

Oracle® Communications

Cloud Native Core, Converged Policy

Troubleshooting Guide



Release 23.4.9

F89674-10

February 2025

ORACLE®

Copyright © 2020, 2025, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

Contents

1	Introduction	
1.1	Overview	1
1.2	Audience	1
2	Troubleshooting Overview	
2.2	General Problem-solving Models	1
2.3	Preparing for Issues	1
2.1	Symptoms, Problems and Solutions	2
3	Finding Error and Status Information	
3.2	Subscriber Activity Logging	1
3.3	Log Block	1
3.4	Using Debug Tool	2
3.4.1	Debug Tool Configuration Parameters	15
3.1	Logs	18
3.1.1	Log Levels	19
3.1.2	Understanding Logs	27
4	Troubleshooting Policy	
4.2	Database Related Issues	1
4.2.1	Policy MySQL DB Access	1
4.4	Upgrade or Rollback Failure	2
4.1	Deployment Related Issues	3
4.1.1	Helm Install Failure	3
4.1.2	Configuration Issue where mysql-username had an Extra Line	5
4.1.3	App Info Worker Time Out	6
4.1.4	Startup Probes	7
4.1.5	Monitoring of Diameter Gateway worker nodes failure	8
4.3	Service Related Issues	9
4.3.1	SM Service Issues	9
4.3.2	CM Service Issues	19

4.3.3	Audit Service Issues	22
4.3.4	UDR Connector Issues	24
4.3.5	CHF Connector Issues	33

5 Alerts

5.1	Configuring Alerts	1
5.2	Configuring SNMP Notifier	4
5.3	List of Alerts	5
5.3.1	Common Alerts	6
5.3.1.1	PodMemoryDoC	6
5.3.1.2	PodMemoryCongested	6
5.3.1.3	POD_DANGER_OF_CONGESTION	7
5.3.1.4	RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD	7
5.3.1.5	RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD	8
5.3.1.6	RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD	8
5.3.1.7	ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD	9
5.3.1.8	ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD	9
5.3.1.9	ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD	10
5.3.1.10	SCP_PEER_UNAVAILABLE	10
5.3.1.11	SCP_PEER_SET_UNAVAILABLE	11
5.3.1.12	STALE_CONFIGURATION	11
5.3.1.13	POLICY_SERVICES_DOWN	12
5.3.1.14	DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD	12
5.3.1.15	DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT	13
5.3.1.16	DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT	14
5.3.1.17	UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD	14
5.3.1.18	UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT	15
5.3.1.19	POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD	16
5.3.1.20	POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT	17
5.3.1.21	POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT	17
5.3.1.22	UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD	18
5.3.1.23	DB_TIER_DOWN_ALERT	19
5.3.1.24	CPU_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD	19
5.3.1.25	CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD	20
5.3.1.26	CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD	21
5.3.1.27	MemoryUsagePerServiceAboveMinorThreshold	22
5.3.1.28	MEMORY_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD	22
5.3.1.29	MEMORY_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD	23
5.3.1.30	POD_CONGESTED	24
5.3.1.31	POD_DANGER_OF_CONGESTION	24
5.3.1.32	POD_PENDING_REQUEST_CONGESTED	25

5.3.1.33	POD_PENDING_REQUEST_DANGER_OF_CONGESTION	25
5.3.1.34	POD_CPU_CONGESTED	26
5.3.1.35	POD_CPU_DANGER_OF_CONGESTION	27
5.3.1.36	SERVICE_OVERLOADED	27
5.3.1.37	SERVICE_RESOURCE_OVERLOADED	28
5.3.1.38	SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD	33
5.3.1.39	SYSTEM_IMPAIRMENT_MAJOR	34
5.3.1.40	SYSTEM_IMPAIRMENT_CRITICAL	35
5.3.1.41	SYSTEM_OPERATIONAL_STATE_NORMAL	35
5.3.1.42	SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN	36
5.3.1.43	SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN	36
5.3.1.44	TDF_CONNECTION_DOWN	37
5.3.1.45	DIAM_CONN_PEER_DOWN	37
5.3.1.46	DIAM_CONN_NETWORK_DOWN	37
5.3.1.47	DIAM_CONN_BACKEND_DOWN	38
5.3.1.48	PerfInfoActiveOverloadThresholdFetchFailed	38
5.3.1.49	SLASYFailCountExceedsCriticalThreshold	39
5.3.1.50	SLASYFailCountExceedsMajorThreshold	39
5.3.1.51	SLASYFailCountExceedsMinorThreshold	40
5.3.1.52	STASYFailCountExceedsCriticalThreshold	40
5.3.1.53	STASYFailCountExceedsMajorThreshold	41
5.3.1.54	STASYFailCountExceedsMinorThreshold	41
5.3.1.55	SMSC_CONNECTION_DOWN	42
5.3.1.56	STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD	42
5.3.1.57	STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD	43
5.3.1.58	STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD	43
5.3.1.59	SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD	44
5.3.1.60	SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD	44
5.3.1.61	SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD	45
5.3.2	PCF Alerts	46
5.3.2.1	INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD	46
5.3.2.2	SM_TRAFFIC_RATE_ABOVE_THRESHOLD	46
5.3.2.3	SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT	47
5.3.2.4	SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT	48
5.3.2.5	PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD	48
5.3.2.6	PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT	49
5.3.2.7	PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD	50
5.3.2.8	PCF_PENDING_BINDING_SITE_TAKEOVER	51
5.3.2.9	PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED	51
5.3.2.10	PCF_PENDING_BINDING_RECORDS_COUNT	51
5.3.2.11	TDF_CONNECTION_DOWN	52
5.3.2.12	AUTONOMOUS_SUBSCRIPTION_FAILURE	52

5.3.2.13	AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT	53
5.3.2.14	AM_AR_ERROR_RATE_ABOVE_1_PERCENT	53
5.3.2.15	UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT	53
5.3.2.16	UE_AR_ERROR_RATE_ABOVE_1_PERCENT	54
5.3.3	PCRF Alerts	54
5.3.3.1	PreUnreachableExceedsThreshold	54
5.3.3.2	PcrfDown	56
5.3.3.3	CCAFailCountExceedsThreshold	56
5.3.3.4	AAAFailCountExceedsThreshold	57
5.3.3.5	RAARxFailCountExceedsThreshold	59
5.3.3.6	RAAGxFailCount ExceedsThreshold	60
5.3.3.7	ASAFailCountExceedsThreshold	61
5.3.3.8	ASATimeoutICountExceedsThreshold	63
5.3.3.9	RAARxTimeoutCountExceedsThreshold	64
5.3.3.10	RAARxTimeoutCountExceedsThreshold	66
5.3.3.11	ResponseErrorRateAbovePercent	67
5.3.3.12	RxResponseErrorRateAbovePercent	69
5.3.3.13	GxResponseErrorRateAbovePercent	70

My Oracle Support

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

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

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

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

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

Acronyms

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

Table Acronyms and Terminologies

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

Table (Cont.) Acronyms and Terminologies

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

What's New in This Guide

This section introduces the documentation updates for release 23.4.x.

Release 23.4.9 - F89674-10, February 2025

There are no changes to this document in this release.

Release 23.4.8 - F89674-09, November 2024

There are no changes to this document in this release.

Release 23.4.7 - F89674-08, October 2024

There are no changes to this document in this release.

Release 23.4.6 - F89674-07, September 2024

There are no changes to this document in this release.

Release 23.4.5 - F89674-06, August 2024

There are no changes to this document in this release.

Release 23.4.4 - F89674-05, July 2024

There are no changes to this document in this release.

Release 23.4.3 - F89674-04, April 2024

There are no changes to this document in this release.

Release 23.4.2 - F89674-03, March 2024

There are no changes to this document in this release.

Release 23.4.1 - F89674-02, February 2024

There are no changes to this document in this release.

Release 23.4.0 - F89674-01, December 2023

The following updates are made in this release:

- Added following alerts for the Bulwark Pod Congestion Control feature:
 - PodDoc
 - PodPendingRequestDoC
 - PodCPUDoC
- Added following alerts for the Diameter Session Retry feature:
 - RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
 - RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
 - RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD
 - ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

- ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
- ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

1

Introduction

This document provides information about troubleshooting Oracle Communications Cloud Native Core, Converged Policy services and managed objects.

1.1 Overview

Oracle Communications Cloud Native Core Policy (Policy) is a functional element used by leading telecommunication service providers for policy control decision and flow-based charging control functionalities. To achieve the mentioned functionalities along with performing other functions, Policy employs a bevy of services including Session Management Service, Access and Mobility Service, Policy Authorization Service, PCRF Core Service, etc. Further, the interconnection to other network functions, database types, and various other third-party products make the Policy deployment a complex environment.

The Policy Troubleshooting Guide provides extensive information about resolving problems you might experience while installing and configuring Policy. This document also provides information about tools available to help you collect and analyze diagnostic data.

The Policy Troubleshooting Guide describes in detail common problems that may arise while installing, configuring, and using Policy. After a user has identified the issue, perform the provided steps to resolve the issue.

Note

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

1.2 Audience

Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide provides guidance to network administrators and professionals responsible for deployment and maintenance of Policy.

2

Troubleshooting Overview

This section provides information on how to identify problems and a systematic approach to resolve the identified issues. It also includes a generic checklist that can help users identify the problems in the right manner.

2.2 General Problem-solving Models

When you are troubleshooting an issue specific to Policy, a systematic approach works best. An unsystematic approach may not only result in wasting valuable time and resources, but can sometimes make symptoms even worse. Define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (preferably from the most likely to the least likely) until the symptoms disappear.

To solve a problem, the following steps can be performed:

1. Create a clear and concise problem statement. Identify the general symptoms and then determine what types of problems could result in these systems.
2. Collect information such as messages and logs to isolate possible causes.
3. Using the information collected in the preceding step, create an action plan for the potential problems. Begin with the most likely problem.
4. Implement the action plan, while testing to see whether the symptom disappears.
5. Whenever a variable or default setting is changed, be sure to gather results.
6. Analyze the results to determine whether the problem has been resolved. If it has, then the process is complete.

Note

If the problem does not get resolved, contact [My Oracle Support](#).

2.3 Preparing for Issues

It is pertinent to have current and accurate information about the Policy instances for effective troubleshooting.

If you have a problem with your Policy deployment, try to answer the following questions:

- What exactly is the problem? Can you isolate it?
A clear and concise description of the problem, including when it began to occur helps in identifying the possible causes.
- Does the problem occur on one instance of the application, or all instances?
- What do the log files say?
Check the error log for the Policy services you are having problems with.

- Read through the Policy troubleshooting checklist. Look through the list of common problems and their solutions.
- Has anything changed in the system? Did you install any new component?
- Have you read the Release Notes?
The Release Notes include information about known bugs and workarounds.
- Has your system usage recently jumped significantly?
- Is the application otherwise operating normally?
- Has response time or the level of system resources changed?

2.1 Symptoms, Problems and Solutions

Problems encountered while deploying or configuring Policy are characterized by specific symptoms, which can be either general or highly specific. You can trace symptoms to one or more problems or causes by using specific troubleshooting tools and techniques. After the issue has been identified, series of actions can be performed to resolve the identified problem.

This guide describes how to define symptoms, identify problems, and implement solutions in Oracle Communications Cloud Native Environment. It is recommended to apply the specific context in which you are troubleshooting to determine how to detect symptoms and diagnose problems for your specific environment.

3

Finding Error and Status Information

Effective troubleshooting relies on the availability of useful and detailed information. The Oracle Communications Cloud Native Core, Converged Policy provides various sources of information that may be helpful in the troubleshooting process.

3.2 Subscriber Activity Logging

Subscriber Activity Logging allows you to define a list of the subscribers (identifier) and trace all the logs related to the identified subscribers separately while troubleshooting certain issues. This functionality can be used to troubleshoot problematic subscribers without enabling logs or traces that can impact all subscribers.

To enable the subscriber activity logging functionality, set value of the **Enable Subscriber Activity Logging** parameter to **true** on the **Subscriber Activity Logging** page on the CNC Console. By default, this functionality remains disabled.

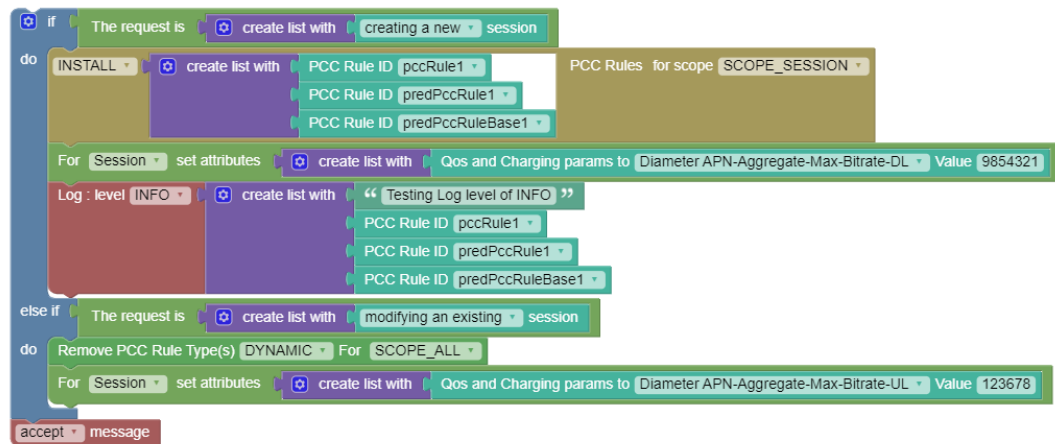
For more information on how to enable this feature, see the section "Subscriber Activity Logging" in *Oracle Communications Cloud Native Core, Converged Policy User's Guide*.

3.3 Log Block

While managing Policy Projects, users can use the **Log** block to log a message or the value of a policy variable in the logging system.

The logged message can subsequently be viewed in Kibana (or other logging) GUI.

The following is a sample policy and the associated log message added in PRE:



```
{
  "messageTimestamp": "2021-07-08T17:54:51.425Z",
  "marker": { "name": "SUBSCRIBER" },
  "level": "INFO",
  "message": {
    "type": "POLICY_EXECUTION",
```

```

    "requestId":"supi;
    imsi-600000000001",
    "policyStartTime":"2021-07-08T17:54:51.423Z",
    "policyEndTime":"2021-07-08T17:54:51.425Z",
    "body":[
      " Start evaluating policy main",
      "request.request.operationType == 'CREATE' evaluates to be true",
      " get row data from table '[Policy Table name]' for service pcf-sm with
conditions column '[Column name]' 'equal to:###eq###'
request.request.smPolicyContextData.dnn",
      " INSTALL PCC Rules [utils.getColumnData((typeof row == "undefined"))?
{rowtableId: "",rowData: null}: row ,
      "[Table name]",
      "[Column name]")]",
      " Execute mandatory action accept message",
      " End evaluating policy main"
    ]
  }"
}

```

For more information on how to use this block, see *Oracle Communications Cloud Native Core, Converged Policy Design Guide*.

3.4 Using Debug Tool

Overview

The Debug Tool provides third-party troubleshooting tools for debugging the runtime issues in the lab environment.

- tcpdump
- ip
- netstat
- curl
- ping
- nmap
- dig

Prerequisites

This section explains the prerequisites for using debug tool.

Note

- For CNE 23.2.0 and later versions, follow [Step a](#) of [#unique_24/unique_24_Connect_42_OL_KVH_YCV_VXB](#).
- For CNE versions prior to 23.2.0, follow [Step b](#) of [#unique_24/unique_24_Connect_42_OL_KVH_YCV_VXB](#).

1. Configuration in CNE

The following configurations must be performed in the Bastion Host.

- a. When Policy is installed on CNE version 23.2.0 or above:

Note

- In CNE version 23.2.0 or above, the default CNE 23.2.0 Kyverno policy, disallow-capabilities, do not allow NET_ADMIN and NET_RAW capabilities that are required for debug tool.
- To run Debug tool on CNE 23.2.0 and above, the user must modify the existing Kyverno policy, disallow-capabilities, as below.

Adding a Namespace to an Empty Resource

- Run the following command to verify if the current disallow-capabilities cluster policy has namespace in it.

Example:

```
$ kubectl get clusterpolicies disallow-capabilities -oyaml
```

Sample output:

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
...
...
spec:
  rules:
    -exclude:
      any:
        -resources: {}
```

- If there are no namespaces, then patch the policy using the following command to add <namespace> under resources.

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
  -p='[{"op": "add", "path": "/spec/rules/0/exclude/any/0/
resources", "value": {"namespaces":["<namespace>"]} }]'
```

Example:

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
  -p='[{"op": "add", "path": "/spec/rules/0/exclude/any/0/
resources", "value": {"namespaces":["occnp"]} }]'
```

Sample output:

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
...
...
spec:
```

```
rules:
-exclude:
  resources:
    namespaces:
    -ocnp
```

- If in case it is needed to remove the namespace added in the above step, use the following command:

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
-p='[{"op": "replace", "path": "/spec/rules/0/exclude/any/0/
resources", "value": {} }]'
```

Sample output:

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
...
...
spec:
  rules:
    -exclude:
      any:
      -resources: {}
```

Adding a Namespace to an Existing Namespace List

- Run the following command to verify if the current disallow-capabilities cluster policy has namespaces in it.

