Multiple-Services-Credit-Control**
- **Offline-Charging:10415**

- **PCEF-Forwarding-Info:971**
- **PCEF-Info:971**
- **PS-Furnish-Charging-Information:10415**
- **PS-information:10415**
- **Packet-Filter-Information:10415**
- **Qos-Information-3GPP2:5535**
- **Qos-Information:10415**
- **Qos-Rule-Install:10415**
- **Qos-Rule-Definition:10415**
- **Qos-Rule-Remove:10415**
- **Qos-Rule-Report:10415**
- **Reachable-Peer:21274**
- **Redirect-Information:10415**
- **Redirect-Server**
- **Requested-Qos:5535**
- **Requested-Service-Unit**
- **Service-Information:10415**
- **Service-Parameter-Info**
- **Siemens-DL-SDP-Data:4329**
- **Siemens-UL-SDP-Data:4329**
- **Subscription Id**
- **Subscription-Id-3GPP:10415**
- **Supported-Features:10415**
- **TDF-Information:10415**
- **TFT-Packet-Filter-Information:10415**
- **TMO-Redirect-Server-29168**
- **Time-Quota-Mechanism:10415**
- **Trigger:10415**
- **Tunnel-Header-Filter:10415**
- **Unit-Value**
- **Usage-Monitoring-Control:21274**
- **Usage-Monitoring-Information:10415**
- **Used-Service-Unit**
- **User-CSG-Information:10415**
- **User-Equipment-Info**
- **User-Location-Info-3GPP:10415**
- **VZW-Access-Network-Physical-Access-ID:12951**

- **Vendor-Specific-Application-Id**
- **Vzw-Trigger:12951**

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 AVP is created.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing Custom AVP

To import the custom vendor:

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**.

Custom Vendor

A custom vendor is used to define a vendor in the CNPCRF system. This dictionary includes vendor IDs and text descriptions. You can define custom vendors and add them to the dictionary.

To create a custom vendor:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **Common**, and then **Custom Attributes**, and then **Custom Vendor**.
   The Custom Vendor screen appears.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The Create Custom Vendor page opens.
3. Enter information as appropriate:
   a. **Vendor Name** (required) — The name you assign to the vendor.
   The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underline (_).
   b. **Description** — Free-form text that identifies the vendor.
   Enter up to 250 characters.
   c. **Vendor Id** — Enter the vendor ID.
   Enter a positive integer.
4. Click **Save**.

The vendor is created.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing Custom Vendor

To import the custom vendor:

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**.

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
- Usage Monitoring Data
- Traffic Control Data
- Condition Data

Configuring Session Rule

You can create and manage session rules from the Session Rule screen. The page provides information about the existing session rules. You can create or refresh the session rules from this page.

To configure the session rules from this page:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **Session Rule**.
   The **Session Rule** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available listings to your system.

2. Click **Add**.

The **Create Session Rule** screen appears.

3. On the **Create Session Rule** screen, enter values for the input fields common to all the groups available on the screen.
The following table describes the fields:

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. Under the **Authorized Session AMBR** group, add the AMBR details.
   a. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Uplink Bandwidth	Specifies the bandwidth in uplink.
Downlink Bandwidth	Specifies the bandwidth in downlink.

> **Note:**
>
> Click **Remove** to cancel the changes.

   b. Click **Add** to save changes.
5. Select value for Condition Data from the drop down menu.
6. Select value for **Authorize Default Qos** from the drop down menu.

> **Note:**
>
> The drop down gets its data from the QoS Information created.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

7. Click **Save**.
The value gets listed on the **Session Rule** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Session Rules

To import the session 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**.

Configuring Session Rule Profile

You can manage and configure the session rule profiles from this page.

To configure the profile:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **Session Rule Profile**.
   The **Session Rule Profile** screen appears with the listing of all the available rules. You can create or import new profiles from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Session Rule Profile** screen appears.
3. On the **Create Session Rule Profile** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

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. Under the **Authorized Session AMBR** group, add the AMBR details:
   a. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Uplink Bandwidth	Specifies the bandwidth in uplink.
Downlink Bandwidth	Specifies the bandwidth in downlink.

      > **Note:**
      >
      > Click **Remove** to cancel the changes.

   b. Click **Add** to save changes.
5. Select value for **Condition Data** from the drop down menu.

6. Select value for **Authorize Default Qos** from the drop down menu.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

7. Click **Save**.
The value gets listed on the **Session Rule Profile** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Session Rule Profiles

To import the session rule profiles:

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** button.

Configuring QoS Information

You can manage, view, import, export and create the QoS Information from QoS Information screen.

To configure the QoS Information data:

1. From the navigation menu, **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **QoS Information**.
The **QoS Information** screen appears with the listing of all the available rules. You can create or import the QoS details from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Add**.
The **Create QoS Information** screen appears.
3. On the **Create QoS Information** screen, enter values for the input fields common to all the groups available on the screen.
The following table describes the fields:

Field Name	Description
Name	Specifies the name assigned to the QOS information.
Description	Free-form text that identifies the QOS information.

Field Name	Description
Default 5G QoS Identifier	Identifier for the authorized QoS parameters for the service data flow. It shall be 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 shall be calculated (NOTE).
Max DataBurstVol	Denotes the largest amount of data that is required to be transferred within a period of 5GAN PDB (NOTE).

4. Add arp details in fields listed under **ARP** group.:
   a. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

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 : Shall 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 : Shall not be pre-empted. • PREEMPTABLE : May be pre-empted.

> **Note:**
>
> Click the **Remove** button to cancel the changes.

   b. Click the **ADD** button to add the changes.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

5. Click **Save**.
   The value gets listed on the **QoS Information** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the QoS Information

To import the session 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** button.

Configuring PCC Rule

You can create and manage PCC Rule from the PCC Rule screen. The page provides information about the existing rules. You can create or refresh the PCC rules from this page.

To configure the rule:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **PCC Rule**.
   The **PCC Rule** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create PCC Rule** screen appears.
3. On the **Create PCC Rule** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

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 go to Step 4 else, go to Step 5.

4. Expand the **Flow Infos** group to add the Flow information:

a. Click the **Add** icon displayed in the window.
   The **Add Flow Infos** appears.

b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Name	Indicates the name for the flow.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Pack Filt Id	An identifier of packet filter.
Packet Filter Usage	The packet shall be sent to the UE. The default value "FALSE" shall apply, 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.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Ethernet Flow Description	
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F

Field Name	Description
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

c. Click **Add** under the **Ethernet Flow Description** group name to expand the group.
The screen displays the available input fields. Enter the applicable values in the input fields.

The following table describes the fields:

Field Name	Description
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F

Field Name	Description
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

> **Note:**
>
> Click **Remove** to cancel the changes.

d. Click **Save** on the **Add Flow Infos** window, under the **Flow Infos** group. The value gets listed on the **Create PCC Rule** screen.

e. Under the **Flow Infos** group, enter values for the rest of the input fields:

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 shall be 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 signalling between the UE and the AF. The default value "NO_INFORMATION" shall apply, if the attribute is not present and has not been supplied previously.
Application Relocation	Indication of application relocation possibility. The default value "NO_INFORMATION" shall apply, 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.

5. Click **Save**.

The value gets listed on the **PCC Rule** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the PCC Rules

To import the session 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**.

Configuring PCC Rule Profile

You can create and manage PCC Rule Profile from the PCC Rule Profile screen. The page provides information about the existing profiles. You can create or refresh the profiles from this page.

To configure the PCC Rule Profile:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **PCC Rule Profile**.
   The **PCC Rule Profile** screen appears with the listing of all the available rules. You can create or import new profile details from this page.

   > **Note:**
   >
   > Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create PCC Rule Profile** screen appears.
3. On the **Create PCC Rule Profile** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

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 go to Step 4 else, go to Step 5.

4. Expand the **Flow Infos** group to add the Flow information:

a. Click the **Add** icon displayed in the window.
   The **Add Flow Infos** appears.

b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Name	Indicates the name for the flow.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Pack Filt Id	An identifier of packet filter.
Packet Filter Usage	The packet shall be sent to the UE. The default value "FALSE" shall apply, 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.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Ethernet Flow Description	
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F

Field Name	Description
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

c. Click **Add** under the **Ethernet Flow Description** group name to expand the group.
The screen displays the available input fields. Enter the applicable values in the input fields.

The following table describes the fields:

Field Name	Description
Dest Mac Address	A string indicating MAC address. Enter a valid MAC address. For example, 3D-F2-C9-A6-B3-4F
Ethernet Type	A two-octet string that represents the Ethertype, in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the ethType shall appear first in the string, and the character representing the 4 least significant bits of the ethType shall appear last in the string.
Flow Description	Indicates the details about flow. Enter a description for the flow.
Flow Direction	Indicates the flow direction. Select from the following options: • DOWNLINK • UPLINK • BIDIRECTIONAL • UNSPECIFIED
Source Mac Address	Enter a MAC Address. For example, 3D-F2-C9-A6-B3-4F

Field Name	Description
Vlan Tags	Customer-VLAN and/or Service-VLAN tags containing the VID, PCP/DEI fields. Each field is encoded as a two-octet string in hexadecimal representation. Each character in the string shall take a value of "0" to "9" or "A" to "F" and shall represent 4 bits. The most significant character representing the 4 most significant bits of the VID or PCF/DEI field shall appear first in the string, and the character representing the 4 least significant bits of the VID or PCF/DEI field shall appear last in the string.

> **Note:**
>
> Click **Remove** to cancel the changes.

d. Click **Save** on the **Add Flow Infos** window, under the **Flow Infos** group. The value gets listed on the **Create PCC Rule** screen

e. Under the **Flow Infos** group, enter values for the rest of the input fields:

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 shall be 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 signalling between the UE and the AF. The default value "NO_INFORMATION" shall apply, if the attribute is not present and has not been supplied previously.
Application Relocation	Indication of application relocation possibility. The default value "NO_INFORMATION" shall apply, 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.

Field Name	Description
Usage Monitoring Data	A reference to UsageMonitoringData policy decision type.
Condition Data	A reference to the condition data.

5. Click **Save**.
   The value gets listed on the **PCC Rule Profile** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the PCC Rule Profiles

To import the session 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**.

Configuring QoS Data

You can create and manage QoS Data from the QoS Data screen. The page provides information about the existing QoS Data. You can create or refresh the QoS Data from this page.

To configure the QoS Data:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **QoS Data**.
   The **QoS Data** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Qos Data** screen appears.
3. On the **Create QoS Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

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.

Field Name	Description
Default 5G QoS Identifier	Identifier for the authorized QoS parameters for the service data flow. It shall be 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	
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.
Averaging Window	Represents the duration over which the guaranteed and maximum bitrate shall be 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 shall 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. Add the arp details under the **ARP** group.

   a. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	Description
Priority Level	Defines the relative importance of a resource request.

Field Name	Description
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

> **Note:**
>
> Click **Cancel** to cancel the configuration.

5. Click **Save**.
   The value gets listed on the **QoS Data** screen.

   > **Note:**
   >
   > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the QoS Data

To import the QoS Data:

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** button.

Configuring Charging Data

You can manage, view, import, export and create the Charging Data from Charging Data screen.