Example:

```
$ kubectl get clusterpolicies disallow-capabilities -oyaml
```

Sample output:

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
...
...
spec:
  rules:
    -exclude:
      any:
      -resources:
        namespaces:
        -namespace1
        -namespace2
        -namespace3
```

- ii. If there are namespaces already added, then patch the policy using the following command to add <namespace> to the existing list:

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
  -p='[{"op": "add", "path": "/spec/rules/0/exclude/any/0/resources/
namespaces/-", "value": "<namespace>" }]'
```

Example:

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
  -p='[{"op": "add", "path": "/spec/rules/0/exclude/any/0/resources/
namespaces/-", "value": "ocnp" }]'
```

Example:

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
  -p='[{"op": "add", "path": "/spec/rules/0/exclude/any/0/resources/
namespaces/-", "value": "ocnp" }]'
```

Sample output:

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
...
spec:
  rules:
    -exclude:
      resources:
        namespaces:
          -namespace1
          -namespace2
          -namespace3
          -ocnp
```

- iii. If in case it is needed to remove the namespace added in the above step, use the following command:

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
  -p='[{"op": "remove", "path": "/spec/rules/0/exclude/any/0/
resources/namespaces/<index>"}]'
```

Example:

```
$ kubectl patch clusterpolicy disallow-capabilities --type=json \
  -p='[{"op": "remove", "path": "/spec/rules/0/exclude/any/0/
resources/namespaces/3"}]'
```

Sample output:

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
```

```
...
...
spec:
  rules:
    -exclude:
      resources:
        namespaces:
        -namespace1
        -namespace2
        -namespace3
```

Note

While removing the namespace, provide the index value for namespace within the array. The index starts from '0'.

b. When Policy is installed on CNE version prior to 23.2.0

PodSecurityPolicy (PSP) Creation

- i. Log in to the Bastion Host.
- ii. Create a new PSP by running the following command from the bastion host. The parameters **readOnlyRootFilesystem**, **allowPrivilegeEscalation**, **allowedCapabilities** are required by debug container.

Note

Other parameters are mandatory for PSP creation and can be customized as per the CNE environment. **Default values** are recommended.

```
$ kubectl apply -f - <<EOF

apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: debug-tool-psp
spec:
  readOnlyRootFilesystem: false
  allowPrivilegeEscalation: true
  allowedCapabilities:
    - NET_ADMIN
    - NET_RAW
  fsGroup:
    ranges:
      - max: 65535
        min: 1
    rule: MustRunAs
  runAsUser:
    rule: MustRunAsNonRoot
  seLinux:
    rule: RunAsAny
```

```
    supplementalGroups:
      rule: RunAsAny
    volumes:
      - configMap
      - downwardAPI
      - emptyDir
      - persistentVolumeClaim
      - projected
      - secret
EOF
```

Role Creation

Run the following command to create a role for the PSP:

```
$ kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: debug-tool-role
  namespace: ocnrf
rules:
- apiGroups:
  - policy
  resources:
  - podsecuritypolicies
  verbs:
  - use
  resourceNames:
  - debug-tool-psp
EOF
```

RoleBinding Creation

Run the following command to associate the service account for the Policy namespace with the role created for the PSP:

```
$ kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: debug-tool-rolebinding
  namespace: ocnrf
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: debug-tool-role
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: system:serviceaccounts
EOF
```

Refer to [Debug Tool Configuration Parameters](#) for parameter details.

2. Configuration in NF specific Helm

Following updates must be performed in `custom_values.yaml` file.

- a. Log in to the Policy server.
- b. Open the `custom_values.yaml` file:

```
$ vim <custom_values file>
```

- c. Under global configuration, add the following:

```
global:
  extraContainers: ENABLED
```

Note

- Debug Tool Container comes up with the default user ID - 7000. If the operator wants to override this default value, it can be done using the ``runAsUser`` field, otherwise the field can be skipped.

Default value: `uid=7000(debugtool) gid=7000(debugtool)`
`groups=7000(debugtool)`

- In case you want to customize the container name, replace the ``name`` field in the above values.yaml with the following:

```
name: {{ printf "%s-tools-%s" (include "getprefix" .)
(include "getsuffix" .) | trunc 63 | trimPrefix "-" |
trimSuffix "-" }}
```

This will ensure that the container name is prefixed and suffixed with the necessary values.

For more information on how to customize parameters in the custom yaml value files, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade and Fault Recovery Guide*.

- d. Under service specific configurations for which debugging is required, add the following:

```
am-service:
  #extraContainers: DISABLED
  envMySQLDatabase: occnp_pcf_am
  resources:
    limits:
      cpu: 1
      memory: 1Gi
    requests:
      cpu: 0.5
      memory: 1Gi
  minReplicas: 1
```

Note

- At the global level, `extraContainers` flag can be used to enable/disable injecting extra containers globally. This ensures that all the services that use this global value have extra containers enabled/disabled using a single flag.
- At the service level, `extraContainers` flag determines whether to use the extra container configuration from the global level or enable/disable injecting extra containers for the specific service.

Running Debug Tool

To run Debug Tool, perform the following steps:

1. Run the following command to retrieve the POD details:

```
$ kubectl get pods -n <namespace>
```

Example:

```
$ kubectl get pods -n occnp
```

2. Run the following command to enter into Debug Tool Container:

```
$ kubectl exec -it <pod name> -c <debug_container name> -n <namespace> bash
```

3. Run the debug tools:

```
bash -4.2$ <debug_tools>
```

Example:

```
bash -4.2$ tcpdump
```

4. Copy the output files from container to host:

```
$ kubectl cp -c <debug_container name> <pod name>:<file location in container> -n <namespace> <destination location>
```

Tools Tested in Debug Container

Following is the list of debug tools that are tested.

tcpdump

Table 3-1 tcpdump

Options Tested	Description	Output	Capabilities
-D	Print the list of the network interfaces available on the system and on which <i>tcpdump</i> can capture packets.	<pre>tcpdump -D 1.eth0 2.nflog (Linux netfilter log (NFLOG) interface) 3.nfqueue (Linux netfilter queue (NFQUEUE) interface) 4.any (Pseudo-device that captures on all interfaces) 5.lo [Loopback]</pre>	NET_ADMIN, NET_RAW
-i	Listen on <i>interface</i> .	<pre>tcpdump -i eth0 tcpdump: verbose output suppressed, use -v or -vv for full protocol decodelistening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes12:10:37.381199 IP cncc-core-ingress-gateway-7ffc49bb7f-2kkhc.46519 > kubernetes.default.svc.cluster.local.https: Flags [P], seq 1986927241:1986927276, ack 1334332290, win 626, options [nop,nop,TS val 849591834 ecr 849561833], length 3512:10:37.381952 IP cncc-core-ingress- gateway-7ffc49bb7f-2kkhc.45868 > kube-dns.kube- system.svc.cluster.local.domain: 62870+ PTR? 1.0.96.10.in- addr.arpa. (40)</pre>	NET_ADMIN, NET_RAW
-w	Write the raw packets to file rather than parsing and printing them.	<pre>tcpdump -w capture.pcap -i eth0</pre>	NET_ADMIN, NET_RAW
-r	Read packets from <i>file</i> (which was created with the -w option).	<pre>tcpdump -r capture.pcap reading from file /tmp/capture.pcap, link-type EN10MB (Ethernet)12:13:07.381019 IP cncc-core-ingress- gateway-7ffc49bb7f-2kkhc.46519 > kubernetes.default.svc.cluster.local.https: Flags [P], seq 1986927416:1986927451, ack 1334332445, win 626, options [nop,nop,TS val 849741834 ecr 849711834], length 3512:13:07.381194 IP kubernetes.default.svc.cluster.local.https > cncc-core- ingress-gateway-7ffc49bb7f-2kkhc.46519: Flags [P], seq 1:32, ack 35, win 247, options [nop,nop,TS val 849741834 ecr 849741834], length 3112:13:07.381207 IP cncc-core- ingress-gateway-7ffc49bb7f-2kkhc.46519 > kubernetes.default.svc.cluster.local.https: Flags [.], ack 32, win 626, options [nop,nop,TS val 849741834 ecr 849741834], length 0</pre>	NET_ADMIN, NET_RAW

ip

Table 3-2 ip

Options Tested	Description	Output	Capabilities
addr show	Look at protocol addresses	ip addr show 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaultlink/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00inet 127.0.0.1/8 scope host lovalid_lft forever preferred_lft forever2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group defaultlink/ipip 0.0.0.0 brd 0.0.0.04: eth0@if190: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1440 qdisc noqueue state UP group defaultlink/ether aa:5a:27:8d:74:6f brd ff:ff:ff:ff:ff:ff link-netnsid 0inet 192.168.219.112/32 scope global eth0valid_lft forever preferred_lft forever	--
route show	List routes	ip route show default via 169.254.1.1 dev eth0 169.254.1.1 dev eth0 scope link	--
addrlabel list	List address labels	ip addrlabel list prefix ::1/128 label 0 prefix ::/96 label 3 prefix ::ffff:0.0.0.0/96 label 4 prefix 2001::/32 label 6 prefix 2001:10::/28 label 7 prefix 3ffe::/16 label 12 prefix 2002::/16 label 2 prefix fec0::/10 label 11 prefix fc00::/7 label 5 prefix ::/0 label 1	--

netstat

Table 3-3 netstat

Options Tested	Description	Output	Capabilities
-a	Show both listening and non-listening (for TCP this means established connections) sockets.	netstat -a Active Internet connections (servers and established) Proto Recv-Q Send-Q Local Address Foreign Address Statetcp 0 0 0.0.0.0:tpoxy 0.0.0.0:* LISTENTcp 0 0 0.0.0.0:websm 0.0.0.0:* LISTENTcp 0 0 cncc-core-ingress:websm 10-178-254-194.ku:47292 TIME_WAITtcp 0 0 cncc-core-ingress:46519 kubernetes.default:https ESTABLISHEDtcp 0 0 cncc-core-ingress:websm 10-178-254-194.ku:47240 TIME_WAITtcp 0 0 cncc-core-ingress:websm 10-178-254-194.ku:47347 TIME_WAITudp 0 0 localhost:59351 localhost:ambit-lm ESTABLISHEDActive UNIX domain sockets (servers and established)Proto RefCnt Flags Type State I-Node Pathunix 2 [] STREAM CONNECTED 576064861	--

Table 3-3 (Cont.) netstat

Options Tested	Description	Output	Capabilities
-l	Show only listening sockets.	netstat -l Active Internet connections (only servers)Proto Recv-Q Send-Q Local Address Foreign Address Statetcp 0 0 0.0.0.0:tpoxy 0.0.0.0:* LISTENtcp 0 0 0.0.0.0:websm 0.0.0.0:* LISTENActive UNIX domain sockets (only servers)Proto RefCnt Flags Type State I-Node Path	--
-s	Display summary statistics for each protocol.	netstat -s Ip:4070 total packets received0 forwarded0 incoming packets discarded4070 incoming packets delivered4315 requests sent outlcmp:0 ICMP messages received0 input ICMP message failed.ICMP input histogram:2 ICMP messages sent0 ICMP messages failedICMP output histogram:destination unreachable: 2	--
-i	Display a table of all network interfaces.	netstat -i Kernel Interface tablelface MTU RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flgeth0 1440 4131 0 0 0 4355 0 0 0 BMRUIo 65536 0 0 0 0 0 0 0 LRU	--

jq

Table 3-4 jq

Options Tested	Description	Output	Capabilities
<jq filter> [file...]	Use it to slice and filter and map and transform structured data. Sample JSON file: { "fruit": { "name": "apple", "color": "green", "price": 1.2 } }	jq '.fruit' sample.json { "name": "apple", "color": "green", "price": 1.2 }	--
	Sample JSON file: { "fruit": { "name": "apple", "color": "green", "price": 1.2 } }	jq '.fruit.color,.fruit.price' sample.json "green" 1.2	--

*curl***Table 3-5** curl

Options Tested	Description	Output	Capabilities
-o	Write output to <file> instead of stdout.	curl -o file.txt http://abc.com/file.txt	--
-x	Use the specified HTTP proxy.	curl -x proxy.com:8080 -o http://abc.com/file.txt	--

*ping***Table 3-6** ping

Options Tested	Description	Output	Capabilities
<ip>	Run a ping test to see whether the target host is reachable or not.	ping 10.178.254.194	NET_ADMIN, NET_RAW
-c	Stop after sending 'c' number of ECHO_REQUEST packets.	ping -c 5 10.178.254.194	NET_ADMIN, NET_RAW
-f (with non-zero interval)	Flood ping. For every ECHO_REQUEST sent, a period "." is printed, while for every ECHO_REPLY received a backspace is printed.	ping -f -i 2 10.178.254.194	NET_ADMIN, NET_RAW

*nmap***Table 3-7** nmap

Options Tested	Description	Output	Capabilities
<ip>	Scan for Live hosts, Operating systems, packet filters, and open ports running on remote hosts.	<pre>nmap 10.178.254.194 Starting Nmap 6.40 (http://nmap.org) at 2020-09-29 05:54 UTC Nmap scan report for 10-178-254-194.kubernetes.default.svc.cluster .local (10.178.254.194) Host is up (0.00046s latency). Not shown: 995 closed ports PORT STATE SERVICE 22/tcp open ssh 179/tcp open bgp 6666/tcp open irc 6667/tcp open irc 30000/tcp open unknown Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds</pre>	--

Table 3-7 (Cont.) nmap

Options Tested	Description	Output	Capabilities
-v	Increase verbosity level.	<pre> nmap -v 10.178.254.194 Starting Nmap 6.40 (http://nmap.org) at 2020-09-29 05:55 UTC Initiating Ping Scan at 05:55 Scanning 10.178.254.194 [2 ports] Completed Ping Scan at 05:55, 0.00s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 05:55 Completed Parallel DNS resolution of 1 host. at 05:55, 0.00s elapsed Initiating Connect Scan at 05:55 Scanning 10-178-254-194.kubernetes.default.svc.cluster .local (10.178.254.194) [1000 ports] Discovered open port 22/tcp on 10.178.254.194 Discovered open port 30000/tcp on 10.178.254.194 Discovered open port 6667/tcp on 10.178.254.194 Discovered open port 6666/tcp on 10.178.254.194 Discovered open port 179/tcp on 10.178.254.194 Completed Connect Scan at 05:55, 0.02s elapsed (1000 total ports) Nmap scan report for 10-178-254-194.kubernetes.default.svc.cluster .local (10.178.254.194) Host is up (0.00039s latency). Not shown: 995 closed ports PORT STATE SERVICE 22/tcp open ssh 179/tcp open bgp 6666/tcp open irc 6667/tcp open irc 30000/tcp open unknown Read data files from: /usr/bin/./share/nmap Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds </pre>	--

Table 3-7 (Cont.) nmap

Options Tested	Description	Output	Capabilities
-iL	Scan all the listed IP addresses in a file.	<pre>nmap -iL sample.txt Starting Nmap 6.40 (http://nmap.org) at 2020-09-29 05:57 UTC Nmap scan report for localhost (127.0.0.1) Host is up (0.00036s latency). Other addresses for localhost (not scanned): 127.0.0.1 Not shown: 998 closed ports PORT STATE SERVICE 8081/tcp open blackice-icecap 9090/tcp open zeus-admin Nmap scan report for 10-178-254-194.kubernetes.default.svc.cluster .local (10.178.254.194) Host is up (0.00040s latency). Not shown: 995 closed ports PORT STATE SERVICE 22/tcp open ssh 179/tcp open bgp 6666/tcp open irc 6667/tcp open irc 30000/tcp open unknown Nmap done: 2 IP addresses (2 hosts up) scanned in 0.06 seconds</pre>	--

dig

Table 3-8 dig

Options Tested	Description	Output	Capabilities
<ip>	It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.	<pre>dig 10.178.254.194 Note: The IP should be reachable from inside the container.</pre>	--
-x	Query DNS Reverse Look-up.	<pre>dig -x 10.178.254.194</pre>	--

3.4.1 Debug Tool Configuration Parameters

Following are the parameters used to configure debug tool.

CNE Parameters

Table 3-9 CNE Parameters

Parameter	Description
apiVersion	APIVersion defines the version schema of this representation of an object.
kind	Kind is a string value representing the REST resource this object represents.
metadata	Standard object's metadata.
metadata.name	Name must be unique within a namespace.
spec	spec defines the policy enforced.
spec.readOnlyRootFilesystem	Controls whether the containers run with a read-only root filesystem (i.e. no writable layer).
spec.allowPrivilegeEscalation	Gates whether or not a user is allowed to set the security context of a container to allowPrivilegeEscalation=true.
spec.allowedCapabilities	Provides a list of capabilities that are allowed to be added to a container.
spec.fsGroup	Controls the supplemental group applied to some volumes. RunAsAny allows any fsGroup ID to be specified.
spec.runAsUser	Controls which user ID the containers are run with. RunAsAny allows any runAsUser to be specified.
spec.seLinux	RunAsAny allows any seLinuxOptions to be specified.
spec.supplementalGroups	Controls which group IDs containers add. RunAsAny allows any supplementalGroups to be specified.
spec.volumes	Provides a list of allowed volume types. The allowable values correspond to the volume sources that are defined when creating a volume.

Role Creation Parameters

Table 3-10 Role Creation

Parameter	Description
apiVersion	APIVersion defines the versioned schema of this representation of an object.
kind	Kind is a string value representing the REST resource this object represents.
metadata	Standard object's metadata.
metadata.name	Name must be unique within a namespace.
metadata.namespace	Namespace defines the space within which each name must be unique.
rules	Rules holds all the PolicyRules for this Role
apiGroups	APIGroups is the name of the APIGroup that contains the resources.
rules.resources	Resources is a list of resources this rule applies to.
rules.verbs	Verbs is a list of Verbs that apply to ALL the ResourceKinds and AttributeRestrictions contained in this rule.
rules.resourceNames	ResourceNames is an optional white list of names that the rule applies to.

Table 3-11 Role Binding Creation

Parameter	Description
apiVersion	APIVersion defines the versioned schema of this representation of an object.
kind	Kind is a string value representing the REST resource this object represents.
metadata	Standard object's metadata.
metadata.name	Name must be unique within a namespace.
metadata.namespace	Namespace defines the space within which each name must be unique.
roleRef	RoleRef can reference a Role in the current namespace or a ClusterRole in the global namespace.
roleRef.apiGroup	APIGroup is the group for the resource being referenced
roleRef.kind	Kind is the type of resource being referenced
roleRef.name	Name is the name of resource being referenced
subjects	Subjects holds references to the objects the role applies to.
subjects.kind	Kind of object being referenced. Values defined by this API group are "User", "Group", and "ServiceAccount".
subjects.apiGroup	APIGroup holds the API group of the referenced subject.
subjects.name	Name of the object being referenced.

Debug Tool Configuration Parameters**Table 3-12 Debug Tool Configuration Parameters**

Parameter	Description
command	String array used for container command.
image	Docker image name
imagePullPolicy	Image Pull Policy
name	Name of the container
resources	Compute Resources required by this container
resources.limits	Limits describes the maximum amount of compute resources allowed
resources.requests	Requests describes the minimum amount of compute resources required
resources.limits.cpu	CPU limits
resources.limits.memory	Memory limits
resources.limits.ephemeral-storage	Ephemeral Storage limits
resources.requests.cpu	CPU requests
resources.requests.memory	Memory requests
resources.requests.ephemeral-storage	Ephemeral Storage requests
securityContext	Security options the container should run with.
securityContext.allowPrivilegeEscalation	AllowPrivilegeEscalation controls whether a process can gain more privileges than its parent process. This directly controls if the no_new_privs flag will be set on the container process
securityContext.readOnlyRootFilesystem	Whether this container has a read-only root filesystem. Default is false.

Table 3-12 (Cont.) Debug Tool Configuration Parameters

Parameter	Description
securityContext.capabilities	The capabilities to add/drop when running containers. Defaults to the default set of capabilities granted by the container runtime.
securityContext.capabilities.drop	Removed capabilities
securityContext.capabilities.add	Added capabilities
securityContext.runAsUser	The UID to run the entrypoint of the container process.
debugToolContainerMemoryLimit	Indicates the memory assigned for the debug tool container.
extraContainersVolumesTpl	Specifies the extra container template for the debug tool volume.
extraContainersVolumesTpl.name	Indicates the name of the volume for debug tool logs storage.
extraContainersVolumesTpl.emptyDir.medium	Indicates the location where emptyDir volume is stored.
extraContainersVolumesTpl.emptyDir.sizeLimit	Indicates the emptyDir volume size.
volumeMounts.mountPath	Indicates the path for volume mount.
volumeMounts.name	Indicates the name of the directory for debug tool logs storage.

3.1 Logs

Log files are used to register system events, together with their date and time of occurrence. They can be valuable tools for troubleshooting. Not only do logs indicate that specific events occurred, they also provide important clues about a chain of events that led to an error or problem.

Collecting Logs

This section describes the steps to collect logs from PODs and containers. Perform the following steps:

1. Run the following command to get the PODs details:

```
$ kubectl -n <namespace_name> get pods
```

2. Collect the logs from the specific pods or containers:

```
$ kubectl logs <podname> -n <namespace> -c <containername>
```

3. Store the log in a file using the following command:

```
$ kubectl logs <podname> -n <namespace> > <filename>
```

4. (Optional) You can also use the following commands for the log stream with file redirection starting with last 100 lines of log:

```
$ kubectl logs <podname> -n <namespace> -f --tail <number of lines> > <filename>
```

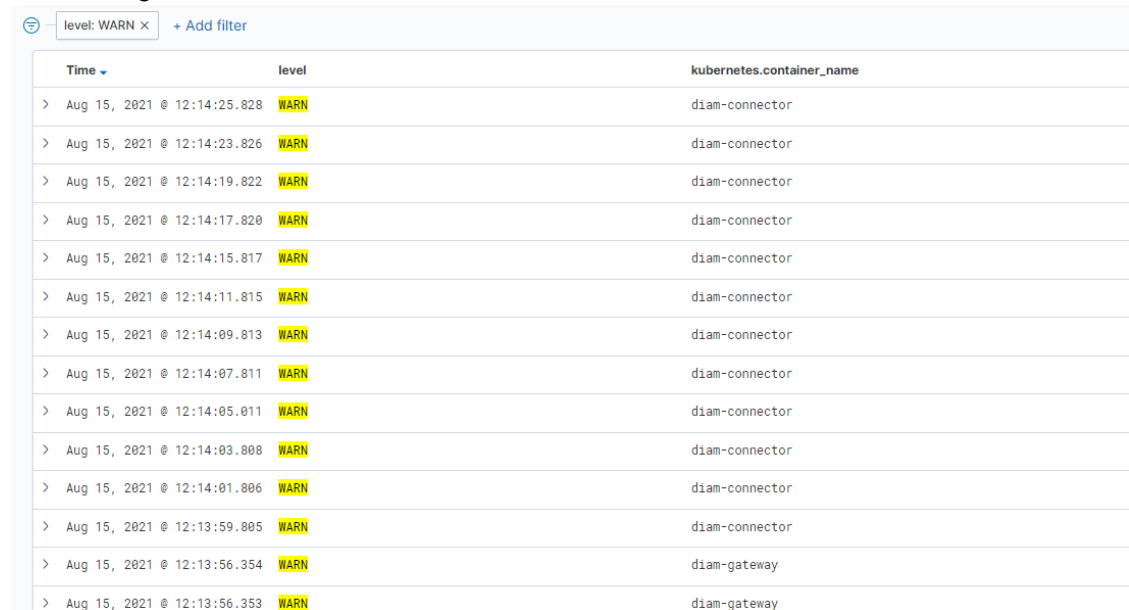
For more information on kubectl commands, see Kubernetes [website](#).

3.1.1 Log Levels

This section provides information on log levels supported by Policy.

A log level helps in defining the severity level of a log message. Using this information, the logs can be filtered based on the system requirements. For instance, if you want to filter the critical information about your system from the informational log messages, set a filter to view messages with only **WARN** log level in Kibana.

As shown in the following image, only log messages with level defined as WARN are shown, after adding filter:



Time	level	kubernetes.container_name
> Aug 15, 2021 @ 12:14:25.828	WARN	diam-connector
> Aug 15, 2021 @ 12:14:23.826	WARN	diam-connector
> Aug 15, 2021 @ 12:14:19.822	WARN	diam-connector
> Aug 15, 2021 @ 12:14:17.820	WARN	diam-connector
> Aug 15, 2021 @ 12:14:15.817	WARN	diam-connector
> Aug 15, 2021 @ 12:14:11.815	WARN	diam-connector
> Aug 15, 2021 @ 12:14:09.813	WARN	diam-connector
> Aug 15, 2021 @ 12:14:07.811	WARN	diam-connector
> Aug 15, 2021 @ 12:14:05.811	WARN	diam-connector
> Aug 15, 2021 @ 12:14:03.808	WARN	diam-connector
> Aug 15, 2021 @ 12:14:01.806	WARN	diam-connector
> Aug 15, 2021 @ 12:13:59.805	WARN	diam-connector
> Aug 15, 2021 @ 12:13:56.354	WARN	diam-gateway
> Aug 15, 2021 @ 12:13:56.353	WARN	diam-gateway

Supported Log Levels

For Policy, the log level for a micro-service can be set to any of the following valid values:

- **TRACE:** A log level describing events showing step by step execution of your code that can be ignored during the standard operation, but may be useful during extended debugging sessions.
- **DEBUG:** A log level used for events considered to be useful during software debugging when more granular information is needed.
- **INFO:** The standard log level indicating that something happened, the application entered a certain state, etc.
- **WARN:** Indicates that something unexpected happened in the application, a problem, or a situation that might disturb one of the processes. But that doesn't mean that the application failed. The WARN level should be used in situations that are unexpected, but the code can continue the work.
- **ERROR:** The log level that should be used when the application hits an issue preventing one or more functionalities from properly functioning.

Configuring Log Levels

To view logging configurations and update logging levels, use the Logging Level page under **Logging Configurations** on the CNC Console. For more information, see the section "Log Level" in *Oracle Communications Cloud Native Core, Converged Policy User's Guide*.

Log Message Examples with different Level values

The following is a sample log message with level *ERROR*:

```
{
  "_index": "logstash-2021.08.15",
  "_type": "_doc",
  "_id": "Diu0SHsBX9U84vckBYS0",
  "_version": 1,
  "_score": null,
  "_source": {
    "stream": "stdout",
    "docker": {
      "container_id":
"fc7c3e68ba775ddca4e7f5d0603c8ba1bc414703e7d28f6177012893ca342a3b"
    },
    "kubernetes": {
      "container_name": "user-service",
      "namespace_name": "mdc3",
      "pod_name": "mdc3-cnppolicy-occpn-udr-connector-697f7f5b8b-9l2jz",
      "container_image": "titans-1-bastion-1:5000/occpn/oc-pcf-user:1.14.0-
nb-20210804",
      "container_image_id": "titans-1-bastion-1:5000/occpn/oc-pcf-
user@sha256:d66b1017fd8b1946744a2115bc088349c95f93db17626a20fbb11e25ff543f83",
      "pod_id": "f0b233bb-10a1-4b4c-9b77-f864659b9c3e",
      "host": "titans-1-k8s-node-2",
      "labels": {
        "application": "occpn",
        "engVersion": "1.14.0-nb-20210804",
        "microservice": "occpn_pcf_user",
        "mktgVersion": "1.0.0",
        "pod-template-hash": "697f7f5b8b",
        "vendor": "Oracle",
        "app_kubernetes_io/instance": "mdc3-cnppolicy",
        "app_kubernetes_io/managed-by": "Helm",
        "app_kubernetes_io/name": "user-service",
        "app_kubernetes_io/part-of": "occpn",
        "app_kubernetes_io/version": "1.0.0",
        "helm_sh/chart": "user-service-1.14.0-nb-20210804",
        "io_kompose_service": "mdc3-cnppolicy-occpn-udr-connector"
      },
      "master_url": "https://10.233.0.1:443/api",
      "namespace_id": "aadab0ec-ce08-4f81-b70c-2ffda2f39055",
      "namespace_labels": {
        "istio-injection": ""
      }
    },
    "instant": {
      "epochSecond": 1629009871,
      "nanoOfSecond": 244837074
    },
    "thread": "CmAgentTask1",
    "level": "ERROR",
    "loggerName": "ocpm.cne.common.cmclient.CmRestClient",
    "message": "Error performing GET operation for URI /pcf/nf-common-
```

```

component/v1/nrf-client-nfmanagement/nfProfileList",
  "thrown": {
    "commonElementCount": 0,
    "localizedMessage": "I/O error on GET request for \"http://mdc3-
cnpolicy-occpn-config-mgmt:8000/pcf/nf-common-component/v1/nrf-client-
nfmanagement/nfProfileList\": Connect to mdc3-cnpolicy-occpn-config-mgmt:8000
[mdc3-cnpolicy-occpn-config-mgmt/10.233.53.78] failed: Connect timed out;
nested exception is org.apache.http.conn.ConnectTimeoutException: Connect to
mdc3-cnpolicy-occpn-config-mgmt:8000 [mdc3-cnpolicy-occpn-config-mgmt/
10.233.53.78] failed: Connect timed out",
    "message": "I/O error on GET request for \"http://mdc3-cnpolicy-occpn-
config-mgmt:8000/pcf/nf-common-component/v1/nrf-client-nfmanagement/
nfProfileList\": Connect to mdc3-cnpolicy-occpn-config-mgmt:8000 [mdc3-
cnpolicy-occpn-config-mgmt/10.233.53.78] failed: Connect timed out; nested
exception is org.apache.http.conn.ConnectTimeoutException: Connect to mdc3-
cnpolicy-occpn-config-mgmt:8000 [mdc3-cnpolicy-occpn-config-mgmt/
10.233.53.78] failed: Connect timed out",
    "name": "org.springframework.web.client.ResourceAccessException",
    "cause": {
      "commonElementCount": 14,
      "localizedMessage": "Connect to mdc3-cnpolicy-occpn-config-mgmt:8000
[mdc3-cnpolicy-occpn-config-mgmt/10.233.53.78] failed: Connect timed out",
      "message": "Connect to mdc3-cnpolicy-occpn-config-mgmt:8000 [mdc3-
cnpolicy-occpn-config-mgmt/10.233.53.78] failed: Connect timed out",
      "name": "org.apache.http.conn.ConnectTimeoutException",
      "cause": {
        "commonElementCount": 14,
        "localizedMessage": "Connect timed out",
        "message": "Connect timed out",
        "name": "java.net.SocketTimeoutException",
        "extendedStackTrace": "java.net.SocketTimeoutException: Connect
timed out\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:546) ~[?:?]
\n\tat sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597) ~[?:?]\n\tat
java.net.SocksSocketImpl.connect(SocksSocketImpl.java:333) ~[?:?]\n\tat
java.net.Socket.connect(Socket.java:645) ~[?:?]\n\tat
org.apache.http.conn.socket.PlainConnectionSocketFactory.connectSocket(PlainCo
nnectionSocketFactory.java:75) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultH
ttpClientConnectionOperator.java:142) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHt
tpClientConnectionManager.java:376) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.ja
va:393) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.ja
va:185) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.ja
va:83) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

```

```

org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:56) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.springframework.http.client.HttpComponentsClientHttpRequest.executeInternal(HttpComponentsClientHttpRequest.java:87) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInternal(AbstractBufferingClientHttpRequest.java:48) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClientHttpRequest.java:66) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776)
~[spring-web-5.3.4.jar!/:5.3.4]\n"
    },
    "extendedStackTrace": "org.apache.http.conn.ConnectTimeoutException:
Connect to mdc3-cnpolicy-occpn-config-mgmt:8000 [mdc3-cnpolicy-occpn-config-
mgmt/10.233.53.78] failed: Connect timed out\n\tat
org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultHttpClientConnectionOperator.java:151) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHttpClientConnectionManager.java:376) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.java:393) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.java:185) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:83) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:56) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.springframework.http.client.HttpComponentsClientHttpRequest.executeInternal(HttpComponentsClientHttpRequest.java:87) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInternal(AbstractBufferingClientHttpRequest.java:48) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClientHttpRequest.java:66) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776)
~[spring-web-5.3.4.jar!/:5.3.4]\nCaused by: java.net.SocketTimeoutException:
Connect timed out\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:546) ~[?:?]\n\tat
sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597) ~[?:?]\n\tat
java.net.SocksSocketImpl.connect(SocksSocketImpl.java:333) ~[?:?]\n\tat
java.net.Socket.connect(Socket.java:645) ~[?:?]\n\tat
org.apache.http.conn.socket.PlainConnectionSocketFactory.connectSocket(PlainConnectionSocketFactory.java:75) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultHttpClientConnectionOperator.java:142) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHttp

```

```

tpClientConnectionManager.java:376) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.ja
va:393) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.ja
va:185) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.ja
va:83) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.ja
va:56) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.springframework.http.client.HttpComponentsClientHttpRequest.executeInterna
l(HttpComponentsClientHttpRequest.java:87) ~[spring-
web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInte
rnal(AbstractBufferingClientHttpRequest.java:48) ~[spring-
web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClie
ntHttpRequest.java:66) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776)
~[spring-web-5.3.4.jar!/:5.3.4]\n\t... 14 more\n"
    },
    "extendedStackTrace":
"org.springframework.web.client.ResourceAccessException: I/O error on GET
request for \"http://mdc3-cnppolicy-occpn-config-mgmt:8000/pcf/nf-common-
component/v1/nrf-client-nfmanagement/nfProfileList\": Connect to mdc3-
cnppolicy-occpn-config-mgmt:8000 [mdc3-cnppolicy-occpn-config-mgmt/
10.233.53.78] failed: Connect timed out; nested exception is
org.apache.http.conn.ConnectTimeoutException: Connect to mdc3-cnppolicy-occpn-
config-mgmt:8000 [mdc3-cnppolicy-occpn-config-mgmt/10.233.53.78] failed:
Connect timed out\n\tat
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:785)
~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.execute(RestTemplate.java:751)
~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.getForEntity(RestTemplate.java:377
) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
ocpm.cne.common.cmclient.CmRestClient.lambda$get$0(CmRestClient.java:54)
~[cne-common-0.0.8-SNAPSHOT-dev.jar!/:?]\n\tat
org.springframework.retry.support.RetryTemplate.doExecute(RetryTemplate.java:3
29) ~[spring-retry-1.3.1.jar!/:?]\n\tat
org.springframework.retry.support.RetryTemplate.execute(RetryTemplate.java:209
) ~[spring-retry-1.3.1.jar!/:?]\n\tat
ocpm.cne.common.cmclient.CmRestClient.get(CmRestClient.java:53) [cne-
common-0.0.8-SNAPSHOT-dev.jar!/:?]\n\tat
ocpm.cne.common.cmclient.CmRestClientTask.run(CmRestClientTask.java:32) [cne-
common-0.0.8-SNAPSHOT-dev.jar!/:?]\n\tat
org.springframework.scheduling.support.DelegatingErrorHandlingRunnable.run(De
legatingErrorHandlingRunnable.java:54) [spring-
context-5.3.4.jar!/:5.3.4]\n\tat

```

```

java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:515) [?:?]
\n\tat java.util.concurrent.FutureTask.runAndReset(FutureTask.java:305) [?:?]
\n\tat
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Sched
uledThreadPoolExecutor.java:305) [?:?]\n\tat
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1130
) [?:?]\n\tat
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:630
) [?:?]\n\tat java.lang.Thread.run(Thread.java:831) [?:?]\nCaused by:
org.apache.http.conn.ConnectTimeoutException: Connect to mdc3-cnpolicy-ocnp-
config-mgmt:8000 [mdc3-cnpolicy-ocnp-config-mgmt/10.233.53.78] failed:
Connect timed out\n\tat
org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultH
ttpClientConnectionOperator.java:151) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHt
tpClientConnectionManager.java:376) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.ja
va:393) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.ja
va:185) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.ja
va:83) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.ja
va:56) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.springframework.http.client.HttpComponentsClientHttpRequest.executeIntern
al(HttpComponentsClientHttpRequest.java:87) ~[spring-
web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInte
rnal(AbstractBufferingClientHttpRequest.java:48) ~[spring-
web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClie
ntHttpRequest.java:66) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776)
~[spring-web-5.3.4.jar!/:5.3.4]\n\t... 14 more\nCaused by:
java.net.SocketTimeoutException: Connect timed out\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:546) ~[?:?]
\n\tat sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597) ~[?:?]\n\tat
java.net.SocksSocketImpl.connect(SocksSocketImpl.java:333) ~[?:?]\n\tat
java.net.Socket.connect(Socket.java:645) ~[?:?]\n\tat
org.apache.http.conn.socket.PlainConnectionSocketFactory.connectSocket(PlainCo
nnectionSocketFactory.java:75) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultH
ttpClientConnectionOperator.java:142) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHt
tpClientConnectionManager.java:376) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.ja
va:393) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)

```