To configure the charging data:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **Charging Data**.
   The **Charging Data** screen appears with the listing of all the available rules. You can create or import new data from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Create**.
   The **Create Charging Data** screen appears.
3. On the **Create Charging Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Charging id	Specifies the charging id.
Name	The name of the Charging Data.
Description	The description of the Charging Data.
Metering Method	The following options are available • DURATION • VOLUME • DURATION_VOLUME • EVENT Defines what parameters shall 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 the attribute is set to NULL, the metering method preconfigured at the SMF is applicable as default metering method.
Offline	Indicates the offline charging is applicable to the PDU session or PCC rule. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously. (NOTE)
Online	Indicates the online charging is applicable to the PDU session or PCC rule. The default value "FALSE" shall apply, if the attribute is not present and has not been supplied previously. (NOTE)
Rating Group	The charging key for the PCC rule used for rating purposes.
Reporting Level	The following options are available: • SER_ID_LEVEL • RAT_GR_LEVEL • SPON_CON_LEVEL Defines on what level the SMF reports the usage for the related PCC rule. 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 reporting level preconfigured at the SMF is applicable as default reporting level.

Field Name	Description
Service Id	Indicates the identifier of the service or service component the service data flow in a PCC rule relates to.
Sponsor Id	Indicates the sponsor identity.
App Svc Prov Id	Indicates the application service provider identity.
Af Charging Identifier	Univocally identifies the charging control policy data within a PDU session.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Charging Data** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Charging Data

To import the session 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**.

Configuring Usage Monitoring Data

You can create and manage Usage Monitoring Data from this page. The page provides information about the existing Usage Monitoring Data as well.

To configure the service:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **Usage Monitoring Data**.
   The **Usage Monitoring Data** screen appears with the listing of all the available rules. You can create or import new rules details from this page.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Usage Monitoring Data** screen appears.
3. On the **Create Usage Monitoring Data** screen, enter values for the input fields common to all the groups available on the screen.

The following table describes the fields:

Field Name	Description
Usage Monitoring id	Specifies the usage monitoring id.
Name	The name of the Usage Monitoring Data.
Description	The description of the Usage Monitoring Data.
Volume Threshold	Indicates a volume threshold.
Volume Threshold Uplink	Indicates a volume threshold in uplink.
Volume Threshold Downlink	Indicates a volume threshold in downlink.
Time Threshold	Indicates a time threshold.
Monitoring Time	Indicates the time at which the UP function is expected to reapply the next thresholds (e.g. nextVolThreshold).
Next Vol Threshold	Indicates a volume threshold after the Monitoring.
Next Vol Threshold Uplink	Indicates a volume threshold in uplink after the Monitoring Time.
Next Vol Threshold Downlink	Indicates a volume threshold in downlink after the Monitoring Time.
Next Time Threshold	Indicates a time threshold after the Monitoring.
Inactivity Time	Defines the period of time after which the time measurement shall stop, if no packets are received.
ex Usage PccRule Ids	Contains the PCC rule identifier(s) which corresponding service data flow(s) shall be excluded from PDU Session usage monitoring. It is only included in the UsageMonitoringData instance for session level usage monitoring.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Usage Monitoring Data** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Usage Monitoring Data

To import the Usage Monitoring Data:

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**.

Configuring Traffic Control Data

You can manage, view, import, export and create the Traffic Control Data from Traffic Control Data screen.

To configure the traffic control data:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **Traffic Control Data**.
   The **Traffic Control Data** screen appears with the listing of all the available rules. You can create or import new data from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create Traffic Control Data** screen appears.
3. On the **Create Traffic Control Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the 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" shall apply, if the attribute is not present and has not been supplied previously.

4. Enter values of the available input fields under **Redirect Information** group.
   The following table describes the fields:

Field Name	Description
Redirect Enabled	Indicates the redirect is enabled.

Field Name	Description
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.
Mute Notification	Indicates whether application's start or stop notification is to be muted. The default value "FALSE" shall apply, 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.

5. Expand the **Route To Locs** group.
   The expanded window displays the available routes. To create new routes:
   a. Click **Add** in the window.
      The **Add Route To Locs** window appears on the screen.
   b. Enter the applicable values in the input fields available on the window.
      The following table describes the fields:

Field Name	Description
Dnai	Identifies the location of the application.
Ipv4 Addr	Ipv4 address of the tunnel end point in the data network.
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.
Route Profile Id	Identifies the routing profile Id.

> **Note:**
>
> Click **Cancel** to cancel the changes.

   c. Click **Save**.
      The value gets listed in the **Tracking Area List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

6. Enter values of the available input fields the **Up Path Chg Event** group.
   The following table describes the fields:

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 shall only be present in the subscription to the DNAI change event. LATE: Late notification of UP path reconfiguration. This string provides forwardcompatibility with future extensions to the enumeration but is not used to encode content defined in the present version of this API.

7. Click **Save**.
   The value gets listed on the **Traffic Control Data** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Traffic Control Data

To import the session 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**.

Configuring Condition Data

You can create and manage condition data from the **Condition Data** screen. The page provides information about the existing Condition Data. You can create or refresh the Condition Data from this page.

To configure the condition data:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Session Management**, and then **Condition Data**.
   The **Condition Data** screen appears with the listing of all the available rules. You can create or import new data from this page.

> **Note:**
>
> Click the **Export** button to download the available listings to your system.

2. Click **Add**.
   The **Create Condition Data** screen appears.
3. On the **Create Condition Data** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

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 shall be activated.
Deactivation Time	The time when the decision data shall be deactivated.

> **Note:**
>
> Click **Cancel** to cancel the configuration.

4. Click **Save**.
   The value gets listed on the **Condition Data** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Condition Data

To import the Condition Datas:

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**.

PCF Access and Mobility

You can configure the PCF Access and Mobility policy services from this page.

The PCF Access and Mobility configuration includes Managing Service Area Restriction.

Configuring Service Area Restriction

You can create and manage service area restrictions from the **Service Area Restriction** screen. The page provides information about the existing Service Area Restrictions as well.

To configure the service area restriction:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF Access and Mobility**, and then **Service Area Restriction**.
   The **Service Area Restriction** screen appears with the listing of all the available rules. You can create or import new data from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Create**.
   The **Create Service Area Restriction** screen appears.
3. On the **Create Service Area Restriction** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	**Description**
Name	Specifies name of the service area restriction.
Description	Specifies description of the service area restriction.
Restriction Type	Specifies the restriction type. Possible values are: • ALLOWED_AREAS • NOT_ALLOWED_AREAS This field is present if and only if the areas attribute is present.

4. To create new area details under the **Area** group:
   a. Click the **Add** button displayed in the window.
   The **Add Areas** window appears on the screen.
   b. Enter the applicable values in the input fields available on the window.
   The following table describes the fields:

Field Name	**Description**
Tacs	Specifies Type Allocation Codes. A decimal number between 0 and 65535. This fields is present if and only if Area Codes is absent.
Area Codes	Specifies area codes. This fields is present if and only if Tacs is absent.

   c. Click on the **Save** button.
   The value gets listed in the **Tracking Area List**.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

5. Enter value of the **Max Number of TAs** input field.

   > **Note:**
   >
   > Click **Cancel** to cancel the configuration.

6. Click **Save**.
   The value gets listed on the **Service Area Restriction** screen.

   > **Note:**
   >
   > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the Service Area Restrictions

To import the Service Area Restrictions:

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**.

PCF UE Policy

You can configure the PCF UE Policy from this page.

The PCF UE Policy configurations includes:

- URSP Rule
- UPSI Rule

Configuring URSP Rule

You can create and manage URSP Rules from the URSP Rule screen. The page provides information about the existing URSP Rules. You can create or refresh the URSP Rules from this page.

To configure the URSP Rules:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF UE Policy**, and then **URSP Rule**.
   The **URSP Rule** screen appears with the listing of all the available reports. You can create or import new rules from this page.

> **Note:**
>
> Click the **Export** button to download the available reports to your system.

2. Click **Add**.
   The **Create URSP Rule** screen appears.
3. On the **Create URSP Rule** screen, enter values for the input fields common to all the groups available on the screen. .
   The following table describes the fields:

Field Name	Description
Name	Name of the URSP rule.
Precedence	Precedence value of the URSP rule.

4. Under the **Traffic Descriptor** group, all available descriptor types are displayed. To create new types:
   1. Click **Add** displayed in the window.
      The **Add Traffic Descriptor** window appears on the screen.
   2. Select a value from the **Type** drop down menu. Possible values are:
      - MATCH_ALL
      - OS_ID_OS_APP_ID
      - IPV4_REMOTE_ADDRESS
      - IPV6_REMOTE_ADDRESS
      - PROTOCOL_IDENTIFIER
      - SINGLE_REMOTE_PORT
      - REMOTE_PORT_RANGE
   3. Click **Save**.
      The value gets listed under the **Traffic Descriptor** group.

      > **Note:**
      >
      > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.
5. The **Route Selection Descriptor List** group displays the available precedence. To create new data:
   1. Click **Add** displayed in the window.
      The **Add Route Selection Descriptor List** window appears on the screen.
   2. Enter the value in the **Precedence** field.
   3. Click **Add** to create a new Route Selection Descriptor Components in the **Route Selection Descriptor Components** group. .
      The Add Route Selection Descriptor Components window appears on the screen.

   d. Select a value from the **Type** drop down menu.
   e. Select a value from the **SSC Mode** drop down menu.
   f. Click **Save**.
      The value gets listed in the **Route Selection Descriptor List**.

      > **Note:**
      >
      > Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

6. Click **Save**.
   The Pra details are listed on the **Presence Reporting Area** screen.

   > **Note:**
   >
   > Click **Cancel** to cancel the configuration.

Importing the URSP Rule

To import the reports:

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**.

Configuring UPSI

You can manage, view, import, export and create UPSI from UPSI screen.

To configure UPSI:

1. From the navigation menu, click **Policy**, and then **Policy Data Configurations**, and then **PCF UE Policy**, and then **UPSI**.
   The **UPSI** screen appears with the listing of all the available rules. You can create or import new profile details from this page.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add**.
   The **Create UPSI** screen appears.
3. On the **Create UPSI** screen, enter values for the input fields common to all the groups available on the screen.
   The following table describes the fields:

Field Name	Description
Name	Name of the UPSI.

Field Name	Description
UPSC	Defines UE Policy Section Code. Enter a number between 0 and 65,535.
URSP Rules	Defines URSP rules.

4. Enter values of the available input fields under the **PLMN** group.
   The following table describes the fields:

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 value gets listed on the **UPSI** screen.

> **Note:**
>
> Use **Edit** or **Delete** buttons available in the next column to update or delete the listing.

Importing the UPSI

To import the UPSIs:

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** button.

PCRF Core

This section describes how to use and configure PCRF Core Managed Objects.

Charging Server

This section describes how to define and manage charging servers within the PCRF Core in Policy GUI. A charging server is an application that calculates billing charges.

To define a charging server:

1. From the navigation pane, click **Policy**, and then **Policy Data Configurations**, and then **PCRF Core**, and then **Charging Server**.

   The **Charging Server** screen appears.

> **Note:**
>
> Click **Export** to download the available listings to your system.

2. Click **Add**.

The Create Charging Server page opens.

3. (Required) Enter the **Name** for the charging server.

   The name can only contain the characters A through Z, a through z, 0 through 9, period (.), hyphen (-), and underline (_).

4. Enter the **Description/Location**.

   Free-form text that identifies the charging server within the network. Enter up to 250 characters.