```

~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.java:185) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:83) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:56) ~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.springframework.http.client.HttpComponentsClientHttpRequest.executeInternal(HttpComponentsClientHttpRequest.java:87) ~[spring-
web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInternal(AbstractBufferingClientHttpRequest.java:48) ~[spring-
web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClientHttpRequest.java:66) ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776)
~[spring-web-5.3.4.jar!/:5.3.4]\n\t... 14 more\n"
    },
    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 21,
    "threadPriority": 5,
    "messageTimestamp": "2021-08-15T06:44:31.244+0000",
    "@timestamp": "2021-08-15T06:44:31.245670273+00:00",
    "tag": "kubernetes.var.log.containers.mdc3-cnpolicy-ocnp-udr-
connector-697f7f5b8b-9l2jz_mdc3_user-service-
fc7c3e68ba775ddca4e7f5d0603c8ba1bc414703e7d28f6177012893ca342a3b.log"
  },
  "fields": {
    "messageTimestamp": [
      "2021-08-15T06:44:31.244Z"
    ],
    "@timestamp": [
      "2021-08-15T06:44:31.245Z"
    ]
  },
  "sort": [
    1629009871245
  ]
}

```

The following is a sample log message with level *INFO*

```

{
  "_index": "logstash-2021.08.15",
  "_type": "_doc",
  "_id": "pYK0SHsBgXqNeaK8Blhv",
  "_version": 1,
  "_score": null,

```

```

    "_source": {
      "stream": "stdout",
      "docker": {
        "container_id":
"d373ee8717f2c21ba1c06d7b78ba1d74b15239e044db24a98d8cbd7e0e0c70b6"
      },
      "kubernetes": {
        "container_name": "perf-info",
        "namespace_name": "mdc2",
        "pod_name": "mdc2-cnppolicy-performance-b9587f5cc-mxvp4",
        "container_image": "titans-1-bastion-1:5000/occpn/oc-perf-info:1.14.0-rc.1",
        "container_image_id": "titans-1-bastion-1:5000/occpn/oc-perf-info@sha256:c7b04350374a238aa4b05f1e5de50feeb65a45c09b48260b0639fb0771094975",
        "pod_id": "13f40f5f-dcea-4a1f-88bf-396520d360df",
        "host": "titans-1-k8s-node-11",
        "labels": {
          "application": "occpn",
          "engVersion": "1.14.0-rc.1",
          "microservice": "perf_info",
          "mktgVersion": "1.0.0",
          "pod-template-hash": "b9587f5cc",
          "vendor": "Oracle",
          "app_kubernetes_io/instance": "mdc2-cnppolicy",
          "app_kubernetes_io/managed-by": "Helm",
          "app_kubernetes_io/name": "perf-info",
          "app_kubernetes_io/part-of": "occpn",
          "app_kubernetes_io/version": "1.0.0",
          "helm_sh/chart": "perf-info-1.14.0-rc.1",
          "io_kompose_service": "mdc2-cnppolicy-performance"
        },
        "master_url": "https://10.233.0.1:443/api",
        "namespace_id": "df5cee99-9b95-4bce-a3cc-d0453c214283",
        "namespace_labels": {
          "istio-injection": ""
        }
      },
      "name": "stat_helper",
      "message": "Probing prometheus URL http://occpn-prometheus-server.occpn-infra/prometheus",
      "level": "INFO",
      "filename": "stat_helper.py",
      "lineno": 36,
      "module": "stat_helper",
      "func": "probe_prometheus_url",
      "thread": "MainThread",
      "messageTimestamp": "2021-08-15T06:44:22.715+0000",
      "@timestamp": "2021-08-15T06:44:22.715709480+00:00",
      "tag": "kubernetes.var.log.containers.mdc2-cnppolicy-performance-b9587f5cc-mxvp4_mdc2_perf-info-d373ee8717f2c21ba1c06d7b78ba1d74b15239e044db24a98d8cbd7e0e0c70b6.log"
    },
    "fields": {
      "messageTimestamp": [
        "2021-08-15T06:44:22.715Z"
      ]
    },
  ],

```

```

    "@timestamp": [
      "2021-08-15T06:44:22.715Z"
    ]
  },
  "sort": [
    1629009862715
  ]
}

```

3.1.2 Understanding Logs

This section provides information on how to read logs for various services of Policy in Kibana.

Understanding Logs

The following is a sample log for Policy services:

```

{
  "instant": {
    "epochSecond": 1627016656,
    "nanoOfSecond": 137175036
  },
  "thread": "Thread-2",
  "level": "INFO",
  "loggerName": "ocpm.pcf.framework.domain.orchestration.AbstractProcess",
  "marker": {
    "name": "ALWAYS"
  },
  "message": "Received RECONFIGURE request",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 34,
  "threadPriority": 5,
  "messageTimestamp": "2021-07-23T05:04:16.137+0000"
}

```

The log message format is same for all the Policy services.

The following table describes key attributes of a log message:

Table 3-13 Log Attributes

Attribute	Description
level	Log level of the log printed
loggerName	Class/Module which printed the log
message	Message related to the log providing brief details
loggerFqcn	Log4j2 Internal, Fully Qualified class name of logger module
thread	Thread name
threadId	Thread ID generated internally by Log4j2
threadPriority	Thread priority generated internally by Log4j2
messageTimeStamp	Timestamp of log from application container

Table 3-13 (Cont.) Log Attributes

Attribute	Description
kubernetes.labels.application	NF Application Name
kubernetes.labels.engineVersion	Engineering version of software
kubernetes.labels.mktgVersion	Marketing version of software
kubernetes.labels.microservice	Name of the microservice
kubernetes.namespace_name	Namespace of OCPCF deployment
kubernetes.host	worker node name on which container is running
kubernetes.pod_name	Pod Name
kubernetes.container_name	Container Name
Docker.container_id	Process ID internally assigned
kubernetes.labels.vendor	Vendor of product

4

Troubleshooting Policy

This chapter provides information to troubleshoot the common errors which can be encountered during the preinstall, installation, upgrade, and rollback procedures of Policy.

Note

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

4.2 Database Related Issues

This section describes the most common database related issues and their resolution steps. It is recommended to perform the resolution steps provided in this guide. If the issue still persists, then contact Oracle Support.

4.2.1 Policy MySQL DB Access

Problem

Keyword - wait-for-db

Tags - "config-server" "database" "readiness" "init" "SQLException" "access denied"

Because of database accessibility issues from the Policy service, pods will stay in the init state.

For some pods, if they come up, they will be kept on getting the exception : " Cannot connect to database server java.sql.SQLException"

Reasons:

1. MySQL host IP address OR MySQL-service name[in case of occne-infra] is not correctly given.
2. Few MySQL nodes are probably down.
3. Username/Password given in the secrets are not created in the database OR not having proper grant/access to service databases.
4. Databases are not created correctly with the same name mentioned in the custom_value file while installing Policy. - **MOST LIKELY**

Resolution Steps

To resolve this issue, perform the following steps:

1. Check if the database IP is proper and pingable from worker nodes of the Kubernetes cluster. Update the database IP and service accordingly. If required, you can use floating

IP as well. If the database connectivity issue is there, then please update the proper IP address.

In the case of the CNE infrastructure, instead of mentioning IP address for MySQL connection, please use FQDN for mysql-connectivity-service to connect to the database.

2. Manually log in to MySQL via the same database IP mentioned in a custom-value file. In case of MySQL service name, describe the service by command :

```
kubectl describe svc <mysql-servicename> -n <namespace>
```

and login to the MySQL database with all sets of IPs described in the MySQL service, If any SQL node is down, it will lead to an intermittent DB query failure issue. So make sure that you can log in to MySQL from all the Nodes mentioned in the IP list of MySQL-service describe command.

Make sure that all the MySQL nodes are up and running before installing the Policy.

3. Check the existing user list into the database using SQL query: "select user from mysql.user;"
Check if all the mentioned users in the custom-value of Policy installation are present in the database.

Note

Create the user with proper password as mentioned in the secret file of the Policy.

4. Check the grants of all the users mentioned into the custom_value file by SQL query: "show grants for <username>;"
If username/password issue is there, then please correctly create the user with the required password and provide grants as per the installation guide.
5. Check the databases are created with the same name mentioned in the custom_value file for the services.

Note

Create the database as per the custom_value file.

6. Check if problematic pods are getting created on any one unique worker node. If yes, then may be the cause of the error can be the worker node. Try draining the problematic worker node and allow pods to move to another node.

4.4 Upgrade or Rollback Failure

When Policy upgrade or rollback fails, perform the following procedure.

1. Check the pre or post upgrade or rollback hook logs in Kibana as applicable.
Users can filter upgrade or rollback logs using the following filters:
 - For upgrade: lifeCycleEvent=9001 or 9011
 - For rollback: lifeCycleEvent=9002
2. Check the pod logs in Kibana to analyze the cause of failure.
3. After detecting the cause of failure, do the following:
 - For upgrade failure:

- If the cause of upgrade failure is database or network connectivity issue, contact your system administrator. When the issue is resolved, rerun the upgrade command.
 - If the cause of failure is not related to database or network connectivity issue and is observed during the preupgrade phase, do not perform rollback because Policy deployment remains in the source or older release.
 - If the upgrade failure occurs during the postupgrade phase, for example, post upgrade hook failure due to target release pod not moving to ready state, then perform a rollback.
 - For rollback failure: If the cause of rollback failure is database or network connectivity issue, contact your system administrator. When the issue is resolved, rerun the rollback command.
4. If the issue persists, contact [My Oracle Support](#).

4.1 Deployment Related Issues

This section describes the most common deployment related issues and their resolution steps. It is recommended to perform the resolution steps provided in this guide. If the issue still persists, then contact Oracle Support.

4.1.1 Helm Install Failure

If `helm install` command Fails

This section covers the reasons and troubleshooting procedures if the `helm install` command fails.

Reasons for `helm install` failure:

- **Chart syntax issue [This issue could be shown in the few seconds]**
Please resolve the chart specific things and rerun the `helm install` command, because in this case, no hooks should have begun.
- **Most possible reason [TIMEOUT]**
If any job stuck in a pending/error state and unable to run, it will result in the timeout after 5 minutes. As default timeout for `helm` command is "5 minutes". In this case, we have to follow the below steps to troubleshoot.
- **`helm install` command failed in case of duplicated chart**

```
helm install /home/cloud-user/pcf_1.6.1/sprint3.1/ocpcf-1.6.1-  
sprint.3.1.tgz --name ocpcf2 --namespace ocpcf2 -f <custom-value-file>
```

Error: release ocpcf2 failed: configmaps "perfinfo-config-ocpcf2" already exists

Here, configmap 'perfinfo-config-ocpcf2' exists multiple times, while creating Kubernetes objects after pre-upgrade hooks, this will be failed. In this case also please go through the below troubleshooting steps.

Troubleshooting steps:

1. Check from describe/logs of failure pods and fix them accordingly. You need to verify what went wrong on the installation of the Policy by checking the below points:

For the PODs which were not started, run the following command to check the failed pods:

```
kubectl describe pod <pod-name> -n <release-namespace>
```

For the PODs which were started but failed to come into "READY" state, run the following command to check the failed pods:

```
kubectl describe logs <pod-name> -n <release-namespace>
```

2. Run the below command to get kubernetes objects:

```
kubectl get all -n <release_namespace>
```

This gives a detailed overview of which objects are stuck or in a failed state.

3. Run the below command to delete all kubernetes objects:

```
kubectl delete all --all -n <release_namespace>
```

4. Run the below command to delete all current configmaps:

```
kubectl delete cm --all -n <release-namespace>
```

5. Run the below command to cleanup the databases created by the helm install command and create the database again:

```
DROP DATABASE IF EXISTS occnp_audit_service;  
DROP DATABASE IF EXISTS occnp_config_server;  
DROP DATABASE IF EXISTS occnp_pcf_am;  
DROP DATABASE IF EXISTS occnp_pcf_sm;  
DROP DATABASE IF EXISTS occnp_pcrf_core;  
DROP DATABASE IF EXISTS occnp_release;  
DROP DATABASE IF EXISTS occnp_binding;  
DROP DATABASE IF EXISTS occnp_policyds;  
DROP DATABASE IF EXISTS occnp_pcf_ue;  
DROP DATABASE IF EXISTS occnp_commonconfig;  
CREATE DATABASE IF NOT EXISTS occnp_audit_service;  
CREATE DATABASE IF NOT EXISTS occnp_config_server;  
CREATE DATABASE IF NOT EXISTS occnp_pcf_am;  
CREATE DATABASE IF NOT EXISTS occnp_pcf_sm;  
CREATE DATABASE IF NOT EXISTS occnp_pcrf_core;  
CREATE DATABASE IF NOT EXISTS occnp_release;  
CREATE DATABASE IF NOT EXISTS occnp_binding;  
CREATE DATABASE IF NOT EXISTS occnp_policyds;  
CREATE DATABASE IF NOT EXISTS occnp_pcf_ue;  
CREATE DATABASE IF NOT EXISTS occnp_commonconfig;
```

In addition, clean up the entries in "mysql.ndb_replication" table by running the following command:

```
DROP TABLE IF EXISTS mysql.ndb_replication;
```

6. Run the following command :

- For Helm2:

```
helm ls --all
```

- For Helm3:

```
helm3 ls -n <release-namespace>
```

If this is in a failed state, please purge the namespace using the following command:

```
helm delete --purge <release_namespace>
```

Once the purge command is succeeded, press "ctrl+c" to stop the above script.

Note

If the command is taking more time, run the following command in another session to clear all the delete jobs.

```
while true; do kubectl delete jobs --all -n <release_namespace>;  
sleep 5;done
```

7. After the database cleanup and creation of the database again, run the `helm install` command.

If `helm install` command fails due to atomic and timeout options

The `helm install` command fails as the external-ip allocation (Loadbalancer) fails for Diameter Gateway, Ingress Gateway, and Configuration Management service as they are of the type loadbalancer.

Reason: The primary reason for this problem is availability of limited infrastructure due to which floating IPs may not be available. It may also happen due to the system taking more time to assign floating IPs, as a result of which charts purge.

Solution: To resolve this issue, user may either skip `--atomic` keyword from the `helm install` command or set a higher timeout value.

4.1.2 Configuration Issue where mysql-username had an Extra Line

Symptom

No suitable driver found for jdbc

Problem

Secret files contain the user id and password for the MySQL. User ID and password inside the secret file shall be base64 encoded. During base64 encoding, if a new line is present in the user id and password – the line is also encoded and may cause issues when they are decoded back.

Resolution Steps

To resolve this issue, perform the following steps:

1. Get the secret file created by customer.
2. Fetch the encoded MySQL username and password.
3. Go to <https://www.base64decode.org/>.
4. Give the username and password and click decode.
5. Verify if the extra line is present in the username and password. If present, remove the extra line.
6. Decode it again.

4.1.3 App Info Worker Time Out

Problem

PCF appinfo pod is stuck in restarting with the following log:

[CRITICAL] WORKER TIMEOUT

The appinfo process has a HTTP server (gunicorn) and a few worker processes. The request comes to the gunicorn process, then the worker processes handle the request. If the worker does not return in 30 seconds, then gunicorn prints "WORKER TIMEOUT" error, and kills the worker. From the log, it appears that the worker processes are stuck somewhere.

Troubleshooting steps:

1. Change the appinfo deployment, increase the liveness threshold value from 3 to a higher value. By doing so, appinfo is not impacted by readiness check.
2. Watch the log of appinfo to check whether the problem still exists.
3. If the problem still exists, then we need to find out why the worker process is stuck. Run the following command to get into appinfo pod:

```
kubectl -n <pcf namespace> exec -it <pod name> /bin/bash
```

4. Create a temporary python file:

```
cat > xxx_test.py

import pdb
import appinfo

pdb.set_trace()
appinfo.app.run(port=9999)
```

5. Run the following command to run this temporary python file

```
python3 xxx_test.py
```

It launches a python debugger, type "continue" to run the app.

6. Open another terminal, run the following command:

```
kubectl -n <pcf namespace> exec -it <pod name> /bin/bash
```

Then, run the following command to check whether this temporary service can return immediately:

```
curl localhost:9999/v1/readiness
```

If curl gets stuck, then we have reproduced the problem. Now in the python debugger, type "ctrl+C", and you should be able to get the stack trace that indicates the problem.

4.1.4 Startup Probes

To increase the application's reliability and availability, startup probes are introduced in Policy. Consider a scenario where the configuration is not loaded or partially loaded but the service goes into a ready state. This may result in different pods showing different behaviour for the same service. With the introduction of startup probe, the readiness and liveness checks for a pod are not initiated until the configuration is loaded completely and startup probe is successful. However, if the startup probe fails, the container restarts.

To check the status of startup probe or investigate the reason of failing, perform the following steps:

1. Log in to a container by running the following command:

```
kubectl exec -it podname -n namespace -- bash
curl -kv http://localhost:<monitoring-port>/<startup-probe-url>
```

Example:

```
kubectl exec -it test-pcrf-core-797cf5997-2zlgf -- curl -kv http://
localhost:9000/actuator/health/startup
```

The sample output can be as follow:

```
[cloud-user@bastion-1 ~]$
* Trying ::1...
* TCP_NODELAY set
* connect to ::1 port 9000 failed: Connection refused
* Trying 127.0.0.1...
* TCP_NODELAY set
* connect to 127.0.0.1 port 9000 failed: Connection refused
* Failed to connect to localhost port 9000: Connection refused
* Closing connection 0
curl: (7) Failed to connect to localhost port 9000: Connection refused
command terminated with exit code 7
[cloud-user@bastion-1 ~]$ k exec -it test-pcrf-core-797cf5997-2zlgf --
curl -kv http://localhost:9000/actuator/health/startup
* Trying ::1...
* TCP_NODELAY set
* Connected to localhost (::1) port 9000 (#0)
> GET /actuator/health/startup HTTP/1.1
> Host: localhost:9000
```

```

> User-Agent: curl/7.61.1
> Accept: */*
>
< HTTP/1.1 503 Service Unavailable
< Date: Thu, 21 Apr 2022 11:18:03 GMT
< Content-Type: application/json; charset=utf-8
< Transfer-Encoding: chunked
< Server: Jetty(9.4.43.v20210629)
<
* Connection #0 to host localhost left intact
{"status":"DOWN"}[cloud-user@bastion-1 ~]$ k exec -it test-pcrf-
core-797cf5997-2zlgf -- curl -kv http://localhost:9000/actuator/health/
startup
* Trying ::1...
* TCP_NODELAY set
* Connected to localhost (::1) port 9000 (#0)
> GET /actuator/health/startup HTTP/1.1
> Host: localhost:9000
> User-Agent: curl/7.61.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Thu, 21 Apr 2022 11:18:04 GMT
< Content-Type: application/json; charset=utf-8
< Transfer-Encoding: chunked
< Server: Jetty(9.4.43.v20210629)
<
* Connection #0 to host localhost left intact
{"status":"UP"}[cloud-user@bastion-1 ~]$

```

2. To check why the startup probe failed, describe the output:

Describe output:

```

Warning Unhealthy <invalid> (x10 over 2m45s) kubelet
Startup probe failed: Get "http://10.233.81.231:9000/actuator/health/
startup": dial tcp 10.233.81.231:9000: connect: connection refused

```

The following could be the possible reasons for startup probe failure:

- Network connectivity issue
 - Database connection issue due to which server is not coming up
 - Due to any other exception
3. If the reason for startup probe failure is not clear, check the logs to determine if it is due to an issue with config-server connection or any issue with fetching configurations from the config-server.

4.1.5 Monitoring of Diameter Gateway worker nodes failure

Symptom

When Diameter Gateway node fails, new replicas are not created in a different worker node.

Problem

On the Diameter Gateway, if the worker node is being shutdown, it is set to "Terminating" state. The diameter gateway pods are statefulsets, due to which new pods are not created until the original pod dies. While in similar scenario new worker nodes are spun for replicaset. The pod has to be forced killed using the --force option.

Resolution

For Diameter Gateway, set `terminationGracePeriodSeconds` to 0s. This is done by configuring the `occnp-custom-values.yaml` file.

Example:

```
diam-gateway:
  # Graceful Termination
  gracefulShutdown:
    gracePeriod:0s
```

Create an alert that gets triggered when a node is down. Do modify the oid and name as per customer deployment if needed.

Example:

```
name: NODE_UNAVAILABLE
expr: kube_node_status_condition{condition="Ready",status="true"}== 0
for: 30s
labels:
oid: XXXXXX
severity: critical
annotations:
description: Kubernetes node {{ $labels.node }} is not in Ready state
summary: Kubernetes node {{ $labels.node }} is unavailable {code}
```

4.3 Service Related Issues

This section describes the most common service related issues and their resolution steps. It is recommended to perform the resolution steps provided in this guide. If the issue still persists, then contact Oracle Support.

4.3.1 SM Service Issues

This section describes the most common SM service issues and their resolution steps. It is recommended to for users to attempt the resolution steps provided in this guide before contacting Oracle Support.

Failed BSF register or deregister binding**Symptom**

On sending BSF register or deregister binding request, the SM service receives 406 NOT_ACCEPTABLE binding reply message from BSF.

Problem

When the SM service initiates a request to register with or deregister from BSF a session, BSF sends 4xx in the response code. It is assumed that bindingSvcEnabled parameter is set to true while deploying the Policy instance.

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant": {
    "epochSecond": 1621844941, "nanoOfSecond": 854958774, "thread": "boundedElastic-1",
    "level": "INFO", "loggerName": "ocpm.pcf.service.sm.serviceconnector.BsfConnector",
    "message": "Sent Binding Request to BSF Service: https://bsf.apigateway:8001/nbsf-management/v2/pcfBindings, {\"supi\": \"imsi-10000000002\", \"contextId\": \"afa7e0cb-87f3-4e6c-a867-166705acfcfe\", \"gpsi\": \"msisdn-10000000001\", \"ipv4Addr\": \"192.168.10.10\", \"ipv6Prefix\": \"2800:a00:cc01::/64\", \"ipDomain\": \"ora.com\", \"dnn\": \"dnn1\", \"pcfFqdn\": \"pcf-sm-service.pcf\", \"pcfDiamHost\": \"pcf-sm-service\", \"pcfDiamRealm\": \"pcf-sm-service.svc\", \"snssai\": {\"sst\": 11, \"sd\": \"abc123\"}}\", \"endOfBatch\": false, \"loggerFqcn\": \"org.apache.logging.slf4j.Log4jLogger\", \"threadId\": 37, \"threadPriority\": 5, \"messageTimestamp\": \"2021-05-24T08:29:01.854+0000\"}
  },
  "instant": {
    "epochSecond": 1621844941, "nanoOfSecond": 945868600, "thread": "boundedElastic-1",
    "level": "INFO", "loggerName": "ocpm.pcf.service.sm.serviceconnector.BsfConnector",
    "message": "Receive Binding Reply from BSF: 406 NOT_ACCEPTABLE\", \"endOfBatch\": false, \"loggerFqcn\": \"org.apache.logging.slf4j.Log4jLogger\", \"threadId\": 37, \"threadPriority\": 5, \"messageTimestamp\": \"2021-05-24T08:29:01.945+0000\"}
  },
  "instant": {
    "epochSecond": 1621844941, "nanoOfSecond": 946569461, "thread": "boundedElastic-1",
    "level": "DEBUG", "loggerName": "ocpm.pcf.service.sm.domain.component.metrics.SmMetrics",
    "message": "Pegging binding response metric. Dnn :dnn1, snssai : 11-abc123, operationType : create ,mode : synchronous ,responseCode : 4xx\", \"endOfBatch\": false, \"loggerFqcn\": \"org.apache.logging.slf4j.Log4jLogger\", \"threadId\": 37, \"threadPriority\": 5, \"messageTimestamp\": \"2021-05-24T08:29:01.946+0000\"}
  }
}
```

Resolution Steps

Policy not evaluated, and instead default policy got applied

Symptom

On sending POST request to binding service, SM service receives failed to call Binding service error.

Problem

When the SM service initiates a POST request towards BSF such as <http://my-cnpolicy-ocnp-binding:8000/binding/v1/contextBinding/context-owner/PCF-SM>, an error occurs and a message is received at SM service stating that the system failed to call Binding service. User may search for a response similar to the following:

```
logMsg=Failed to call policy service: {}
```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant": {
    "epochSecond": 1623052588,
    "nanoOfSecond": 652897378
  },
  "thread": "boundedElastic-7",
  "level": "ERROR",
  "loggerName":
"ocpm.pcf.service.common.domain.serviceconnector.PolicyServiceException",
  "message": "Max Attempts Reached for PRE connections",
  "endOfBatch": false,
  "loggerFqn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 125,
  "threadPriority": 5,
  "messageTimestamp": "2021-06-07T07:56:28.652+0000"
}
{
  "instant": {
    "epochSecond": 1623052588,
    "nanoOfSecond": 653125047
  },
  "thread": "boundedElastic-7",
  "level": "ERROR",
  "loggerName":
"ocpm.pcf.service.common.domain.serviceconnector.PolicyServiceConnector",
  "message": "Failed to call policy service: {} ",
  "thrown": {
    "commonElementCount": 0,
    "name":
"ocpm.pcf.service.common.domain.serviceconnector.PolicyServiceException",
    "extendedStackTrace":
"ocpm.pcf.service.common.domain.serviceconnector.PolicyServiceException:
null\n\tat
ocpm.pcf.service.common.domain.serviceconnector.PolicyServiceConnector.lambda$
processObject$4(PolicyServiceConnector.java:106) ~[classes!/:?]\n\tat
reactor.util.retry.RetryBackoffSpec.lambda$generateCompanion$4(RetryBackoffSpe
c.java:557) ~[reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.FluxConcatMap$ConcatMapImmediate.drain(FluxConcatMap.ja
va:374) [reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.FluxConcatMap$ConcatMapImmediate.onNext(FluxConcatMap.j
ava:250) [reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.EmitterProcessor.drain(EmitterProcessor.java:491)
[reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.EmitterProcessor.tryEmitNext(EmitterProcessor.java:299)
[reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.SinkManySerialized.tryEmitNext(SinkManySerialized.java:
97) [reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.InternalManySink.emitNext(InternalManySink.java:27)
[reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.FluxRetryWhen$RetryWhenMainSubscriber.onError(FluxRetry
When.java:189) [reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.publisher.MonoPublishOn$PublishOnSubscriber.run(MonoPublishOn.jav
a:187) [reactor-core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.scheduler.SchedulerTask.call(SchedulerTask.java:68) [reactor-
```

```

core-3.4.3.jar!/:3.4.3]\n\tat
reactor.core.scheduler.SchedulerTask.call(SchedulerTask.java:28) [reactor-
core-3.4.3.jar!/:3.4.3]\n\tat
java.util.concurrent.FutureTask.run(FutureTask.java:264) [?:?]\n\tat
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Sched
uledThreadPoolExecutor.java:304) [?:?]\n\tat
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1130
) [?:?]\n\tat
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:630
) [?:?]\n\tat java.lang.Thread.run(Thread.java:832) [?:?]\n"
    },
    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 125,
    "threadPriority": 5,
    "messageTimestamp": "2021-06-07T07:56:28.653+0000"
  }
}
{
  "instant": {
    "epochSecond": 1623052588,
    "nanoOfSecond": 653405431
  },
  "thread": "boundedElastic-7",
  "level": "DEBUG",
  "loggerName":
"ocpm.pcf.service.common.domain.component.policy.PolicyManager",
  "message": "process PolicyReply",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 125,
  "threadPriority": 5,
  "messageTimestamp": "2021-06-07T07:56:28.653+0000"
}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. Check whether all the pods are running or not.
2. Verify that correct URLs have been mentioned in the deployment file.
3. Update any incorrect or missing information in the deployment file.
4. Run the policy again.

Inter-microservice communication failures

Symptom

SM service receives failed to call Policy service error.

Problem

When the microservices are unable to establish communication with the each other, an error occurs and a message is received at SM service stating that the system failed to call Policy service. Search for an error message similar to the following:

```

logMsg=Failed to call Binding service for
a8f8cf48-b889-44ee-95e6-a9b82fdeef3

```

Error has been observed at the following site(s):
|_ checkpoint ? Request to POST <http://my-cnpolicy-occp-binding:8000/binding/v1/contextBinding/context-owner/PCF-SM> [DefaultWebClient]

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant":
  {
    "epochSecond":1622547969,"nanoOfSecond":166956262},
  "thread":"boundedElastic-14",
  "level":"ERROR",
  "loggerName":"ocpm.pcf.service.sm.serviceconnector.BindingServiceConnector",
  "message":"Failed to call Binding service for a8f8cf48-b889-44ee-95e6-a9b82fdeef3 :

```

```
org.springframework.web.reactive.function.client.WebClientRequestException:
Connection
  refused; nested exception is java.net.ConnectException: Connection refused

```

```
",
  "endOfBatch":false,
  "loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
  "threadId":23640,
  "threadPriority":5,
  "messageTimestamp":"2021-06-01T11:46:09.166+0000"}
org.springframework.web.reactive.function.client.WebClientRequestException:
Connection
  refused; nested exception is java.net.ConnectException: Connection
refusedat

```

```
org.springframework.web.reactive.function.client.ExchangeFunctions$DefaultExchangeFunction.lambda$wrapException$9(ExchangeFunctions.java:137)Suppressed:
reactor.core.publisher.FluxOnAssembly$OnAssemblyException:Error has been
observed at the following site(s):|_ checkpoint ? Request to POST http://my-cnpolicy-occp-binding:8000/binding/v1/contextBinding/context-owner/PCF-SM
[DefaultWebClient]Stack trace:at

```

```
org.springframework.web.reactive.function.client.ExchangeFunctions$DefaultExchangeFunction.lambda$wrapException$9(ExchangeFunctions.java:137)at
reactor.core.publisher.MonoErrorSupplied.subscribe(MonoErrorSupplied.java:70)at
reactor.core.publisher.Mono.subscribe(Mono.java:4046)at

```

```
reactor.core.publisher.FluxOnErrorResume$ResumeSubscriber.onError(FluxOnErrorResume.java:103)at

```

```
reactor.core.publisher.FluxPeekFuseable$PeekFuseableSubscriber.onError(FluxPeekFuseable.java:234)at

```

```
reactor.core.publisher.FluxPeekFuseable$PeekFuseableSubscriber.onError(FluxPeekFuseable.java:234)at
reactor.core.publisher.Operators$MonoSubscriber.onError(Operators.java:1862)at

```

```
reactor.core.publisher.MonoIgnoreThen$ThenAcceptInner.onError(MonoIgnoreThen.java:315)at

```

```
org.eclipse.jetty.reactive.client.internal.AbstractSingleProcessor.onError(AbstractSingleProcessor.java:119)at

```

```
org.eclipse.jetty.reactive.client.internal.ResponseListenerProcessor.onComplete(ResponseListenerProcessor.java:140)at

```

```
org.eclipse.jetty.client.ResponseNotifier.notifyComplete(ResponseNotifier.java
:218)at

org.eclipse.jetty.client.ResponseNotifier.notifyComplete(ResponseNotifier.java
:210)at

org.eclipse.jetty.client.HttpExchange.notifyFailureComplete(HttpExchange.java:
269)at org.eclipse.jetty.client.HttpExchange.abort(HttpExchange.java:240)at
org.eclipse.jetty.client.HttpConversation.abort(HttpConversation.java:149)at
org.eclipse.jetty.client.HttpRequest.abort(HttpRequest.java:818)at
org.eclipse.jetty.client.HttpDestination.abort(HttpDestination.java:506)at
org.eclipse.jetty.client.HttpDestination.failed(HttpDestination.java:253)at

org.eclipse.jetty.client.AbstractConnectionPool$FutureConnection.failed(Abstra
ctConnectionPool.java:551)at
org.eclipse.jetty.util.Promise$Wrapper.failed(Promise.java:136)at
org.eclipse.jetty.client.HttpClient$1$1.failed(HttpClient.java:633)at

org.eclipse.jetty.http2.client.http.HttpClientTransportOverHTTP2$SessionListen
erPromise.failConnectionPromise(HttpClientTransportOverHTTP2.java:261)at

org.eclipse.jetty.http2.client.http.HttpClientTransportOverHTTP2$SessionListen
erPromise.failed(HttpClientTransportOverHTTP2.java:194)at

org.eclipse.jetty.http2.client.HTTP2Client$ClientSelectorManager.connectionFai
led(HTTP2Client.java:516)at
org.eclipse.jetty.io.ManagedSelector$Connect.failed(ManagedSelector.java:929)at
org.eclipse.jetty.io.ManagedSelector.processConnect(ManagedSelector.java:335)at
org.eclipse.jetty.io.ManagedSelector.access$1600(ManagedSelector.java:62)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.processSelected(ManagedSelector
.java:639)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.produce(ManagedSelector.java:50
1)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.produceTask(EatWhatYouKi
ll.java:360)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.doProduce(EatWhatYouKill
.java:184)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.tryProduce(EatWhatYouKil
l.java:171)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.run(EatWhatYouKill.java:
129)at

org.eclipse.jetty.util.thread.ReservedThreadExecutor$ReservedThread.run(Reserv
edThreadExecutor.java:375)at
org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:77
3)at

org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPool.jav
a:905)at java.base/java.lang.Thread.run(Thread.java:832)Caused by:
java.net.ConnectException: Connection refusedat java.base/
sun.nio.ch.Net.pollConnect(Native Method)at java.base/
```

```

sun.nio.ch.Net.pollConnectNow(Net.java:660)at java.base/
sun.nio.ch.SocketChannelImpl.finishConnect(SocketChannelImpl.java:875)at
org.eclipse.jetty.io.SelectorManager.doFinishConnect(SelectorManager.java:355)at
org.eclipse.jetty.io.ManagedSelector.processConnect(ManagedSelector.java:313)at
org.eclipse.jetty.io.ManagedSelector.access$1600(ManagedSelector.java:62)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.processSelected(ManagedSelector
.java:639)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.produce(ManagedSelector.java:50
1)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.produceTask(EatWhatYouKill
.java:360)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.doProduce(EatWhatYouKill
.java:184)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.tryProduce(EatWhatYouKill
.java:171)at

org.eclipse.jetty.util.thread.strategy.EatWhatYouKill.run(EatWhatYouKill.java:
129)at

org.eclipse.jetty.util.thread.ReservedThreadExecutor$ReservedThread.run(Reserv
edThreadExecutor.java:375)at
org.eclipse.jetty.util.thread.QueuedThreadPool.runJob(QueuedThreadPool.java:77
3)at

org.eclipse.jetty.util.thread.QueuedThreadPool$Runner.run(QueuedThreadPool.jav
a:905)at java.base/java.lang.Thread.run(Thread.java:832)

```

Resolution Steps

To resolve this issue, perform the following steps:

PCF is suspended with both primary and secondary NRF

Symptom

SM service receives status of services associated with NfType: PCF is Deregistration service warning.

Problem

When the SM service tries to establish communication with the NRF client, but PCF is suspended with both primary and secondary NRF, a warning message is received. User may search for the following log message:

```
logMsg=Status of services associated with NfType :PCF is Deregistration, nrfInstanceId=<>,
response=<>
```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```

{
  "instant": {
    "epochSecond": 1622098819,
    "nanoOfSecond": 615494329
  },
  "thread": "main",
  "level": "WARN",

```

```

    "loggerName": "com.oracle.cgbu.cnc.nrf.NRFManagement",
    "message": "Status of services associated with NfType :PCF is
Deregistration",
    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 1,
    "threadPriority": 5,
    "source": {
      "method": "registerNfInstance",
      "file": "NRFManagement.java",
      "line": 843,
      "class": "com.oracle.cgbu.cnc.nrf.NRFManagement"
    },
    "messageTimestamp": "2021-05-27T07:00:19.615+0000"
  }
}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. Check whether the `primaryNrfApiRoot` and `secondaryNrfApiRoot` point to the correct endpoints.
2. Check the status of the **pcf-sm-service** pod.
3. Check the logs of `nrf-management` pod.
4. If the `pcf-sm-service` is down and NRF discovery is not able to register then restart the `pcf-sm-service` pod.
5. Check the logs of `nrf-management` pod again to verify if the registration has happened successfully.

Failed to write to database

Symptom

SM service receives error on trying to save data in database.

Problem

When the SM service tries to write to database, but the request is not processed and the following error message is generated:

```
logMsg="Could not create connection to database server"
```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```

{
  "instant": {
    "epochSecond": 1622819336,
    "nanoOfSecond": 250368963
  },
  "thread": "main",
  "level": "INFO",
  "loggerName": "ocpm.cne.common.db.JdbcDbClient",
  "message": "Maximum Pool Size is: 32 ",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 1,

```

```

    "threadPriority": 5,
    "messageTimestamp": "2021-06-04T15:08:56.250+0000"
  }
  {
    "instant": {
      "epochSecond": 1622819336,
      "nanoOfSecond": 265776725
    },
    "thread": "main",
    "level": "WARN",
    "loggerName": "com.zaxxer.hikari.HikariConfig",
    "message": "HikariPool-1 - idleTimeout has been set but has no effect
because the pool is operating as a fixed size pool.",
    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 1,
    "threadPriority": 5,
    "messageTimestamp": "2021-06-04T15:08:56.265+0000"
  }
  {"instant":
{"epochSecond":1622819342,"nanoOfSecond":432547862},"thread":"main","level":"E
RROR","loggerName":"com.zaxxer.hikari.pool.HikariPool","message":"HikariPool-1
- Exception during pool
initialization.,"thrown":
{"commonElementCount":0,"localizedMessage":"Could not create
connection to database server. Attempted reconnect 3 times. Giving
up.,"message":"Could
not create connection to database server. Attempted reconnect 3 times.
Giving
up.,"name":"java.sql.SQLException","cause":
{"commonElementCount":67,"localizedMessage":"Communications
link failure\n\nThe last packet sent successfully to the server was 0
milliseconds ago. The
driver has not received any packets from the
server.,"message":"Communications link
failure\n\nThe last packet sent successfully to the server was 0
milliseconds ago. The driver
has not received any packets from the

server.,"name":"com.mysql.cj.exceptions.CJCommunicationsException","cause":
{"commonElementCount":67,"localizedMessage":"Connection
refused","message":"Connection
refused","name":"java.net.ConnectException","extendedStackTrace":"java.net.ConnectE
xception: Connection refused\n\tat sun.nio.ch.Net.pollConnect\(Native Method\)
~\[?:?\]\n\tat sun.nio.ch.Net.pollConnectNow\(Net.java:660\) ~\[?:?\]\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect\(NioSocketImpl.java:542\)
~\[?:?\]\n\tat sun.nio.ch.NioSocketImpl.connect\(NioSocketImpl.java:597\)
~\[?:?\]\n\tat java.net.SocksSocketImpl.connect\(SocksSocketImpl.java:333\) ~\[?:?\]
\n\tat java.net.Socket.connect\(Socket.java:648\) ~\[?:?\]\n\tat

com.mysql.cj.protocol.StandardSocketFactory.connect\(StandardSocketFactory.java
:155\)
~\[mysql-connector-java-8.0.23.jar!/8.0.23\]\n\tat

com.mysql.cj.protocol.a.NativeSocketConnection.connect\(NativeSocketConnection.
java:63\)

```

```

-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat
com.mysql.cj.NativeSession.connect(NativeSession.java:144)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat

com.mysql.cj.jdbc.ConnectionImpl.connectWithRetries(ConnectionImpl.java:847)
-[mysql-connector-
java-8.0.23.jar!/:8.0.23]\n"}, "extendedStackTrace": "com.mysql.cj.exceptions.CJ
CommunicationsException:
    Communications link failure\n\nThe last packet sent successfully to the
server was 0
    milliseconds ago. The driver has not received any packets from the
server.\n\tat
    jdk.internal.reflect.NativeConstructorAccessorImpl.newInstance0(Native
Method) ~[?:?]\n\tat

jdk.internal.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstruct
orAccessorImpl.java:64)
~[?:?]\n\tat

jdk.internal.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingC
onstructorAccessorImpl.java:45)
~[?:?]\n\tat
java.lang.reflect.Constructor.newInstanceWithCaller(Constructor.java:500)
~[?:?]\n\tat
java.lang.reflect.Constructor.newInstance(Constructor.java:481) ~[?:?]\n\tat

com.mysql.cj.exceptions.ExceptionFactory.createException(ExceptionFactory.java
:61)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat

com.mysql.cj.exceptions.ExceptionFactory.createException(ExceptionFactory.java
:105)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat

com.mysql.cj.exceptions.ExceptionFactory.createException(ExceptionFactory.java
:151)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat

com.mysql.cj.exceptions.ExceptionFactory.createCommunicationsException(Excepti
onFactory.java:167)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat

com.mysql.cj.protocol.a.NativeSocketConnection.connect(NativeSocketConnection.
java:89)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat
com.mysql.cj.NativeSession.connect(NativeSession.java:144)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]\n\tat

com.mysql.cj.jdbc.ConnectionImpl.connectWithRetries(ConnectionImpl.java:847)
-[mysql-connector-java-8.0.23.jar!/:8.0.23]

```

Resolution Steps

To resolve this issue, perform the following steps:

1. Check the database connection details of the specific deployment file.
2. Update any missing or incorrect details.

3. Check whether the database tables are created properly and include all the required columns.

4.3.2 CM Service Issues

This section describes the most common Configuration Management (CM) service issues and their resolution steps. It is recommended for users to attempt the resolution steps provided in this guide before contacting Oracle Support.

Configuration Management GUI not loading configuration data

Symptom

Configuration data is not updated in the GUI, that is, Cloud Native Configuration Console (CNC Console).

Problem

When the configuration data is not loaded in the configuration management GUI, the following error message is generated:

```
logMsg=Error fetching config-items for topic: common.logging.config-mgmt,
retry after 1000
      milliseconds and retry count = 1
```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{"instant":
{"epochSecond":1622099002,"nanoOfSecond":761814372},"thread":"pool-6-
thread-1","level":"ERROR","loggerName":"ocpm.cne.common.configclient.ConfigSer
verConnectionWithRetry","message":"Could
      not fetch config-items for topic: common.logging.config-mgmt, maxRetry
is
exhausted.", "endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLog
ger","threadId":28,"threadPriority":5,"messageTimestamp":"2021-05-27T07:03:22.
761+0000"}{"instant":
{"epochSecond":1622099005,"nanoOfSecond":792401204},"thread":"pool-6-
thread-1","level":"WARN","loggerName":"ocpm.cne.common.configclient.ConfigServ
erConnectionWithRetry","message":"Error
      fetching config-items for topic: common.logging.config-mgmt, retry
after 1000 milliseconds and
      retry count = 1. Exception:
      ", "thrown":
{"commonElementCount":0,"localizedMessage":"java.net.ConnectException:
Connection refused","message":"java.net.ConnectException: Connection
refused","name":"javax.ws.rs.ProcessingException","cause":
{"commonElementCount":16,"localizedMessage":"Connection
      refused","message":"Connection
refused","name":"java.net.ConnectException","extendedStackTrace":"java.net.ConnectE
xception: Connection refused\n\tat sun.nio.ch.Net.pollConnect(Native Method)
~[?:?]\n\tat sun.nio.ch.Net.pollConnectNow(Net.java:660) ~[?:?]\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:549)
~[?:?]\n\tat sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597)
~[?:?]\n\tat java.net.Socket.connect(Socket.java:648) ~[?:?]\n\tat
sun.net.NetworkClient.doConnect(NetworkClient.java:177) ~[?:?]\n\tat
```

```

sun.net.www.http.HttpClient.openServer(HttpClient.java:474) ~[?:?]\n\tat
sun.net.www.http.HttpClient.openServer(HttpClient.java:569) ~[?:?]\n\tat
sun.net.www.http.HttpClient.<init>(HttpClient.java:242) ~[?:?]\n\tat
sun.net.www.http.HttpClient.New(HttpClient.java:341) ~[?:?]\n\tat
sun.net.www.http.HttpClient.New(HttpClient.java:362) ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getNewHttpClient(HttpURLConnection.j
ava:1261)
    ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.plainConnect0(HttpURLConnection.java
:1194)
    ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.java:
1082)
    ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.connect(HttpURLConnection.java:1016)
    ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getInputStream0(HttpURLConnection.ja
va:1600)
    ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.jav
a:1528)
    ~[?:?]\n\tat
java.net.HttpURLConnection.getResponseCode(HttpURLConnection.java:527) ~[?:?]
\n\tat

org.glassfish.jersey.client.internal.HttpUrlConnector._apply(HttpUrlConnector.
java:367)
    ~[jersey-client-2.30.1.jar!/:?]\n\tat

org.glassfish.jersey.client.internal.HttpUrlConnector.apply(HttpUrlConnector.j
ava:259)
    ~[jersey-client-2.30.1.jar!/:?]
\n"}, "extendedStackTrace": "javax.ws.rs.ProcessingException:
java.net.ConnectException: Connection refused\n\tat

org.glassfish.jersey.client.internal.HttpUrlConnector.apply(HttpUrlConnector.j
ava:261)
    ~[jersey-client-2.30.1.jar!/:?]\n\tat
    org.glassfish.jersey.client.ClientRuntime.invoke(ClientRuntime.java:296)
    ~[jersey-client-2.30.1.jar!/:?]\n\tat

org.glassfish.jersey.client.JerseyInvocation.lambda$invoke$2(JerseyInvocation.
java:643)
    ~[jersey-client-2.30.1.jar!/:?]\n\tat
    org.glassfish.jersey.internal.Errors.process(Errors.java:292)
    ~[jersey-common-2.30.1.jar!/:?]\n\tat
    org.glassfish.jersey.internal.Errors.process(Errors.java:274)
    ~[jersey-common-2.30.1.jar!/:?]\n\tat
    org.glassfish.jersey.internal.Errors.process(Errors.java:205)
    ~[jersey-common-2.30.1.jar!/:?]\n\tat

org.glassfish.jersey.process.internal.RequestScope.runInScope(RequestScope.jav
a:390)
    ~[jersey-common-2.30.1.jar!/:?]\n\tat

org.glassfish.jersey.client.JerseyInvocation.invoke(JerseyInvocation.java:641)

```

```

~[jersey-client-2.30.1.jar!/:?]\n\tat
org.glassfish.jersey.client.JerseyInvocation$Builder.method(JerseyInvocation.java:414)
~[jersey-client-2.30.1.jar!/:?]\n\tat
org.glassfish.jersey.client.JerseyInvocation$Builder.get(JerseyInvocation.java:305)
~[jersey-client-2.30.1.jar!/:?]\n\tat
ocpm.cne.common.configclient.ConfigServerConnectionWithRetry.getConfigurati
onItemByTopicWithRetry(ConfigServerConnectionWithRetry.java:313)
[cne-common-1.11.0.jar!/:?]\n\tat
ocpm.cne.common.configclient.ConfigClient.getConfigurati
onItemByTopic(ConfigClient.java:178)
[cne-common-1.11.0.jar!/:?]\n\tat
ocpm.cne.common.configclient.ConfigClient.getConfigurati
onItemByTopic(ConfigClient.java:149)
[cne-common-1.11.0.jar!/:?]\n\tat
ocpm.cne.common.logging.level.PullLogLevelConfigTask.run(PullLogLevelConfigTask.java:68)
[cne-common-1.11.0.jar!/:?]\n\tat
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1130)
[?:?]\n\tat
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:630)
[?:?]\n\tat
java.lang.Thread.run(Thread.java:832) [?:?]\nCaused by:
java.net.ConnectException: Connection refused\n\tat
sun.nio.ch.Net.pollConnect(Native Method) ~[?:?]\n\tat
sun.nio.ch.Net.pollConnectNow(Net.java:660) ~[?:?]\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:549)
~[?:?]\n\tat sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597)
~[?:?]\n\tat java.net.Socket.connect(Socket.java:648) ~[?:?]\n\tat
sun.net.NetworkClient.doConnect(NetworkClient.java:177) ~[?:?]\n\tat
sun.net.www.http.HttpClient.openServer(HttpClient.java:474) ~[?:?]\n\tat
sun.net.www.http.HttpClient.openServer(HttpClient.java:569) ~[?:?]\n\tat
sun.net.www.http.HttpClient.<init>(HttpClient.java:242) ~[?:?]\n\tat
sun.net.www.http.HttpClient.New(HttpClient.java:341) ~[?:?]\n\tat
sun.net.www.http.HttpClient.New(HttpClient.java:362) ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getNewHttpClient(HttpURLConnection.java:1261)
~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.plainConnect0(HttpURLConnection.java:1194)
~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.java:1082)
~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.connect(HttpURLConnection.java:1016)
~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getInputStream0(HttpURLConnection.java:

```

```

va:1600)
    ~[?:?]\n\tat
    sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.jav
a:1528)
    ~[?:?]\n\tat
    java.net.HttpURLConnection.getResponseCode(HttpURLConnection.java:527) ~[?:?]
\n\tat

org.glassfish.jersey.client.internal.HttpUrlConnector._apply(HttpUrlConnector.
java:367)
    ~[jersey-client-2.30.1.jar!/:?]\n\tat

org.glassfish.jersey.client.internal.HttpUrlConnector.apply(HttpUrlConnector.j
ava:259)
    ~[jersey-client-2.30.1.jar!/:?]\n\t... 16

more\n"},"endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger
","threadId":28,"threadPriority":5,"messageTimestamp":"2021-05-27T07:03:25.792
+0000"}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. Check the status of the config-management and config-server pods.
 2. Check the logs of config-server pod and rule out errors related to database or connection.
 3. If the config-server is itself down, restart the config-server pod. Then, check the logs of config-management.
- After performing these steps, the data should be available on CNC Console.

4.3.3 Audit Service Issues

This section describes the most common Audit service issues and their resolution steps. It is recommended for users to attempt the resolution steps provided in this guide before contacting Oracle Support.

Audit service unable to notify services about stale session

Symptom

Audit service receives error message on sending a notification request.

Problem

When the audit service detects a stale session, it sends a notification to the owner service about the stale records. When the notification request sent by Audit service is not successful, it receives a response similar to the following error:

```

logMsg=Error sending notification request to http://my-cnpolicy-occpn-pcf-
sm:8005/audit/notify

```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```

{
  "instant": {

```

```

        "epochSecond": 1623075339,
        "nanoOfSecond": 71945796
    },
    "thread": "main",
    "level": "WARN",
    "loggerName": "org.hibernate.orm.connections.pooling",
    "message": "HHH10001002: Using Hibernate built-in connection pool (not for
production use!)",
    "endOfBatch": false,
    "loggerFqcn": "org.hibernate.internal.log.ConnectionPoolingLogger_$logger",
    "threadId": 1,
    "threadPriority": 5,
    "messageTimestamp": "2021-06-07T14:15:39.071+0000"
}
{
    "instant": {
        "epochSecond": 1623075340,
        "nanoOfSecond": 282816509
    },
    "thread": "Thread-6",
    "level": "ERROR",
    "loggerName": "ocpm.common.service.audit.services.NotifyTask",
    "message": "Error sending notification request to http://my-cnpolicy-occp-
pcf-sm:8005/audit/notify",
    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 69,
    "threadPriority": 5,
    "messageTimestamp": "2021-06-07T14:15:40.282+0000"
}
{
    "instant": {
        "epochSecond": 1623075340,
        "nanoOfSecond": 285152533
    },
    "thread": "pool-4-thread-1",
    "level": "ERROR",
    "loggerName": "ocpm.common.service.audit.services.NotifyTask",
    "message": "Notification was not sent to http://my-cnpolicy-occp-pcf-
sm:8005/audit/notify due to an error",
    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 62,
    "threadPriority": 5,
    "messageTimestamp": "2021-06-07T14:15:40.285+0000"
}
}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. Verify if the correct value has been entered for `AUDIT_NOTIFICATION_URL` in the deployment file of SM service.
2. Ensure that the value of `notificationUri` in the **AuditRegistrations** database table has the same value as mentioned in the SM service deployment file.
After performing these steps, check the logs again.

4.3.4 UDR Connector Issues

This section describes the most common UDR Connector issues and their resolution steps. Users are recommended to attempt the resolution steps provided in this guide before contacting Oracle Support.

Failed or no UDR on-demand discovery to NRF on Egress Gateway

Symptom

UDR returns status code: 424 FAILED_DEPENDENCY on receiving a request from UDR connector.