5. (Required) Enter the **Host Name**.

   The FQDN (fully qualified domain name assigned) to the charging server.

6. Enter the **Port** number on which the charging server is listening for messages.

   If left blank, port 3868 is used.

7. Select the **Transport** protocol used to communicate with the charging server:

   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**.

   - **sctp**
     Stream Control Transmission Protocol

8. Select the Authentication, Authorization, and Accounting (AAA) **Protocol** used to communicate with the charging server.

   Available options include:

   - **diameter**
   - **radius**

   > **Note:**
   >
   > If you configure the Transport protocol as **udp**, you cannot configure the AAA Protocol as **diameter**.

9. Select if transport **Security** is used to communicate with the charging server.

10. Click **Save**.

The charging server is displayed on the Charging Server page.

> **Note:**
>
> Use pencil icon or trash bin icon available in the next column to edit or update the created charging server.

Importing Charging Server

To import charging server:

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** button.

Media Profile

This section defines how to manage media profiles under PCRF Core in the CNC Policy GUI. In a cable network, a media profile describes a CODEC supported for Rx-to-PCMM translation.

> **Note:**
>
> Media Profiles is a function that is applicable to Cable mode only.

To create a media profile:

1. From the navigation pane, click **Policy**, and then **Policy Data Configurations**, and then **PCRF Core**, and then **Media Profile**.

   The **Media Profile** screen appears.

   > **Note:**
   >
   > Click **Export** to download the available listings to your system.

2. Click **Add.**

   The Create Media Profile page opens.

3. Enter the following information:

   a. **ID** — Unique ID assigned to the media profile.

   b. **Name** — Unique name assigned to the media profile.

   c. **Description** — specifies the description of the media profile.

   d. **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.

   e. **Transport Type** — Select from the following:

- **RTP/AVP** (default) — RTP audio-video profile.
- **RTP/SAVP** — RTP secure audio-video profile.
- **RTP/AVPF** — RTP extended audio-video profile with feedback.

f. **Payload Number** — The payload number.

   Valid payload numbers range from 0 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.

g. **Sample Rate (kHz)** — The sampling rate of the CODEC in KHz.

   The valid range is an integer from 1 through 100 KHz.

h. **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.

i. **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.

j. **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.

k. **Always Use Default Ptime** — Select to always use the default packetization time, ignoring the value received in the SDP message.

   The default is unchecked.

4. Click **Save**.

The media profile is created.

> **Note:**
>
> Use pencil icon or trash bin icon available in the next column to edit or update the created media profile.

Importing Media Profile

To import media profile:

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** button.

Policy Management

CNC Policy offers a Policy Design editor based on Blockly interface. You can create and manage a policy project for each of the policy services that you may want to deploy:

- Session Management and Policy Authorization
- Access and Mobility Management
- UE Management
- PCRF Core
- Policy Data Source

For more information on blocks, see *Oracle Communications Cloud Native Policy Design Guide*. This guide has been made available on MOS.

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**. By default, **Dev** state is assigned to the policy project. Dev Projects will not process any traffic in PRE. Prod projects will process traffic in PRE.

To create and deploy a policy project:

1. From the **Policy** section of the navigation pane, click **Policy Management**, and then **Policy Projects**.
   The Policy Projects screen appears. You can view all the created projects for each service type.
2. Choose the service type and click **Create** to create a new policy project.
   The **Create Policy Project** window opens.

   > **Note:**
   >
   > If the maximum limit for project is reached per service then an error message is displayed on clicking the **Create** button. For Example, Maximum number of projects supported in this release is 10.

3. Enter information as appropriate:
   - **Name** (required) — The name you assign to the policy project. The name can only contain the characters A–Z, a–z, 0–9, period (.), hyphen (-), and underscore (_). The maximum length is 32 characters.

> **Note:**
>
> You must assign a unique name to the policy project per service type. The name is case sensitive.

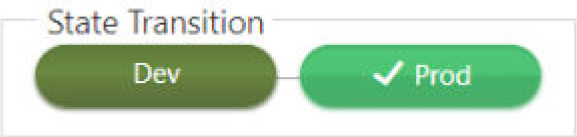
- **Description** — Free-form text that identifies the policy project. The maximum length is 255 characters.

4. Click **Save**.
   The policy project is created.

> **Note:**
>
> If needed, you can unit test the project. For more information on testing the projects, see Test Policy Projects section int the *Oracle Communications Cloud Native Policy Design Guide*.

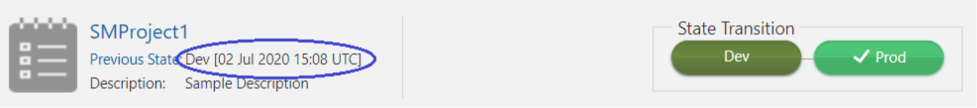
5. You can change the state of a project. There are two possible states in this release, **Dev** and **Prod**. These states are represented using the buttons on the page with the Label named as **Dev** and **Prod**. A tick mark and light green color button helps to identify the current state of a project. Available state button will be in dark green color.

   Below screenshot illustrates the different states of a project. When you click on any of the button to change the state, a message appears asking you to confirm the state change. Click **Yes**. The project state will be changed.



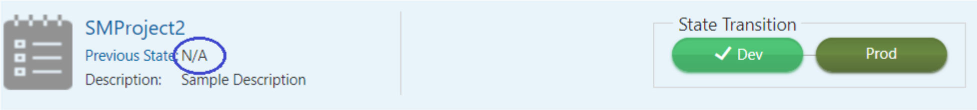
> **Note:**
>
> At any point of time there can be only one project in **Prod** state for a given Service. If you change the state of project to **Prod** and there is already a project with the **Prod** state for that service, the **Prod** state for the existing project will be automatically moved to **Dev** state. And, the project in**Dev** state will be moved to **Prod** state.

6. You can view the last policy project's state with a timestamp by default. Below screenshot is an example displaying that the project is currently in Dev state and the last state was Prod with the Exit timestamp.



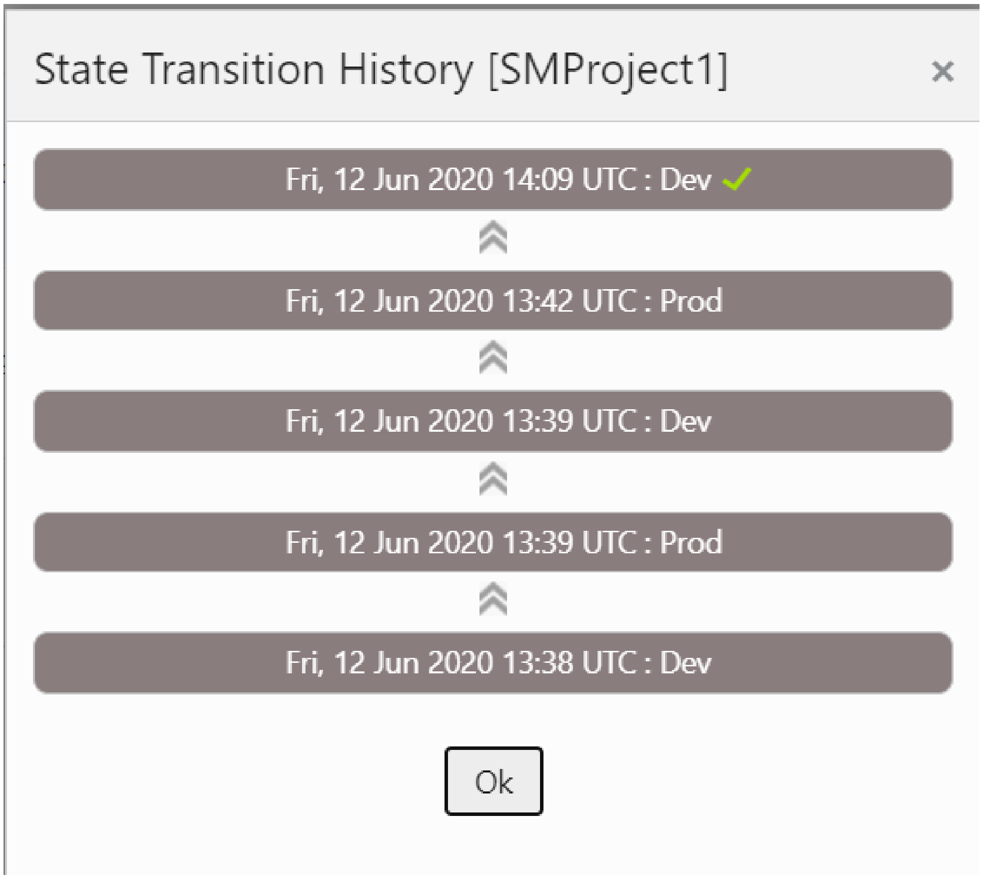
SMProject1
Previous State Dev [02 Jul 2020 15:08 UTC]
Description: Sample Description

Below screenshot is an example displaying that the project is just created and is in Dev state and hence it does not have any previous state.



SMProject2
Previous State: N/A
Description: Sample Description

Below screenshot is an example displaying that you can view the full state history by clicking the **Previous States** link.



State Transition History [SMProject1]

Fri, 12 Jun 2020 14:09 UTC : Dev ✓

Fri, 12 Jun 2020 13:42 UTC : Prod

Fri, 12 Jun 2020 13:39 UTC : Dev

Fri, 12 Jun 2020 13:39 UTC : Prod

Fri, 12 Jun 2020 13:38 UTC : Dev

7. You can filter the projects based on Name and Active State using the **Filter**.

8. Click ⧉ icon to clone the existing policy project. Select an existing policy project and click Clone icon; the Clone Policy Project window opens. You can enter the required information and click **Save**.

9. Click ✎ icon to edit the policy project details.

10. Click trash 🗑 icon to delete the policy project. When you click on the Delete icon, a confirmation dialog box appears asking you to confirm the deletion. After clicking the 'Yes' button, the project and it's associated policies will be deleted.

11. Click 🗀 icon to open a Blockly editor.
You can construct one or more policies as required using the building blocks provided in the Left Side Panel of the editor.

> **Note:**
>
> The project in **Prod** state is not editable you can view the policies but can't modify the project and the policies associated with that project.

See *Policy Design Guide* for more details on the blocks. This guide has been made available on MOS.

Diameter Configurations

You can manage and view the Diameter Configurations from this page. These configurations are a part of PCF mode only for now. For converged and cnPCRF, you have to configure these configurations through Helm Config Map.

Settings

To edit the Settings:

1. From the navigation menu, click **Policy**, and then **Diameter Configurations**, and then **Settings**.
   The Settings screen appears.
2. Click **Edit** to edit the settings.
3. Enter the following information:
   Timer
   - **Reconnect Delay (sec)**- Enter the time frame to delay before attempting to reconnect after a connection failure in seconds. The default is 3 seconds.
   - **Response Timeout (sec)**- Enter the response timeout interval in seconds. The default is 5 seconds.
   - **Connection Timeout (sec)**- Enter the connection timeout interval in seconds. The default is 3 seconds.
   - **WatchDog Interval (sec)**- Enter the watchdog interval in seconds. The default is 6 seconds.

   Transport
   - **Protocol** - TCP/SCTP
4. Click **Save**.

Peer Nodes

To edit the Peer Nodes Configurations:

1. From the navigation menu, click **Policy**, and then **Diameter Configurations**, and then **Peer Nodes**.
   The Peer Nodes screen appears.
2. Click **Add** to create peer node. The Create Peer Node screen appears.
3. Enter the following information:
   - **Name**- Unique Name of the peer node.

- **Type**- Defines which type of diameter service it should take up. The value can be Application function (af) or diameter routing agent(dra).
- **Reconnect Limit (sec)** -
- **Initiate Connection**- Set it to True to initiate a connection for this peer node.
- **Port**- Enter the port number. Enter a number from 0 to 65535.
- **Host**- Enter the host name. Enter a FQDN, ipv4 or ipv6 address available for establishing diameter transport connections to the peer node .
- **Realm**- Enter the realm name, that is, FQDNs to all of that computers that transact diameter traffic.
- **Identity**- Enter a identity to define a node in a realm.

4. Click **Save**.

> **Note:**
>
> You can import and export the Peer Node configurations by clicking on **Import** and **Export** on Peer Nodes Configurations screen.

Configuring Diameter Routing Table

You can define the next hop for Cloud Native Core Policy initiated diameter requests based on Diameter application-id, Destination-Realm and Destination-Host using diameter routing table.You can configure the route entries from this page.

To configure the PCRF Core Settings:

1. From the navigation menu, click **Policy**, and then **Diameter Configurations**, and then **Routing Table**.
   The Diameter Routing Table Configurations screen appears.
2. Click **Edit** to edit the diameter routing table configurations. This enables the **Add** button in **Diamter Routing Table** group.
3. Click **Add**. The **Add Diamter Routing Table** window opens.
4. a. Enter the values for the following fields in the **Diamter Routing Table** group:
   - **Priority**- Defines the order of use when one or more routes have overlapping criteria. The range is 0-65535.
   - **Name**- Unique name of the diameter routing table.
   - **Type**- The value can be Realm or Host.
   - **Realms**- **Realms** field is displayed when the **Realm** is selected in the **Type** field.
   - **Hosts**
     Hosts field is displayed when the **Host** is selected in the **Type** field.
   - **Application ID**
     Select Rx (default), Gq, Ty, Gx, Gxx, Sy, Gy, Sh, or All.
   - **Server Identifier**
     Enter a free-form text.

> **Note:**
>
> * (asterisk) wildcard character is allowed in **Hosts**, **Realms**, and **Server Identifier** fields.

Click **Save**.

b. Enter the value for the **Server Identifier** field in the **Default Route** group.

5. Click **Save**.

The Diameter Routing Table is configured.

Data Source Configurations

Cloud Native Core Policy (CNC Policy) establishes connections with data sources to retrieve information about subscribers from the database. The CNC Policy 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 contained in the database.

The CNC Policy supports Lightweight Directory Access Protocol (LDAP) data source. Based on the conditions implemented in PCF system, Policy Data Source (PDS) would retrieve all the relevant information from LDAP data source based on the rules configured in the system through LDAP gateway.

To enable PDS and LDAP gateway service, set the following flags to true in custom.yaml file as part of CNC Policy installation:

- **ldapGatewayEnable**
- **policydsEnable**

When these flags are set to true, Session Management (SM) service routes its traffic to User service through PDS. For more information on custom.yaml file, refer to *Oracle Communications Cloud Native Core Policy Installation Guide*.

LDAP credentails are stored as kubernetes secret along with Authentication DN and LDAP name. You must create a kuberenetes secret to store LDAP credentials before setting a PDS as LDAP data source.

To create a kubernetes secret for storing LDAP credentails:

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=vodafone,c=hu,o=vodafone"
```

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 datsource.

> **Note:**
>
> For different LDAP data sources more entries can be added in above format only the key of the entry should be the ldap name specified in the CNC Policy Graphical User Interface (GUI).

2. Create the 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.

Data Sources

Creating Data Source

To create data source using CNC Console GUI:

1. From the navigation menu, under **Policy**, then under **Data Source Configurations**, click **Data Sources**. The Data Sources page opens.
2. Click **Add** to create a data source.
   The **Create Data Source** page opens.
3. On the **Create Data Source** page, enter the following information:
   a. **Name**- Unique name of the data source.
   b. **Description**- Details about the data source.
   c. **Type**- Select the value from the drop-down. Possible values are : Sh, LDAP, and Sy.
   d. **Read Connection**- This parameter is available only if you add LDAP as a data source type. Number of read connections established with data source.
   e. Enable/Dsiable the **admin state**. When value is set to true, datasource (sh/sy) interaction takes place.
   f. **Realm**- Defines the realm of the primary and optional secondary servers to connect (required).
   g. **Role**- This parameter is available only if you add Sy as a data source type. Possible values are: **Primary** – Irrespective of policy deployed, interaction with datasource will happen. **Secondary** – **On Demand** – When policy demands, then only interaction with datasource happens.

h. Enable/Disable the **Enable Subscription**- This parameter is available only if you add Sh as a data source type. Indicates whether MPE needs to subscribe to notifications from Sh.

i. Enable/Disable the **Use Notif Eff**- This parameter is available only if you add Sh as a data source type. Specifies the user data Request/Answer will allow multiple data references, service indications, and identity sets. The user data Answer will be able to combine DataReference items resulting in the user data Answer contents including a single XML document with the separate XML sections populated.

j. **Sh Profile**- This parameter is available only if you add Sh as a data source type. Select the Sh Profile from the drop-down to use with this data source.

k. **Timer Profile**- Timer profile for the data source.

l. **Primary Server**- Primary data source server. The data source connection will be established with primary data source.

m. **Secondary Server**- Secondary data source server. If Primary server is not reachable, then data source connection will be established with secondary (if available). You can add or remove the secondary data source server.

n. **Tertiary Server**- Tertiary data source server. If primary and secondary are not reachable, then LDAP connection will be established with tertiary (if available). You can add or remove the tertiary data source server.

o. **Quaternary Server**- Quaternary data source server. If primary , secondary and tertiary are not reachable then LDAP connection will be established with tertiary (if available). You can add or remove the quaternary data source server.

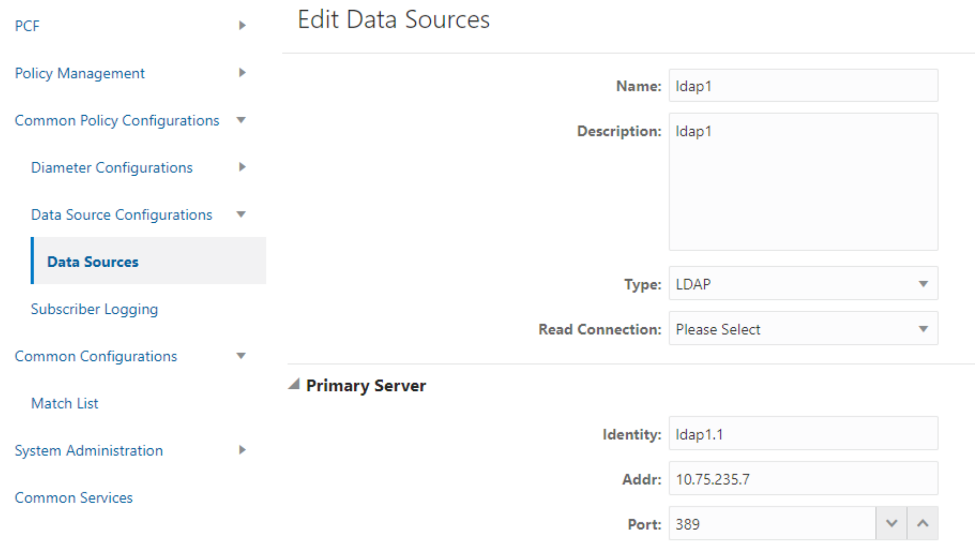
p. **Search Criteria**- The criteria on which the data source search will be performed. You can add or remove the Search Criteria settings.

   - For LDAP data source, enter **Root DN** and **Base DN Attribute**. **root dn** is the root of the LDAP tree in which to search and **Base DN Attribute** maps the key.

To set Policy Data Source as LDAP using CNC Console GUI:

1. Add LDAP data source. To add LDAP data source, From the navigation menu, under **Policy**, then under **Data Source Configurations**, click **Data Sources**. The Data Sources page opens. Click **Add** to create a data source. On the **Create Data Source** page, select **LDAP** in the **Type** drop-down list.

The following screen capture shows the example of adding LDAP data source in GUI:



Edit Data Sources

Name: ldap1

Description: ldap1

Type: LDAP

Read Connection: Please Select

Primary Server

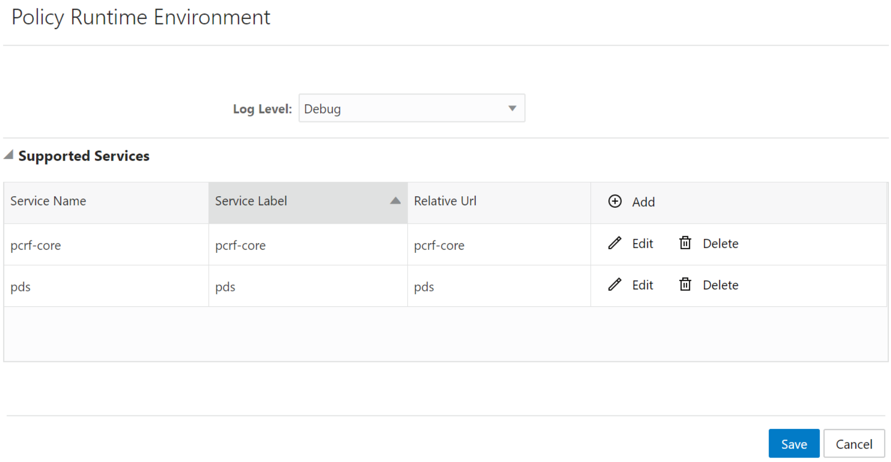
Identity: ldap1.1

Addr: 10.75.235.7

Port: 389

In the above example, LDAP datasource with name **LDAP1** is created.

2. Create **pds** service type in PCF system. To create **pds** service type, From the navigation menu, under **Policy Management**, click **Settings** . On Settings page, click **Add** to create **pds** service type.
   The following screen capture shows the example of creating **pds** service type in GUI:



Policy Runtime Environment

Log Level: Debug

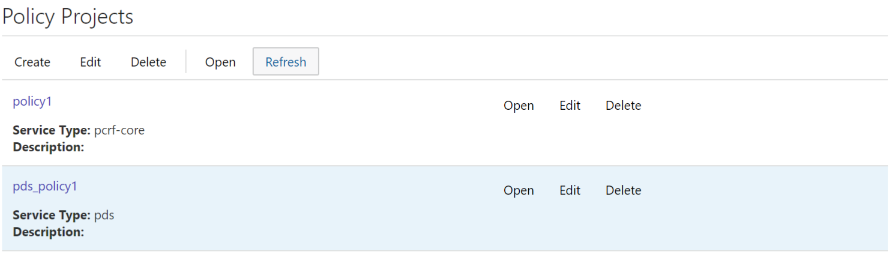
Supported Services

Service Name	Service Label	Relative Url	⊕ Add
pcrf-core	pcrf-core	pcrf-core	Edit Delete
pds	pds	pds	Edit Delete

In the above example, **pds** service type is created.

> **Note:**
>
> The service name should be entered as **pds**.

3. Create Policy Project with **pds** Service Type. From the navigation menu, under **Policy Management**, click **Policy Projects**. On Policy Projects page, click **Create** to create policy project. While creating a policy project select **pds** as a service type.
   The following screen capture shows the example of creating policy project with **pds** service type in GUI:



policy1

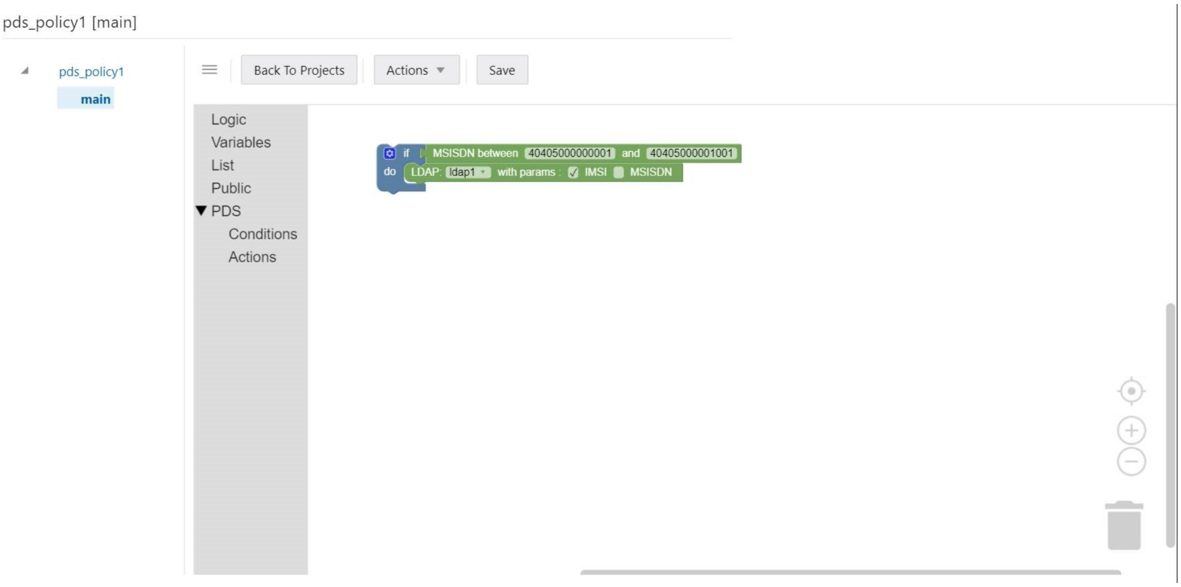
Service Type: pcrf-core
Description:

pds_policy1

Service Type: pds
Description:

In the above example, **s** policy project is created with pds service type.

4. Create policy action and condition in previously created policy project. Click **Open** for the selected policy project and you can see the project is a file. You can create the policy action and condition by using the different blocks available under **Conditions** and **Actions** under **PDS**.
   The following screen capture shows the example of creating policy action and condition in GUI:



if MSISDN between 404050000000001 and 404050000001001
do LDAP: ldap1 with params : ☑ IMSI □ MSISDN

In the above example, if request received for configured IMSI ranges between 404050000000001 and 404050000000001, then PCF will forward request to PDS and PDS will forward the request to LDAP gateway to lookup user information in LDAP1.

Administration

This section describes how to perform administration tasks such as bulk import and bulk export of configurable objects into the system.

Bulk Export/Bulk Import

This section describes how to perform a bulk export and bulk import of managed objects (MOs).

In Release 1.8.x, you can use either of the modes to bulk export and bulk import all the MO's configurations:

- Using GUI to export and import the MO's configuration data
- Using REST APIs to export and import the MO's configuration data

Exporting Managed Object Files Using GUI

To export the MO's configuration data using GUI:

1. From the navigation pane, click **Policy**, and then **Administration**, and then **Import & Export**.
   The **Export** and **Import** tabs appear on the screen.
2. Click **Export** to export the configuration data.
   The **Export Data** dialog box opens containing a list of the managed objects to be exported.
3. Click **Export** in the dialog box.

   > **Note:**
   >
   > You can not select the managed objects in the **Export Data** dialog box in Release 1.8.x.

   All the configurations related to the managed objects are exported and a row is created in the Export status table displaying the export status with the additional details as follows:

   - A new **Export Resource Id** is generated for each export action using which you get the export status.
   - The export status table auto refreshes till the progress reaches 100%.
   - The **Creation TimeStamp** gives the timestamp at which the Export ResourceId got generated.
   - The **Progress (%)** shows the Progress Bar percentage done.
   - The **Actions** cloumn has 2 buttons. These buttons will be enabled once the status is **DONE**.
     - **Downloading Exported Configurations**: Click folder button to download the exported configurations in Zip format containing MO's data in JSON files.
     - **Downlaoding Export Report**: Click Report button to download the report of exported files in .txt format giving details about the MO's exported.
   - Below are the status displayed by bulk export:
     - **IN_PROGRESS**: If the export is running.
     - **DONE**: If the export is finished. Following are the possible value of **RESULT** field if the export is in **DONE** status:
       - **SUCCESS** : If the export is successful

        * **FAILED** : If the export is failed
        * **PARTIAL_SUCCESS** : If the export is partially successful

For more information on Bulk Export REST APIs, see *Oracle Communications Cloud Native Core Policy REST Specification Document*.

Importing Managed Object Files Using GUI

To import json or ZIP files:

1. From the navigation pane, click **Policy**, and then **Administration**, and then **Import & Export**.
   The **Export** and **Import** tabs appear on the screen.
2. Click **Import**.
   The **Import Data** dialog box opens.
3. Locate the file to be imported.

   > **Note:**
   >
   > You can not select the managed objects in the **Import Data** dialog box in Release 1.8.x.

4. Select a processing option to use to **Handle collisions between imported items and existing items**:
   - **Ignore records already present in DB from overwrite** For each object in the import file, if the object exists in the system, the import does not update the object with the configuration contained in the import file. If an object does not exist, the system adds the object to the system.
   - **Replace all the records** For each object in the import file, if the object exists in the system, the import updates the object with the configuration contained in the import file. If an object does not exist, the system adds the object to the system.
5. Click **Import**.

The configuration objects and their configuration settings are imported into the database. After the import is complete, the window reports the results for each json file contained in the ZIP file.

- A new **Import ResourceId** is generated for each export action using which you get the import status.
- The import status table auto refreshes till the progress reaches 100%.
- The **Creation TimeStamp** gives the timestamp at which the Import ResourceId got generated.
- The **Progress (%)** shows the Progress Bar percentage done.
- The **Actions** cloumn has one button. This button will be enabled once the status is **DONE**. Click Report button to download the report of exported files in .txt format giving details about the Mo's imported.
- Below are the status displayed by bulk import:
  – **IN_PROGRESS**: If the import is running.

- **DONE**: If the import is finished. Following are the possible value of **RESULT** field if the import is in **DONE** status:
  - **SUCCESS** : If the import is successful
  - **FAILED** : If the import is failed
  - **PARTIAL_SUCCESS** : If the import is partially successful

For more information on Bulk Import REST APIs, see *Oracle Communications Cloud Native Core Policy REST Specification Document*.

Curl Commands for Bulk Import and Bulk Export

Import: curl -X POST "http://<ipAddress>:<port>/oc-cnpolicy-configuration/v1/administration/import" -H "accept: */*" -H "Content-Type: multipart/form-data" -F "importFile=@<exported zip file name>;type=application/x-zip-compressed"

where, <exported zip file name> specifies name of the zip file to be exported.

Import Report: curl -X GET "http://<ipAddress>:<port>/oc-cnpolicy-configuration/v1/administration/import/<importResourceId>/report" -H "accept: application/octet-stream"

Import Status: curl -X GET "http://<ipAddress>:<port>/oc-cnpolicy-configuration/v1/administration/import/<importResourceId>/status" -H "accept: application/json"

Export : curl -X POST "http://<ipAddress>:<port>/oc-cnpolicy-configuration/v1/administration/export" -H "accept: */*" -d ""

Download: curl -X GET "http://<ipAddress>:<port>/oc-cnpolicy-configuration/v1/administration/export/<exportResourceId>/download" -H "accept: application/octet-stream"

Export Report: curl -X GET "http://<ipAddress>:<port>/oc-cnpolicy-configuration/v1/administration/export/<exportResourceId>/report" -H "accept: application/octet-stream"

Export Status: curl -X GET "http://<ipAddress>:<port>/oc-cnpolicy-configuration/v1/administration/export/<exportResourceId>/status" -H "accept: application/json"

Support for Spending Limit Pending Counter

Policy solution enables you to use activation time in 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 in this release.

In the below Spending Limit Pending Counter Sample:, PCF selects one of policy counter by policyCounterId and and policyCounterStatus, then use the activationTime as the activationTime and/or deactivationTime of Condition Data of PCC Rule or Session Rule, and finally send the related PCC Rule or Session Rule to SMF.

```
{
 "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"
 }
 ]
 }
 ]
}
```

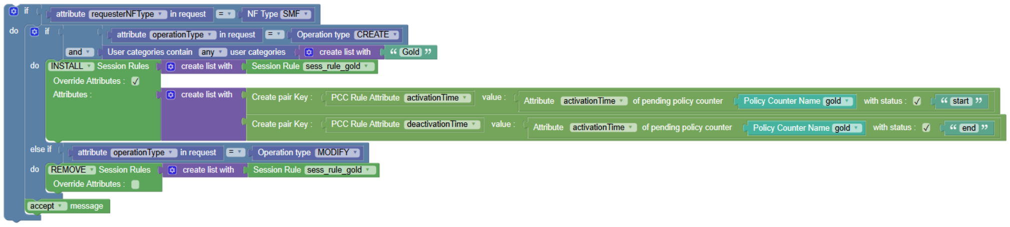
See Configuring Policy Counter Id, Configuring Condition Data, Configuring PCC Rule, and Configuring Session Rule for the configuration details of Policy Counter ID, Condition Data, PCC Rule, and Session Rule.

The existing policies are extended to support using the spending limit pending counter. The policy changes supports:

1. Select the activationTime of pending counter by policyCounterIdand and policyCounterStatus.
2. 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.
3. 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 Communcations Cloud Native Core Policy Design Guide*.

A Policy Sample, this sample is used to install session rule using policy pending counter from the above sample.



```
if   attribute requesterNFType in request  =  NF Type SMF
do   if      attribute operationType in request  =  Operation type CREATE
         and  User categories contain any user categories   create list with  " Gold "
     do   INSTALL Session Rules   create list with   Session Rule sess_rule_gold
            Override Attributes : ✓
            Attributes :          create list with   Create pair Key :  PCC Rule Attribute activationTime  value :  Attribute activationTime of pending policy counter  Policy Counter Name gold  with status : ✓  " start "
                                                     Create pair Key :  PCC Rule Attribute deactivationTime  value :  Attribute activationTime of pending policy counter  Policy Counter Name gold  with status : ✓  " end "
     else if   attribute operationType in request  =  Operation type MODIFY
     do   REMOVE Session Rules   create list with   Session Rule sess_rule_gold
            Override Attributes : □
     accept message
```

7 Policy Alerts

This section provides information on policy alerts and their configuration. It includes:

- PCF Alerts
- PCRF Alerts

Policy Control Function Alerts

This section includes information about alerts for PCF.

Table 7-1 Common Alerts

Alert Name	Description	Severity
PCF_SERVICES_DOWN	Alert if any PCF service down for 5mins for given namespace in AlertRules file	Critical
IngressErrorRateAbove10PercentPerPod	Alert if ingress error rate on each pod above 10%	Critical

Table 7-2 SM Service Alerts

Alert Name	Description	Severity
SMTrafficRateAboveThreshold	Alert if Ingress traffic on SM service reaches 90% of max MPS in 2mins	Major
SMIngressErrorRateAbove10Percent	Alert if Ingress transaction error rate exceeds 10% of all SM transactions in last 24 hours	Critical
SMEgressErrorRateAbove1Percent	Alert if Egress transaction error rate exceeds 1% of all SM transactions in last 24 hours	Minor

Table 7-3 Diameter Connector Alerts

Alert Name	Description	Severity
DiamTrafficRateAboveThreshold	Alert if Diameter Connector traffic reaches 90% of max MPS	Major
DiamIngressErrorRateAbove10Percent	Alert if error rate exceeds 10% of all Diameter transactions in last 24 hours	Critical
DiamEgressErrorRateAbove1Percent	Alert if Egress transaction error rate exceeds 1% of all Diameter transactions	Minor

Table 7-4 User Service - UDR Alerts

Alert Name	Description	Severity
PcfUdrIngressTrafficRateAboveThreshold	Alert if Ingress traffic from UDR reaches 90% of max MPS	Major
PcfUdrEgressErrorRateAbove10Percent	Alert if error rate exceeds 10% of all UDR transactions	Critical

Table 7-5 User Service - CHF Alerts

Alert Name	Description	Severity
PcfChfIngressTrafficRateAboveThreshold	Alert if Ingress traffic from CHF reaches 90% of max MPS	Major
PcfChfEgressErrorRateAbove10Percent	Alert if error rate exceeds 10% of all CHF transactions	Critical

Table 7-6 PolicyDS Service Alerts

Alert Name	Description	Severity
PolicyDsIngressTrafficRateAboveThreshold	Alert if Ingress traffic reaches 90% of max MPS	Major
PolicyDsIngressErrorRateAbove10Percent	Alert if Ingress error rate exceeds 10% of all PolicyDS transactions	Critical
PolicyDsEgressErrorRateAbove1Percent	Alert if Egress error rate exceeds 10% of all PolicyDS transactions	Minor

Table 7-7 Binding Service Alerts

Alert Name	Description	Severity
BindingServiceIngressTrafficRateAboveThreshold	Alert if Ingress traffic reaches 90% of max MPS	Major
BindingServiceIngressErrorRateAbove10Percent	Alert if Ingress error rate exceeds 10% of all Binding Service transactions	Critical
BindingServiceEgressErrorRateAbove1Percent	Alert if Egress error rate exceeds 10% of all BindingService transactions	Minor

PCF Alert Configuration

This section describes the Measurement based Alert rules configuration for PCF. The Alert Manager uses the Prometheus measurements values as reported by microservices in conditions under alert rules to trigger alerts.

PCF Alert Configuration

> **Note:**
>
> - The alertmanager and prometheus tools should run in Oracle CNE namespace, for example, occne-infra.
> - Alert file is packaged with PCF Custom Templates. The **PCF Templates.zip** file can be downloaded from OHC. Unzip the **PCF Templates.zip** file to get **PcfAlertRules.yaml** file.
> - Edit the value of the following parameters in the**PcfAlertRules.yaml** file before following the procedure for configuring the alerts:
>   - **[90% of Max MPS]**.
>   For Example, if the value of **Max MPS** is 10000, set **[90% of Max MPS]** as 9000 in yaml file as follows:
>
>     ```
>     sum(rate(ocpm_ingress_request_total{servicename_3gpp="npcf-smpolicycontrol"}[2m])) >=9000
>     ```
>
>   - **kubernetes_namespace**.
>   For Example,
>
>   If PCF is deployed at more than one site, set **kubernetes_namespace** in yaml file as follows:
>
>     ```
>     expr: up{kubernetes_namespace=~"pcf|ocpcf"} == 0
>     ```
>
>   If PCF is deployed at only one site, set **kubernetes_namespace** in yaml file as follows:
>
>     ```
>     expr: up{kubernetes_namespace="pcf"}==0
>     ```

To Configure PCF alerts in Prometheus:

1. Find the config map to configure alerts in prometheus server by executing the following command:

   ```
   kubectl get configmap -n <Namespace>
   ```

   where, <Namespace> is the prometheus server namespace used in helm install command.

For Example, assuming prometheus server is under **occne-infra** namespace, execute the following command to find the config map:

```
kubectl get configmaps -n occne-infra  | grep prometheus-server
```

Output: occne-prometheus-server 4 46d

2. Take Backup of current config map of prometheus server by executing the following command:

   ```
   kubectl get configmaps <Name> -o yaml -n <Namespace> > /tmp/
   t_mapConfig.yaml
   ```

   where, <Name> is the prometheus config map name used in helm install command.

3. Check if **alertspcf** is present in the **t_mapConfig.yaml** file by executing the following command:

   ```
   cat /tmp/t_mapConfig.yaml  | grep alertspcf
   ```

4. If **alertspcf** is present, delete the **alertspcf** entry from the **t_mapConfig.yaml** file, by executing the following command:

   ```
   sed -i '/etc\/config\/alertspcf/d' /tmp/t_mapConfig.yaml
   ```

   > **Note:**
   >
   > This command should be executed only once.

5. If **alertspcf** is not present, add the **alertspcf** entry in the **t_mapConfig.yaml** file by executing the following command:

   ```
   sed -i '/rule_files:/a\    \- /etc/config/alertspcf'  /tmp/
   t_mapConfig.yaml
   ```

   > **Note:**
   >
   > This command should be executed only once.

6. Reload the config map with the modifed file by executing the following command:

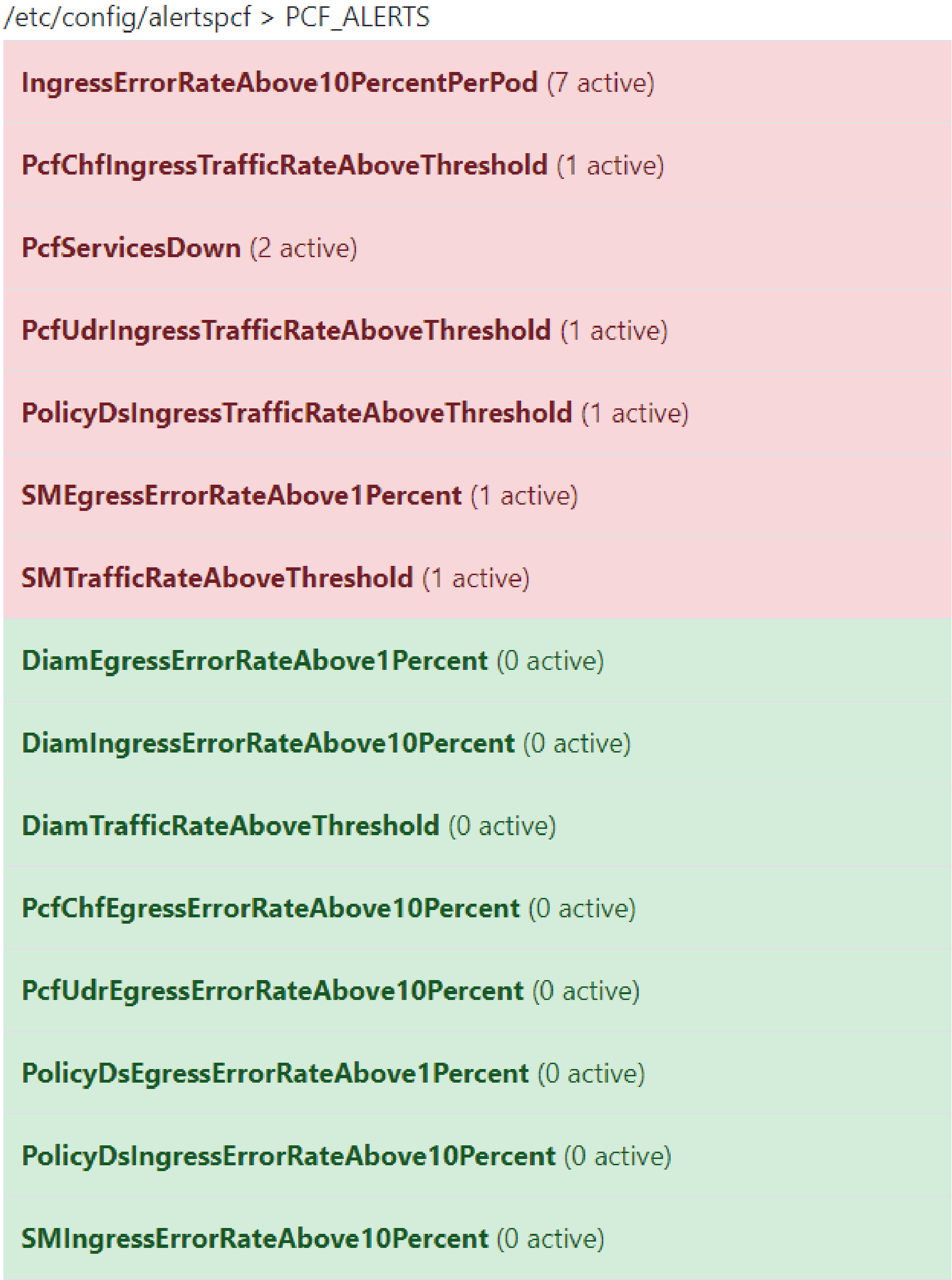
   ```
   kubectl replace configmap <Name> -f /tmp/t_mapConfig.yaml
   ```

7. Add **PcfAlertRules.yaml** file into prometheus config map by executing the following command :

   ```
   kubectl patch configmap <Name> -n <Namespace> --type merge --patch
   "$(cat <PATH>/PcfAlertRules.yaml)"
   ```

where, <PATH> is the location of the **PcfAlertRules.yaml** file.

8. Restart prometheus-server pod.
9. Verify the alerts in prometheus GUI. Below screenshot displays the PCF alerts:



/etc/config/alertspcf > PCF_ALERTS

IngressErrorRateAbove10PercentPerPod (7 active)

PcfChfIngressTrafficRateAboveThreshold (1 active)

PcfServicesDown (2 active)

PcfUdrIngressTrafficRateAboveThreshold (1 active)

PolicyDsIngressTrafficRateAboveThreshold (1 active)

SMEgressErrorRateAbove1Percent (1 active)

SMTrafficRateAboveThreshold (1 active)

DiamEgressErrorRateAbove1Percent (0 active)

DiamIngressErrorRateAbove10Percent (0 active)

DiamTrafficRateAboveThreshold (0 active)

PcfChfEgressErrorRateAbove10Percent (0 active)

PcfUdrEgressErrorRateAbove10Percent (0 active)

PolicyDsEgressErrorRateAbove1Percent (0 active)

PolicyDsIngressErrorRateAbove10Percent (0 active)

SMIngressErrorRateAbove10Percent (0 active)

Cloud Native Policy and Charging Rule Function Alerts

This section includes information about alerts for CNPCRF.

Alarm Name	Alarm Description	Severity	App/Metrics
PRE_UNREACHABLE	PRE is unreachable	CRITICAL	Metrics
PDS_DOWN	PDS is down	CRITICAL	Metrics

Alarm Name	Alarm Description	Severity	App/Metrics
PDS_UP	PDS is up	INFO	Metrics
DB_UNREACHABLE	Connectivity to DB lost	CRITICAL	Metrics
DB_REACHABLE	Connectivity to DB available	INFO	Metrics
SH_UNREACHABLE	Remote Sh connection is unreachable	CRITICAL	App
SY_UNREACHABLE	Remote Sy connection is unreachable	CRITICAL	App
SOAP_CONNECTOR_DOWN	SOAP Connector is down	CRITICAL	Metrics
SOAP_CONNECTOR_UP	SOAP Connector is up	INFO	Metrics
CONFIG_SERVER_DOWN	Config server is down	CRITICAL	Metrics
CONFIG_SERVER_UP	Config server is up	INFO	Metrics
DIAM_GATEWAY_DOWN	Diameter Gateway is down	CRITICAL	Metrics
DIAM_GATEWAY_UP	Diameter Gateway is up	INFO	Metrics
LDAP_GATEWAY_DOWN	LDAP Gateway is down	CRITICAL	Metrics
LDAP_GATEWAY_UP	LDAP Gateway is up	INFO	Metrics
LDAP_DATASOURCE_UNREACHABLE	LDAP Datasource is unreachable	CRITICAL	App
CM_SERVICE_DOWN	CM Service is down	CRITICAL	Metrics
CM_SERVICE_UP	CM Service is up	INFO	Metrics
CCA_SEND_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA Send Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCAI_SEND_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA-I Send Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCAT_SEND_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA-T Send Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCAU_SEND_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA-U Send Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
ASA_SEND_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of ASA Send Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
RAA_SEND_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of RAA Send Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
STA_SEND_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of STA Send Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCA_RECV_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA Receive Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics

Alarm Name	Alarm Description	Severity	App/Metrics
CCAI_RECV_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA-I Receive Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCAT_RECV_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA-T Receive Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCAU_RECV_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of CCA-U Receive Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
ASA_RECV_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of ASA Receive Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
RAA_RECV_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of RAA Receive Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
STA_RECV_FAIL_COUNT_EXCEEDS_THRESHOLD	Rate of STA Receive Failure has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCR_TIMEOUT_COUNT_EXCEEDS_THRESHOLD	Rate of CCR Timeout count has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCRI_TIMEOUT_COUNT_EXCEEDS_THRESHOLD	Rate of CCR-I Timeout count has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCRT_TIMEOUT_COUNT_EXCEEDS_THRESHOLD	Rate of CCR-T Timeout count has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
CCRU_TIMEOUT_COUNT_EXCEEDS_THRESHOLD	Rate of CCR-U Timeout count has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
ASR_TIMEOUT_COUNT_EXCEEDS_THRESHOLD	Rate of ASR Timeout count has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
RAR_TIMEOUT_COUNT_EXCEEDS_THRESHOLD	Rate of RAR Timeout count has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics
STR_TIMEOUT_COUNT_EXCEEDS_THRESHOLD	Rate of STR Timeout count has exceeded threshold limit(1000 times) in 1 min	CRITICAL	Metrics

PCRF Alert Configuration

This section describes the Measurement based Alert rules configuration for CNPCRF. The Alert Manager uses the Prometheus measurements values as reported by microservices in conditions under alert rules to trigger alerts.

PCRF Alert Configuration

To configure cnPCRF alerts in Prometheus:

> **Note:**
>
> 1. The alert manager and prometheus tools should run in the default namespace.
> 2. The PCRF Templates.zip file can be downloaded from OHC. Unzip the package after downloading to get cnpcrfalertrule.yaml and mib files.

1. Find the config map to configure alerts in prometheus server by executing the following command:

   ```
   kubectl get configmap -n Namespace
   ```

   where, *Namespace* is the namespace used in helm install command.
2. Take Backup of current config map of prometheus server by executing the following command:

   ```
   kubectl get configmaps NAME -o yaml -n Namespace  /tmp/
   t_mapConfig.yaml
   ```

   where, *Name* is the release name used in helm install command.
3. Delete the entry **alertscnpcrf** under rule_files, if present, in the Alert Manager config map by executing the following command:

   ```
   sed -i '/etc\/config\/alertscnpcrf/d' /tmp/t_mapConfig.yaml
   ```

   > **Note:**
   >
   > This command should be executed only once.
4. Add entry **alertscnpcrf** under rule_files in the prometheus server config map by executing the following command:

   ```
   sed -i '/rule_files:/a\    \- /etc/config/alertscnpcrf'  /tmp/
   t_mapConfig.yaml
   ```

> **Note:**
>
> This command should be executed only once.

5. Reload the modified config map by executing the following command:

   ```
   kubectl replace configmap <_NAME_> -f /tmp/t_mapConfig.yaml
   ```

   > **Note:**
   >
   > This step is not required for AlertRules.

6. Add cnpcrfAlertrules in config map by executing the following command :

   ```
   kubectl patch configmap _NAME_-server -n _Namespace_--type merge --
   patch
   "$(cat ~/cnpcrfAlertrules.yaml)"
   ```

8 Cloud Native Core Policy Metrics

This chapter includes information about Metrics for Oracle Communications Cloud Native Policy Control Function (PCF).

Ingress Metrics

Below are the different metrics and respective tags that are available for Ingress:

Metric Name	SM Service Tags	UE Service Tags	AM Service Tags	User Service Tags	DIAM-CONN Service Tags	PolicyDS Tags	LDAP Gateway Tags	Binding Tags
ocpm_ingress_request_total	operation_type dnn snssai nf_instance_id sbi_priority servicename_3gpp = ["npcf-smpolicycontrol"," npcf-policyauthorization"]	operation_type service name_ 3gpp = "npcfuepolicycontrol "	operation_type nf_instance_id sbi_priority service name_ 3gpp = "npcfampolicycontrol "	NA	operation_type dnn nf_instance_id servicename_3gpp = ["rx"]	NA	NA	NA
ocpm_userservice_inbound_count_total	NA	NA	NA	operation_type service_resource [udr-service,chf-service,user-service]	NA	NA	NA	NA

Metric Name	SM Service Tags	UE Service Tags	AM Service Tags	User Service Tags	DIAM-CONN Service Tags	PolicyDS Tags	LDAP Gateway Tags	Binding Tags
ocpm_ingress_response_total	operation_type dnn snssai nf_instance_id sbi_priority servicename_3gpp = ["npcf-smpolicycontrol","npcf-policyauthorization"] response_code	operation_type servicename_3gpp = "npcf-ue-policy-control" response_code	operation_type nf_instance_id sbi_priority servicename_3gpp = "npcf-am-policy-control" response_code	NA	operation_type nf_instance_id dnn servicename_3gpp = ["rx"] response_code	NA	NA	NA
client_request_total	NA	NA	NA	NA	NA	operation task	NA	NA
client_response_total	NA	NA	NA	NA	NA	operation task response	code	NA
ldap_request_total	NA	NA	NA	NA	NA	NA	code	NA
ocpm_binding_inbound_request_total	NA	NA	NA	NA	NA	NA	NA	operation_type servicename_3gpp

Egress Metrics

Below are the different metrics and respective tags that are available for Egress:

Metric Name	SM Service Tags	UE Service Tags	AM Service Tags	User Service Tags	DIAM-CONN Service Tags	PolicyDS Tags	LDAP Gateway Tags	Binding Tags
ocpm_egress_request_total	operation_type dnn snssai nf_instance_id sbi_priority servicename_3gpp = ["npcf-smpolicycontrol","npcf-policyauthorization"]	operation_type dnn snssai nf_instance_id sbi_priority servicename_3gpp = ["namf-comm", "npcf-ue-policy-control"]	operation_type nf_instance_id sbi_priority servicename_3gpp = "npcf-am-policy-control"	NA	operation_type dnn nf_instance_id servicename_3gpp = ["rx"]	NA	NA	NA
ocpm_udr_tracking_request_total	NA	NA	NA	operation_type nf_instance_id servicename_3gpp= ["nudr-dr"] service_resource ["policy-data"] service_version ["v1,v2"] service_subresource [am-data, sm-data, ue-policy-set, subs-to-notify]	NA	NA	NA	NA

Metric Name	SM Service Tags	UE Service Tags	AM Service Tags	User Service Tags	DIAM-CONN Service Tags	PolicyDS Tags	LDAP Gateway Tags	Binding Tags
ocpm_chf_tracking_request_total	NA	NA	NA	operation_type nf_instance_id servicename_3gpp= ["nchf-spendinglimitcontrol"] service_resource ["subscriptions"] service_version ["v1,v1"]	NA	NA	NA	NA
ocpm_egress_response_total	operation_type dnn snssai nf_instance_id sbi_priority servicename_3gpp = ["npcf-smpolicycontrol"," npcf-policyauthorization"] response_code latency	operation_type dnn snssai nf_instance_id sbi_priority servicename_3gpp = ["namf-comm", "npcf-ue-policy-control"] response_code latency	operation_type nf_instance_id sbi_priority servicename_3gpp = ["npcf-am-policy-control"] response_code latency	NA	operation_type nf_instance_id dnn servicename_3gpp = ["rx"] response_code	NA	NA	NA

Metric Name	SM Service Tags	UE Service Tags	AM Service Tags	User Service Tags	DIAM-CONN Service Tags	PolicyDS Tags	LDAP Gateway Tags	Binding Tags
ocpm_udr_tracking_response_total	NA	NA	NA	operation_type nf_instance_id 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	NA	NA	NA	NA
ocpm_chf_tracking_response_total	NA	NA	NA	operation_type nf_instance_id servicename_3gpp= ["nchf-spendinglimitcontrol"] service_resource ["subscriptions"] service_version ["v1"] response_code	NA	NA	NA	NA

Metric Name	SM Service Tags	UE Service Tags	AM Service Tags	User Service Tags	DIAM-CONN Service Tags	PolicyDS Tags	LDAP Gateway Tags	Binding Tags
server_request_total	NA	NA	NA	NA	NA	operation task	NA	NA
server_response_total	NA	NA	NA	NA	NA	operation task response	NA	NA
ldap_response_total	NA	NA	NA	NA	NA	NA	ReqType Code	NA
ocpm_binding_inbound_response_total	NA	NA	NA	NA	NA	NA	NA	operation task response_code

Tag Description

Tags	Description	Values
operation_type	Type of operation	• create • get • put • update • terminate • update_notify • terminate_notify • subscribe • unsubscribe • transfer • resubscribe
dnn	Data Network Name or Access Point Name	
snssai	Single Network Slice Selection Assistance Information	
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.	
nf_instance_Id	Unique id of the nf Instance.	**HTTP interfaces:** • ingress: source nfInstanceId • egress: destination nfInstanceId **Diameter interfaces:** • ingress: Origin-Host AVP • egress: Destination-Host AVP
sbi_priority	Service Based Interface	
service_version	Service version	[UDR = "v1,v2", CHF = "v1"]

SM Service

Examples

1. ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="create",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
2. ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="create",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
3. ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="update",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
4. ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="update",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
5. ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="delete",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol,snssai="11-abc123",} 1.0 ; Type-Counter
6. ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="delete",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
7. ocpm_ingress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="get",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
8. ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="get",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
9. ocpm_egress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="update_notify",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
10. ocpm_egress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",,latency="9",operation_type="update_notify",response_code="2xx",sbi_pri

ority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter

11. ocpm_egress_request_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="terminate_notify",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter
12. ocpm_egress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",latency="6",operation_type="terminate_notify",response_code="4xx",sbi_priority="",servicename_3gpp="npcf-smpolicycontrol",snssai="11-abc123",} 1.0 ; Type-Counter

PA Service

Examples

1. 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
2. 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
3. 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
4. ocpm_ingress_response_total{application="pcf_smservice",dnn="dnn1",nf_instance_id="",operation_type="update",response_code="2xx",sbi_priority="",servicename_3gpp="npcf-policyauthorization",snssai="11-abc123",} 1.0 ; Type-Counter
5. 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
6. 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",} 1.0 ; Type-Counter
7. 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
8. 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",} 1.0 ; Type-Counter

UE Service

Examples

1. ocpm_ingress_request_total{operation_type="get",servicename_3gpp="npcf-ue-policy-control",} 2.0 ; Type-Counter
2. ocpm_ingress_request_total{operation_type="delete",servicename_3gpp="npcf-ue-policy-control",} 2.0 ; Type-Counter
3. ocpm_ingress_response_total{operation_type="get",response_code="5xx",servicename_3gpp="npcf-ue-policy-control",} 4.0 ; Type-Counter

4. ocpm_ingress_response_total{operation_type="delete",response_code="4xx",servicename_3gpp="npcf-ue-policy-control",} 2.0 ; Type-Counter
5. ocpm_egress_request_total{operation_type="subscribe",servicename_3gpp="npcf-ue-policy-control",} 1.0 ; Type-Counter
6. ocpm_egress_response_total{operation_type="subscribe",response_code="2xx",servicename_3gpp="npcf-ue-policy-control",} 1.0 ; Type-Counter

AM Service

Examples:

1. ocpm_ingress_response_total{nf_instance_id="",operation_type="create",response_code="2xx",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter
2. ocpm_ingress_request_total{nf_instance_id="",operation_type="create",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter
3. ocpm_ingress_response_total{nf_instance_id="",operation_type="get",response_code="2xx",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter
4. ocpm_ingress_request_total{nf_instance_id="",operation_type="get",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter
5. ocpm_egress_response_total{latency="0",nf_instance_id="",operation_type="terminate_notify",response_code="2xx",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter
6. ocpm_egress_response_total{latency="0",nf_instance_id="",operation_type="update_notify",response_code="2xx",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter
7. ocpm_egress_request_total{nf_instance_id="",operation_type="update_notify",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 2.0 ; Type-Counter
8. ocpm_egress_request_total{nf_instance_id="",operation_type="terminate_notify",sbi_priority=" ",servicename_3gpp="npcf-am-policy-control/v1",} 1.0 ; Type-Counter

User Service

Examples

1. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="post",service_resource="udr-service",} 0.0 ; Type-Counter
2. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="get",service_resource="chf-service",} 0.0 ; Type-Counter
3. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="get",service_resource="udr-service",} 0.0 ; Type-Counter
4. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="notify",service_resource="chf-service",} 0.0 ; Type-Counter
5. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="delete",service_resource="user-service",} 0.0 ; Type-Counter
6. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="get",service_resource="user-service",} 0.0 ; Type-Counter

7. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="notify",service_resource="udr-service",} 0.0 ; Type-Counter
8. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="delete",service_resource="udr-service",} 0.0 ; Type-Counter
9. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="terminate",service_resource="chf-service",} 0.0 ; Type-Counter
10. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="delete",service_resource="chf-service",} 0.0 ; Type-Counter
11. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="patch",service_resource="udr-service",} 0.0 ; Type-Counter
12. ocpm_userservice_inbound_count_total{application="pcf_userservice",operation_type="put",service_resource="udr-service",} 0.0 ; Type-Counter
13. ocpm_ar_setup_total{anchorFqdn="chfanchor.allsim.svc",application="pcf_userservice",scheme="http",} 1.0 ; Type-Counter
14. ocpm_ar_request_total{application="pcf_userservice",fqdn="udmanchor.allsim.svc",scheme="http",} 1.0 ; Type-Counter
15. ocpm_ar_response_total{application="pcf_userservice",fqdn="udmanchor.allsim.svc",responseCode="2xx",scheme="http",} 1.0 ; Type-Counter
16. ocpm_ar_lookup_request_total{anchorFqdn="udmanchor.allsim.svc",application="pcf_userservice",scheme="http",} 1.0 ; Type-Counter
17. ocpm_ar_lookup_response_total{anchorFqdn="udmanchor.allsim.svc",application="pcf_userservice",responseCode="2xx",scheme="http",} 1.0 ; Type-Counter

UDR

1. 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
2. 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
3. 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
4. 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
5. ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",operation_type="subscribe",response_code="2xx",service_resour

ce="policy-data",service_subresource="",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter

6. ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",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
7. ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",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
8. ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",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
9. ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",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
10. ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",operation_type="get",response_code="2xx",service_resource="policy-data",service_subresource="",service_version="v1",servicename_3gpp="nudr-dr",} 0.0 ; Type-Counter
11. ocpm_udr_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-c6d70b1babc1",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

CHF

1. ocpm_chf_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="unsubscribe",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter
2. ocpm_chf_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="put",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter
3. ocpm_chf_tracking_request_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="subscribe",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 1.0 ; Type-Counter

4. ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="subscribe",response_code="5xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter
5. ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="put",response_code="4xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter
6. ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="put",response_code="1xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter
7. ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="unsubscribe",response_code="4xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter
8. ocpm_chf_tracking_response_total{HostName="",application="pcf_userservice",nf_instance_id="fe7d992b-0541-4c7d-ab84-666666666667",operation_type="unsubscribe",response_code="2xx",service_resource="subscriptions",service_version="v1",servicename_3gpp="nchf-spendinglimitcontrol",} 0.0 ; Type-Counter

Diam Connector

1. ocpm_egress_response_total{latency="3",nf_instance_id="AF.oracle.com",operation_type="update_notify",response_code="2xxx",servicename_3gpp="rx",} 1.0 ; Type-Counter
2. ocpm_egress_request_total{nf_instance_id="AF.oracle.com",operation_type="update_notify",servicename_3gpp="rx",} 1.0 ; Type-Counter
3. ocpm_ingress_request_total{apn="",nf_instance_id="AF.oracle.com",operation_type="create",servicename_3gpp="rx",} 5.0 ; Type-Counter
4. ocpm_ingress_response_total{apn="",nf_instance_id="ocpcf",operation_type="create",response_code="2xxx",servicename_3gpp="rx",} 2.0 ; Type-Counter

Diameter Gateway

1. occnp_diam_conn_network{destHost="",destRealm="",origHost="dsr.oracle.com", origRealm="oracle.com",} 1.0 ; Type-Gauge
2. occnp_diam_conn_app_network{appID="16777238",destHost="",destRealm="",origHost="pgw1.oracle.com",origRealm="oracle.com",} 1.0 ; Type-Gauge
3. occnp_diam_conn_app_network{appID="16777236",destHost="",destRealm="",origHost="af.oracle.com",origRealm="oracle.com",} 1.0 ; Type-Gauge
4. occnp_diam_conn_app_network{appID="16777238,16777236",destHost="",destRealm="",origHost="dsr.oracle.com",origRealm="oracle.com",} 1.0 ; Type-Gauge
5. occnp_diam_conn_backend{appType="pcrf",} 1.0 ; Type-Gauge

6. ocpm_egress_request_total{egress_service="Binding",operation_type="read",servicename_3gpp="DiameterGateway",} 1.0 ; Type-Counter
7. ocpm_egress_response_total{egress_service="Binding",latency="9",operation_type="read",response_code="2xx",servicename_3gpp="DiameterGateway",} 1.0 ; Type-Counter

Policy DS

1. client_request_total{application="policyds",operation="SEARCH",workflow="LDAP",} 1.0 ; Type-Counter
2. client_response_total{application="policyds",operation="SEARCH",response="200",workflow="LDAP",} 1.0 ; Type-Counter
3. server_request_total{application="policyds",operation="SEARCH",task="USER_SERVICE",} 1.0 ; Type-Counter
4. server_request_total{application="policyds",operation="GET",task="LDAP",} 1.0 ; Type-Counter
5. server_request_total{application="policyds",operation="INSERT",task="PRE",} 1.0 ; Type-Counter
6. server_response_total{application="policyds",operation="POST",response="200",} 1.0 ; Type-Counter

LDAP Gateway

- ldap_request_total{ReqType="GET",application="ldapgateway"} 13.0 ; Type-Counter
- ldap_response_total{Code="4xx",ReqType="GET",application="ldapgateway"} 0.0 ; Type-Counter
- ldap_response_total{Code="2xx",ReqType="GET",application="ldapgateway"} 13.0 ; Type-Counter
- ldap_response_total{Code="5xx",ReqType="GET",application="ldapgateway"} 0.0 ; Type-Counter

Audit Service

- audit_recs_stale{ServiceName="sm-service",TableName="SmPolicyAssociation"} 55.0 ; Type-Counter
- audit_recs_notif{ServiceName="sm-service"} 50.0 ; Type-Counter
- audit_recs_remv{ServiceName="sm-service",TableName="SmPolicyAssociation"} 5.0 ; Type-Counter
- audit_recs_remv_ex{ServiceName="sm-service",TableName="SmPolicyAssociation"} 0.0 ; Type-Counter
- audit_recs_notif_ex{ServiceName="sm-service"} 0.0 ; Type-Counter
- audit_recs_notif_err{ServiceName="sm-service"} 13.0 ; Type-Counter
- audit_recs_deque_for_notif{ServiceName="sm-service"} 50.0 ; Type-Counter
- audit_recs_enque_for_notif{ServiceName="sm-service"} 50.0 ; Type-Counter
- audit_recs_enque_err{ServiceName="sm-service"} 0.0 ; Type-Counter
- 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_records_count{Service="sm-service",Table="SiteJsonSchemaVersionInfo",} 4.0 ; Type-Gauge

Binding Service

1. ocpm_binding_inbound_response_total{operation_type="delete",response_code="2xx",servicename_3gpp="binding.1.0",} 10.0 ; Type-Counter
2. ocpm_binding_inbound_response_total{operation_type="write",response_code="2xx",servicename_3gpp="binding.1.0",} 91.0 ; Type-Counter
3. ocpm_binding_inbound_response_total{operation_type="read",response_code="4xx",servicename_3gpp="binding.1.0",} 1.0 ; Type-Counter
4. ocpm_binding_inbound_response_total{operation_type="read",response_code="5xx",servicename_3gpp="binding.1.0",} 1.0 ; Type-Counter
5. ocpm_binding_inbound_request_total{operation_type="read",servicename_3gpp="binding.1.0",} 5.0 ; Type-Counter
6. ocpm_binding_inbound_request_total{operation_type="delete",servicename_3gpp="binding.1.0",} 10.0 ; Type-Counter
7. ocpm_binding_inbound_request_total{operation_type="write",servicename_3gpp="binding.1.0",} 91.0 ; Type-Counter