Problem

When the UDR connector sends a request to UDR to fetch for example SmPolicyData, UDR tries to establish connection with NRF on Egress Gateway to process the on-demand discovery request. However, when it is unable to establish the connection, it returns the following status code:

ClientResponse has erroneous status code: 424 FAILED_DEPENDENCY

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant": {
    "epochSecond": 1622112585,
    "nanoOfSecond": 184133637
  },
  "thread": "XNIO-1 task-5",
  "level": "INFO",
  "loggerName":
"ocpm.pcf.service.ud.intf.restful.api.UserDataUniformApiController",
  "message": "Received GET request, ueIdList: [imsi-650081000000606],
reqParam: {\smPolicyDataReq\":
{\\"subscription\":false,\\"params\":null,\\"snssai\":
{\\"sst\":11,\\"sd\":\\"abc123\\"},\\"dnn\":\\"dnn1\\",\\"fields\":null},\\"ldapDataReq
\":{\\"subscription\":false,\\"params\":null},\\"ssvEnabled\":false}",
  "endOfBatch": false,
  "loggerFqn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 86,
  "threadPriority": 5,
  "messageTimestamp": "2021-05-27T10:49:45.184+0000"
}
{
  "instant": {
    "epochSecond": 1622112585,
    "nanoOfSecond": 186728033
  },
  "thread": "UserService_ThreadPool_6",
  "level": "DEBUG",
  "loggerName": "ocpm.pcf.service.ud.core.AbstractCommonService",
  "message": "Initialize user for [imsi-650081000000606], result:
{\pk\":\\"6966884214826339058\\",\\"ueIdList\":
[\imsi-650081000000606\\],\\"policyDataProfile\":{\\"subscriptionMap\":{}}}",
```

```

    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 115,
    "threadPriority": 5,
    "messageTimestamp": "2021-05-27T10:49:45.186+0000"
  }
}
{
  "instant": {
    "epochSecond": 1622112585,
    "nanoOfSecond": 189665164
  },
  "thread": "UserService_ThreadPool_6",
  "level": "INFO",
  "loggerName": "ocpm.pcf.service.ud.dbplugin.ds.udr.UdrDataSourceService",
  "message": "discover UDR instance on demand: http://pcf1111-ocnp-nrf-client-nfdiscovery:8000/nnrf-disc/v1/nf-instances?target-nf-type=UDR&requester-nf-type=PCF&service-names=nudr-dr&supi=imsi-650081000000606",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 115,
  "threadPriority": 5,
  "messageTimestamp": "2021-05-27T10:49:45.189+0000"
}

{"instant":
{"epochSecond":1622112585,"nanoOfSecond":184133637},"thread":"XNIO-1
task-5","level":"INFO","loggerName":"ocpm.pcf.service.ud.intf.restful.api.User
DataUniformApiController","message":"Received GET request, ueIdList:
[imsi-650081000000606], reqParam: {\smPolicyDataReq\":
{\subscription\":false,\"params\":null,\"snssai\":
{\sst\":11,\"sd\": \"abc123\"},\"dnn\": \"dnn1\", \"fields\":null},\"ldapDataReq
\":
{\subscription\":false,\"params\":null,\"ssvEnabled\":false}},\"endOfBatch\":f
alse,\"loggerFqcn\":\"org.apache.logging.slf4j.Log4jLogger\",\"threadId\":86,\"thread
Priority\":5,\"messageTimestamp\":\"2021-05-27T10:49:45.184+0000\"}
{"instant":
{"epochSecond":1622112585,\"nanoOfSecond\":186728033},\"thread\":\"UserService_Thre
adPool_6\",\"level\":\"DEBUG\",\"loggerName\":\"ocpm.pcf.service.ud.core.AbstractCommo
nService\",\"message\":\"Initialize user for [imsi-650081000000606], result:
{\pk\": \"6966884214826339058\", \"ueIdList\":
[\imsi-650081000000606], \"policyDataProfile\":{\subscriptionMap\":
{}}},\"endOfBatch\":false,\"loggerFqcn\":\"org.apache.logging.slf4j.Log4jLogger\", \"
threadId\":115,\"threadPriority\":5,\"messageTimestamp\":\"2021-05-27T10:49:45.186+0
000\"}
{"instant":
{"epochSecond":1622112585,\"nanoOfSecond\":189665164},\"thread\":\"UserService_Thre
adPool_6\",\"level\":\"INFO\",\"loggerName\":\"ocpm.pcf.service.ud.dbplugin.ds.udr.Udr
DataSourceService\",\"message\":\"discover UDR instance on demand: http://pcf1111-
ocnp-nrf-client-nfdiscovery:8000/nnrf-disc/v1/nf-instances?target-nf-
type=UDR&requester-nf-type=PCF&service-names=nudr-
dr&supi=imsi-650081000000606\", \"endOfBatch\":false,\"loggerFqcn\":\"org.apache.logg
ing.slf4j.Log4jLogger\", \"threadId\":115,\"threadPriority\":5,\"messageTimestamp\":\"2
021-05-27T10:49:45.189+0000\"}

```

```

{"instant":
{"epochSecond":1622112586,"nanoOfSecond":782028662},"thread":"UserService_Thre
adPool_6","level":"WARN","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.udr.Udr
DataSourceService","message":"ClientResponse has erroneous status code: 424
FAILED_DEPENDENCY, body:
","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thre
adId":115,"threadPriority":5,"messageTimestamp":"2021-05-27T10:49:46.782+0000"
}
{"instant":
{"epochSecond":1622112586,"nanoOfSecond":782274717},"thread":"UserService_Thre
adPool_6","level":"DEBUG","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.udr.Ud
rDataSourceService","message":"Check for
response:null","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4j
Logger","threadId":115,"threadPriority":5,"messageTimestamp":"2021-05-27T10:49
:46.782+0000"}
{"instant":
{"epochSecond":1622112586,"nanoOfSecond":782622756},"thread":"UserService_Thre
adPool_6","level":"DEBUG","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.udr.Ud
rDataSourceService","message":"Retry Exception result:
true","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","
threadId":115,"threadPriority":5,"messageTimestamp":"2021-05-27T10:49:46.782+0
000"}
{"instant":
{"epochSecond":1622112586,"nanoOfSecond":782858203},"thread":"UserService_Thre
adPool_6","level":"DEBUG","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.Altern
ateRouteServiceHelper","message":"Check Retry: Profile: RetryProfileObject
[name = udr-retry, enableRetrySettings = true, enableAlternateRouting = true]
SubQuery_Count: 0 retryCount:
2","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thr
eadId":115,"threadPriority":5,"messageTimestamp":"2021-05-27T10:49:46.782+0000
"}
{"instant":
{"epochSecond":1622112586,"nanoOfSecond":783021549},"thread":"UserService_Thre
adPool_6","level":"DEBUG","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.Altern
ateRouteServiceHelper","message":"RETRY status: true, subQueryRetry: 1,
ConfiguredRetryCount:
2","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","thr
eadId":115,"threadPriority":5,"messageTimestamp":"2021-05-27T10:49:46.783+0000
"}
{"instant":
{"epochSecond":1622112586,"nanoOfSecond":783292038},"thread":"UserService_Thre
adPool_6","level":"INFO","loggerName":"ocpm.pcf.service.ud.dbplugin.ds.udr.Udr
DataSourceService","message":"discover UDR instance on demand: http://pcf1111-
ocnp-nrf-client-nfdiscovery:8000/nnrf-disc/v1/nf-instances?target-nf-
type=UDR&requester-nf-type=PCF&service-names=nudr-
dr&supi=imsi-650081000000606","endOfBatch":false,"loggerFqcn":"org.apache.logg
ing.slf4j.Log4jLogger","threadId":115,"threadPriority":5,"messageTimestamp":"2
021-05-27T10:49:46.783+0000"}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. In the application-config yaml file, check whether UDR is present in **nrfClientSubscribeTypes** values or not. If it is not present, then add UDR.
2. Restart nrf-management pod.

3. Verify on-demand flag in PCF user connector GUI.
4. After resending the request, check the UDR and NRF-management logs to verify if the request for on-demand discovery has been processed successfully.

Failed or no Policy data request to UDR on Egress Gateway

Symptom

UDR returns Could NOT find any NFProfile, set NullDataSource for UDR on receiving a policy data request from UDR connector on Egress Gateway.

Problem

To fetch policy data, for example SmPolicyData, UDR connector sends a request to UDR. However, when the UDR is unable to process the policy data request successfully, the following response is received in the log message:

Could NOT find any NFProfile, set NullDataSource for UDR

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant":
  {
    "epochSecond":1622025233,"nanoOfSecond":476028210},
    "thread":"main","level":"WARN",
    "loggerName":"io.undertow.websockets.jsr","message":"UT026010:
      Buffer pool was not set on WebSocketDeploymentInfo, the default pool
      will be

used","endOfBatch":false,"loggerFqcn":"io.undertow.websockets.jsr.JsrWebSocket
Logger_$logger","threadId":1,"threadPriority":5,"messageTimestamp":"2021-05-26
T10:33:53.476+0000"}{
  "instant":
  {
    "epochSecond":1622027281,"nanoOfSecond":565754129},
    "thread":"UserService_Thre
adPool_1","level":"WARN",
    "loggerName":"ocpm.pcf.service.ud.dbplugin.ds.udr.Udr
DataSourceService","message":"Could
      NOT find any NFProfile, set NullDataSource for

UDR","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":50,"threadPriority":5,"messageTimestamp":"2021-05-26T11:08:01.565+000
0"}{
  "instant":
  {
    "epochSecond":1622027281,"nanoOfSecond":576403066},
    "thread":"UserService_Thre
adPool_1","level":"WARN",
    "loggerName":"ocpm.pcf.service.ud.core.UdrService","m
essage":"Failed
      GET class ocpm.pcf.service.ud.domain.SmPolicyData, ueId:
      imsi-650081000000606, result:

FAILURE_DATASOURCENOTFOUND","endOfBatch":false,"loggerFqcn":"org.apache.loggin
g.slf4j.Log4jLogger","threadId":50,"threadPriority":5,"messageTimestamp":"2021
-05-26T11:08:01.576+0000"}{
  "instant":
  {
    "epochSecond":1622027281,"nanoOfSecond":580718514},
    "thread":"UserService_Thre
adPool_1","level":"WARN",
    "loggerName":"ocpm.pcf.service.ud.intf.restful.api.Ap
iControllerHelper","message":"A
      child [GET] request failed, <500 INTERNAL_SERVER_ERROR Internal Server
      Error,
[>","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":50,"threadPriority":5,"messageTimestamp":"2021-05-26T11:08:01.580+000
0"}{
  "instant":
  {
    "epochSecond":1622027281,"nanoOfSecond":582259973},
    "thread":"UserService_Thre
```

```

adPool_1", "level": "WARN", "loggerName": "ocpm.pcf.service.ud.intf.restful.api.ApiControllerHelper", "message": "Request
failed 500 INTERNAL_SERVER_ERROR,
requestContext=RequestContext{userIds=[imsi-650081000000606],
requestParams='{\"smPolicyDataReq\":
{\"subscription\":false,\"params\":null,\"snssai\":
{\"sst\":11,\"sd\": \"abc123\"}, \"dnn\": \"dnn1\", \"fields\":null}, \"ldapDataReq
\": {\"subscription\":false,\"params\":null}}',

requestType='GET'}.\", \"endOfBatch\":false, \"loggerFqcn\": \"org.apache.logging.slf4j
.Log4jLogger\", \"threadId\":50, \"threadPriority\":5, \"messageTimestamp\": \"2021-05-26T
11:08:01.582+0000\"}{\"instant\":
{\"epochSecond\":1622027658, \"nanoOfSecond\":279448141}, \"thread\": \"UserService_Thre
adPool_2\", \"level\": \"WARN\", \"loggerName\": \"ocpm.pcf.service.ud.dbplugin.ds.udr.Udr
DataSourceService\", \"message\": \"Could
NOT find any NFProfile, set NullDataSource for

UDR\", \"endOfBatch\":false, \"loggerFqcn\": \"org.apache.logging.slf4j.Log4jLogger\", \"t
hreadId\":55, \"threadPriority\":5, \"messageTimestamp\": \"2021-05-26T11:14:18.279+000
0\"}{\"instant\":
{\"epochSecond\":1622027658, \"nanoOfSecond\":280438989}, \"thread\": \"UserService_Thre
adPool_2\", \"level\": \"WARN\", \"loggerName\": \"ocpm.pcf.service.ud.core.UdrService\", \"m
essage\": \"Failed
GET class ocpm.pcf.service.ud.domain.SmPolicyData, ueId:
imsi-650081000000606, result:

FAILURE_DATASOURCENOTFOUND\", \"endOfBatch\":false, \"loggerFqcn\": \"org.apache.loggin
g.slf4j.Log4jLogger\", \"threadId\":55, \"threadPriority\":5, \"messageTimestamp\": \"2021
-05-26T11:14:18.280+0000\"}{\"instant\":
{\"epochSecond\":1622027658, \"nanoOfSecond\":280904616}, \"thread\": \"UserService_Thre
adPool_2\", \"level\": \"WARN\", \"loggerName\": \"ocpm.pcf.service.ud.intf.restful.api.Ap
iControllerHelper\", \"message\": \"A
child [GET] request failed, <500 INTERNAL_SERVER_ERROR Internal Server
Error,
[>\", \"endOfBatch\":false, \"loggerFqcn\": \"org.apache.logging.slf4j.Log4jLogger\", \"t
hreadId\":55, \"threadPriority\":5, \"messageTimestamp\": \"2021-05-26T11:14:18.280+000
0\"}{\"instant\":
{\"epochSecond\":1622027658, \"nanoOfSecond\":282162222}, \"thread\": \"UserService_Thre
adPool_2\", \"level\": \"WARN\", \"loggerName\": \"ocpm.pcf.service.ud.intf.restful.api.Ap
iControllerHelper\", \"message\": \"Request
failed 500 INTERNAL_SERVER_ERROR,
requestContext=RequestContext{userIds=[imsi-650081000000606],
requestParams='{\"smPolicyDataReq\":
{\"subscription\":false,\"params\":null,\"snssai\":
{\"sst\":11,\"sd\": \"abc123\"}, \"dnn\": \"dnn1\", \"fields\":null}, \"ldapDataReq
\": {\"subscription\":false,\"params\":null}}',

requestType='GET'}.\", \"endOfBatch\":false, \"loggerFqcn\": \"org.apache.logging.slf4j
.Log4jLogger\", \"threadId\":55, \"threadPriority\":5, \"messageTimestamp\": \"2021-05-26T
11:14:18.282+0000\"}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. Check in the application-config yaml file whether UDR is present in **nrfClientSubscribeTypes** values or not. If it is not present, then add UDR.

2. Restart nrf-management pod.
3. Check the logs of udr-connector to verify if the policy data request registration has been sent successfully.

UDR profile is found, but UDR request fails

Symptom

UDR returns error response with code 503 on receiving a request from UDR connector.

Problem

To fetch policy data, for example SmPolicyData, UDR connector sends a request to UDR. However, when the UDR is unable to process the policy data request despite finding the UDR profile, the following response is received in the log message:

```
logMsg=<500 INTERNAL_SERVER_ERROR Internal Server
      Error,{"type":"","title":"Service
      Unavailable"},"status":503,
```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant": {
    "epochSecond": 1627388645,
    "nanoOfSecond": 749163068
  },
  "thread": "UserService_ThreadPool_16",
  "level": "WARN",
  "loggerName": "ocpm.pcf.service.ud.intf.restful.api.ApiControllerHelper",
  "message": "A child [GET] request failed, <500 INTERNAL_SERVER_ERROR
  Internal Server Error,{"type":"","title":"Service
  Unavailable"},"status":503,\"detail\":\"Service
  Unavailable\",\"instance\":\"null\",\"cause\":\"null\",\"invalidParams\":\"null\"},[>",
  "endOfBatch": false,
  "loggerFqn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 3092,
  "threadPriority": 5,
  "messageTimestamp": "2021-07-27T12:24:05.749+0000"
}
{
  "instant": {
    "epochSecond": 1627388645,
    "nanoOfSecond": 749294213
  },
  "thread": "UserService_ThreadPool_16",
  "level": "WARN",
  "loggerName": "ocpm.pcf.service.ud.intf.restful.api.ApiControllerHelper",
  "message": "Request failed 500 INTERNAL_SERVER_ERROR,
  requestContext=RequestContext{userIds=[imsi-450081000000001],
  requestParams='{\"smPolicyDataReq\":
  {\"subscription\":false,\"params\":null,\"snssai\":
  {\"sst\":\"11\",\"sd\":\"abc123\"},\"dnn\":\"dnn1\",\"fields\":null},\"ldapDataReq
  \":{\"subscription\":false,\"params\":null,\"ssvEnabled\":true}',
  requestType='GET'}.",
  "endOfBatch": false,
```

```

    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 3092,
    "threadPriority": 5,
    "messageTimestamp": "2021-07-27T12:24:05.749+0000"
  }

```

Resolution Steps

To resolve this issue, perform the following steps:

- As UDR discovery is on-demand, when a request is received, check whether NRF-Management returns correct FQDN for UDR. If the FQDN is incorrect, update with the current value and initiate the request again.

Retry to CHF or UDR alternate route on timeout or error

Symptom

UDR returns error response for retrying to CHF or UDR alternate route on timeout or error in previous attempt.

Problem

To fetch policy data, for example SmPolicyData, UDR connector sends a request to UDR. However, when the UDR is unable to process the policy data request despite finding the UDR profile, the following response is received in the log message:

```

logMsg=Error performing GET operation for URI
      /nf-common-component/v1/nrf-client-nfmanagement/nfProfileList"

```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```

{"instant":
{"epochSecond":1627368379,"nanoOfSecond":172423065},"thread":"CmAgentTask1","level":"ERROR","loggerName":"ocpm.cne.common.cmclient.CmRestClient","message":"Error
    performing GET operation for URI
    /nf-common-component/v1/nrf-client-nfmanagement/nfProfileList","thrown":
{"commonElementCount":0,"localizedMessage":"I/O
    error on GET request for \"http://localhost:5000/nf-common-component/v1/nrf-client-nfmanagement/nfProfileList\": Connect to localhost:5000 [localhost/127.0.0.1,
    localhost/0:0:0:0:0:0:1] failed:
        Connection refused; nested exception is
    org.apache.http.conn.HttpHostConnectException: Connect
        to localhost:5000 [localhost/127.0.0.1, localhost/0:0:0:0:0:0:1]
    failed: Connection
        refused","message":"I/O error on GET request for \"http://localhost:5000/nf-common-component/v1/nrf-client-nfmanagement/nfProfileList\": Connect to localhost:5000
    [localhost/127.0.0.1, localhost/0:0:0:0:0:0:1] failed:
        Connection refused; nested exception is
    org.apache.http.conn.HttpHostConnectException: Connect
        to localhost:5000 [localhost/127.0.0.1, localhost/0:0:0:0:0:0:1]
    failed: Connection
        refused","name":"org.springframework.web.client.ResourceAccessException","cause":{
        "commonElementCount":14,"localizedMessage":"Connect
            to localhost:5000 [localhost/127.0.0.1, localhost/0:0:0:0:0:0:1]
            failed: Connection

```

```

        refused", "message": "Connect to localhost:5000 [localhost/127.0.0.1,
        localhost/0:0:0:0:0:0:0:1] failed: Connection
        refused", "name": "org.apache.http.conn.HttpHostConnectException", "cause":
{"commonElementCount":14, "localizedMessage": "Connection
        refused", "message": "Connection
        refused", "name": "java.net.ConnectException", "extendedStackTrace": "java.net.ConnectE
xception: Connection refused\n\tat sun.nio.ch.Net.pollConnect(Native Method)
~[?:?]\n\tat sun.nio.ch.Net.pollConnectNow(Net.java:669) ~[?:?]\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:542)
~[?:?]\n\tat sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597)
~[?:?]\n\tat java.net.SocksSocketImpl.connect(SocksSocketImpl.java:333) ~[?:?]
\n\tat java.net.Socket.connect(Socket.java:645) ~[?:?]\n\tat

org.apache.http.conn.socket.PlainConnectionSocketFactory.connectSocket(PlainCo
nnectionSocketFactory.java:75)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultH
ttpClientConnectionOperator.java:142)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHt
tpClientConnectionManager.java:376)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.ja
va:393)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat
org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.ja
va:185)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.ja
va:83)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.ja
va:56)
~[httpclient-4.5.13.jar!/:4.5.13]\n\tat

org.springframework.http.client.HttpComponentsClientHttpRequest.executeInterna
l(HttpComponentsClientHttpRequest.java:87)
~[spring-web-5.3.4.jar!/:5.3.4]\n\tat

```

```
org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInternal(AbstractBufferingClientHttpRequest.java:48)
    ~[spring-web-5.3.4.jar!/5.3.4]\n\tat

org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClientHttpRequest.java:66)
    ~[spring-web-5.3.4.jar!/5.3.4]\n\tat

org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776)
    ~[spring-
web-5.3.4.jar!/5.3.4\n"}, "extendedStackTrace": "org.apache.http.conn.HttpHostConnectException:
    Connect to localhost:5000 [localhost/127.0.0.1, localhost/
0:0:0:0:0:0:1] failed: Connection
    refused\n\tat

org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultHttpClientConnectionOperator.java:156)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHttpClientConnectionManager.java:376)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.java:393)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:186)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat
    org.apache.http.impl.execchain.RetryExec.execute(RetryExec.java:89)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.java:185)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:83)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:56)
    ~[httpclient-4.5.13.jar!/4.5.13]\n\tat

org.springframework.http.client.HttpComponentsClientHttpRequest.executeInternal(HttpComponentsClientHttpRequest.java:87)
    ~[spring-web-5.3.4.jar!/5.3.4]\n\tat

org.springframework.http.client.AbstractBufferingClientHttpRequest.executeInternal(AbstractBufferingClientHttpRequest.java:48)
```

```

ernal(AbstractBufferingClientHttpRequest.java:48)
    ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.http.client.AbstractClientHttpRequest.execute(AbstractClientHttpRequest.java:66)
    ~[spring-web-5.3.4.jar!/:5.3.4]\n\tat
org.springframework.web.client.RestTemplate.doExecute(RestTemplate.java:776)
    ~[spring-web-5.3.4.jar!/:5.3.4]\nCaused by: java.net.ConnectException:
Connection refused\n\tat sun.nio.ch.Net.pollConnect(Native Method) ~[?:?]\n\tat
sun.nio.ch.Net.pollConnectNow(Net.java:669) ~[?:?]\n\tat
sun.nio.ch.NioSocketImpl.timedFinishConnect(NioSocketImpl.java:542)
    ~[?:?]\n\tat sun.nio.ch.NioSocketImpl.connect(NioSocketImpl.java:597)
~[?:?]\n\tat java.net.SocksSocketImpl.connect(SocksSocketImpl.java:333) ~[?:?]
\n\tat java.net.Socket.connect(Socket.java:645) ~[?:?]\n\tat
org.apache.http.conn.socket.PlainConnectionSocketFactory.connectSocket(PlainConnectionSocketFactory.java:75)

```

Resolution Steps

4.3.5 CHF Connector Issues

This section describes the most common CHF connector issues and their resolution steps. It is recommended for users to attempt the resolution steps provided in this guide before contacting Oracle Support.

No CHF profile found

Symptom

CHF Connector receives an error response message saying no CHF Profile found.

Problem

When the CHF connector tries to establish communication with the CHF to process a request, but the request is rejected by CHF because the end user specified in the request cannot be served by the CHF. In the response message, it sends the following response:

```
message":"Not found matching CHF, refuse this request"
```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant": 1621844768666347628,
  "epochSecond": 1621844768,
  "nanoOfSecond": 666347628,
  "thread": "UserService_ThreadPool_7",
  "level": "WARN",
  "loggerName": "ocpm.pcf.service.ud.dbplugin.ds.chf.ChfDataSourceService",
  "message": "Not found matching CHF, refuse this request",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 103,
  "threadPriority": 5,
  "messageTimestamp": "2021-05-24T08:26:08.666+0000"
}
```

```

op:SUBSCRIBE","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":103,"threadPriority":5,"messageTimestamp":"2021-05-24T08:26:08.666+0000"}{"instant":
{"epochSecond":1621844768,"nanoOfSecond":667139735},"thread":"UserService_Thre
adPool_7","level":"WARN","loggerName":"ocpm.pcf.service.ud.intf.restful.api.Ap
iControllerHelper","message":"A
    child [GET] request failed, <500 INTERNAL_SERVER_ERROR Internal Server
    Error,
[]>","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":103,"threadPriority":5,"messageTimestamp":"2021-05-24T08:26:08.667+00
00"}{"instant":
{"epochSecond":1621844768,"nanoOfSecond":667602486},"thread":"UserService_Thre
adPool_7","level":"WARN","loggerName":"ocpm.pcf.service.ud.intf.restful.api.Ap
iControllerHelper","message":"Request
    failed 500 INTERNAL_SERVER_ERROR,
requestContext=RequestContext{userIds=[imsi-100000000002],
    requestParams='{\"spendingLimitReq\":
{\"gpsi\": \"msisdn-10000000001\", \"plmn\":
{\"mcc\": \"450\", \"mnc\": \"08\"}, \"policyCounterIds\": null, \"supportedFeatures
\": null, \"asyncQuery\": false}, \"ldapDataReq\":
{\"subscription\": false, \"params\": null}}',

requestType='GET'}.", "endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j
.Log4jLogger", "threadId":103,"threadPriority":5,"messageTimestamp":"2021-05-24
T08:26:08.667+0000"}{"instant":
{"epochSecond":1621844768,"nanoOfSecond":672460909},"thread":"XNIO-1

task-1","level":"INFO","loggerName":"ocpm.pcf.service.ud.intf.restful.api.ApiC
ontrollerHelper","message":"Send
    reply: \n<500 INTERNAL_SERVER_ERROR Internal Server Error,All sub
request
    failed.,
[]>","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger",
"threadId":65,"threadPriority":5,"messageTimestamp":"2021-05-24T08:26:08.672+000
0"}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. In the application-config yaml file, check whether CHF is added as a value to the nrfClientSubscriberTypes parameter. If it is not added, add CHF.
2. Restart nrf-management pod.
3. Initiate a request again.
4. Check the logs of chf-connector again to verify if the request has been sent successfully.

CHF Profile found, but CHF request fails

Symptom

CHF Connector receives an error response with code 503.

Problem

When the CHF connector tries to establish communication with the CHF to process a request, but the request cannot be served by the CHF despite finding the CHF profile. In the response message, it sends the following response:

```
logMsg="WARN", "loggerName": "com.oracle.cgbu.cnc.nrf.api.NRFClientApi", "message": "Error"
```

Response received with code 503

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant": {
    "epochSecond": 1627391543,
    "nanoOfSecond": 982425153
  },
  "thread": "HttpLoggingJettyHttpClient@720ce1b8-7778",
  "level": "WARN",
  "loggerName": "ocpm.pcf.service.ud.intf.restful.api.ApiControllerHelper",
  "message": "A child [GET] request failed, <503 SERVICE_UNAVAILABLE Service
Unavailable,{\"type\":null,\"title\": \"Service
Unavailable\", \"status\":503,\"detail\": \"Service
Unavailable\", \"instance\":null,\"cause\":null,\"invalidParams\":null},[]>",
  "endOfBatch": false,
  "loggerFqn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 7778,
  "threadPriority": 5,
  "messageTimestamp": "2021-07-27T13:12:23.982+0000"
}
{
  "instant": {
    "epochSecond": 1627391543,
    "nanoOfSecond": 982547688
  },
  "thread": "HttpLoggingJettyHttpClient@720ce1b8-7778",
  "level": "WARN",
  "loggerName": "ocpm.pcf.service.ud.intf.restful.api.ApiControllerHelper",
  "message": "Request failed 500 INTERNAL_SERVER_ERROR,
requestContext=RequestContext{userIds=[imsi-450081000011001],
requestParams='{\"spendingLimitReq\":
{\"gpsi\": \"msisdn-81000000002\", \"plmn\":
{\"mcc\": \"450\", \"mnc\": \"08\"}, \"policyCounterIds\": null, \"supportedFeatures
\": null, \"asyncQuery\": false}, \"ldapDataReq\":
{\"subscription\": false, \"params\": null}, \"ssvEnabled\": true}',
requestType='GET'}.",
  "endOfBatch": false,
  "loggerFqn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 7778,
  "threadPriority": 5,
  "messageTimestamp": "2021-07-27T13:12:23.982+0000"
}
{
  "instant": {
    "epochSecond": 1627391543,
    "nanoOfSecond": 982811514
```

```

    },
    "thread": "HttpLoggingJettyHttpClient@720ce1b8-7778",
    "level": "DEBUG",
    "loggerName":
"ocpm.pcf.service.ud.common.metrics.ChfDataSourceMetricsHelper",
    "message": "Pegging CHF response metric. OperationType : SUBSCRIBE,
nfInstanceId : fe7d992b-0541-4c7d-ab84-666666666666, ServiceName : nchf-
spendinglimitcontrol, ServiceVersion : v1, ServiceResource : subscriptions,
ResponseCode : 5xx",
    "endOfBatch": false,
    "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
    "threadId": 7778,
    "threadPriority": 5,
    "messageTimestamp": "2021-07-27T13:12:23.982+0000"
  }
}
{
  "instant": {
    "epochSecond": 1627391543,
    "nanoOfSecond": 984365884
  },
  "thread": "XNIO-1 task-2",
  "level": "INFO",
  "loggerName": "ocpm.pcf.service.ud.intf.restful.api.ApiControllerHelper",
  "message": "Send reply: \n<500 INTERNAL_SERVER_ERROR Internal Server
Error,All sub request failed.,[]>",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 7692,
  "threadPriority": 5,
  "messageTimestamp": "2021-07-27T13:12:23.984+0000"
}
{
  "instant": {
    "epochSecond": 1627391586,
    "nanoOfSecond": 37087769
  },
  "thread": "Thread-2",
  "level": "INFO",
  "loggerName": "ocpm.cne.common.configclient.ConfigurationAgent",
  "message": "Configuration removed from topic=NRF.UDR,
key=fe7d992b-0541-4c7d-ab84-555552222222",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 27,
  "threadPriority": 5,
  "messageTimestamp": "2021-07-27T13:13:06.037+0000"
}
}

```

Resolution Steps

To resolve this issue, perform the following steps:

1. Check whether CHF simulator is registered with NRF management. If it is not registered, register it.
2. If it is registered, verify that correct FQDN is added.
3. Initiate a request again.

4. Check the logs of chf-connector again to verify if the request has been processed successfully.

Failed or No Spending Limit data request to CHF on egress

Symptom

CHF Connector receives an error response message saying no CHF Profile found.

Problem

When the CHF connector tries to establish communication with the CHF to process a request from PCF to retrieve policy counter status information for a specific UE, but the request is rejected by CHF because the end user specified in the request cannot be served by the CHF. In the response message, it sends the following response:

```
message":"No CHF NFProfile found
```

Sample Error Logs

The following is a sample for error logs that the user may see for this issue:

```
{
  "instant": {
    "epochSecond": 1622028135, "nanoOfSecond": 231441903, "thread": "UserService_Thre
adPool_3", "level": "WARN", "loggerName": "ocpm.pcf.service.ud.dbplugin.ds.chf.Chf
DataSourceService", "message": "No CHF NFProfile
found.", "endOfBatch": false, "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
"threadId": 76, "threadPriority": 5, "messageTimestamp": "2021-05-26T11:22:15.231+
0000"}
  "instant": {
    "epochSecond": 1622028135, "nanoOfSecond": 232856398, "thread": "UserService_Thre
adPool_3", "level": "ERROR", "loggerName": "ocpm.pcf.service.ud.dbplugin.ds.chf.Ch
fDataSourceService", "message": "No CHF DataSource
found", "endOfBatch": false, "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
"threadId": 76, "threadPriority": 5, "messageTimestamp": "2021-05-26T11:22:15.232+0
000"}
  "instant": {
    "epochSecond": 1622028135, "nanoOfSecond": 233241908, "thread": "UserService_Thre
adPool_3", "level": "WARN", "loggerName": "ocpm.pcf.service.ud.dbplugin.ds.chf.Chf
DataSourceService", "message": "Not found matching CHF, refuse this
request", "endOfBatch": false, "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
"threadId": 76, "threadPriority": 5, "messageTimestamp": "2021-05-26T11:22:15.233
+0000"}
  "instant": {
    "epochSecond": 1622028135, "nanoOfSecond": 238565694, "thread": "UserService_Thre
adPool_3", "level": "ERROR", "loggerName": "ocpm.pcf.service.ud.core.SpendingLimit
Service", "message": "No Data Source found for
op:SUBSCRIBE", "endOfBatch": false, "loggerFqcn": "org.apache.logging.slf4j.Log4jL
ogger", "threadId": 76, "threadPriority": 5, "messageTimestamp": "2021-05-26T11:22:1
5.238+0000"}
  "instant": {
    "epochSecond": 1622028135, "nanoOfSecond": 239436215, "thread": "UserService_Thre
adPool_3", "level": "WARN", "loggerName": "ocpm.pcf.service.ud.intf.restful.api.Ap
iControllerHelper", "message": "A child [GET] request failed, <500
INTERNAL_SERVER_ERROR Internal Server Error,
[]>", "endOfBatch": false, "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger", "t
hreadId": 76, "threadPriority": 5, "messageTimestamp": "2021-05-26T11:22:15.239+000
0"}
  "instant": {
```

```
{
  "epochSecond":1622028135,
  "nanoOfSecond":240114557,
  "thread":"UserService_Thre
adPool_3",
  "level":"WARN",
  "loggerName":"ocpm.pcf.service.ud.intf.restful.api.Ap
iControllerHelper",
  "message":"Request failed 500 INTERNAL_SERVER_ERROR,
requestContext=RequestContext{userIds=[imsi-650081000000606],
requestParams='{\"spendingLimitReq\":
{\"gpsi\": \"msisdn-20000000606\", \"plmn\":
{\"mcc\": \"313\", \"mnc\": \"350\"}, \"policyCounterIds\": null, \"supportedFeature
s\": null, \"asyncQuery\": false}, \"ldapDataReq\":
{\"subscription\": false, \"params\": null}}',
requestType='GET'}.\",
  \"endOfBatch\": false,
  \"loggerFqcn\": \"org.apache.logging.slf4j
.Log4jLogger\",
  \"threadId\": 76,
  \"threadPriority\": 5,
  \"messageTimestamp\": \"2021-05-26T
11:22:15.240+0000\"}
}
```

Resolution Steps

To resolve this issue, perform the following steps:

1. In the application-config yaml file, check whether CHF is added as a value to the nrfClientSubscriberTypes parameter. If it is not added, add CHF.
2. Restart nrf-management pod.
3. Initiate a request again.
4. Check the logs of chf-connector again to verify if the request has been sent successfully.

5

Alerts

This section provides information on Policy alerts and their configuration.

Note

The performance and capacity of the system can vary based on the call model, configuration, including but not limited to the deployed policies and corresponding data, for example, policy tables.

5.1 Configuring Alerts

This section describes how to configure alerts in Policy. The Alert Manager uses the Prometheus measurements values as reported by microservices in conditions under alert rules to trigger alerts.

Note

- Sample alert files are packaged with Policy Custom Templates. The Policy Custom Templates.zip file can be downloaded from MOS. Unzip the folder to access the following files:
 - Common_Alertrules_cne1.5+.yaml
 - Common_Alertrules_cne1.9+.yaml
 - PCF_Alertrules_cne1.5+.yaml
 - PCF_Alertrules_cne1.9+.yaml
 - PCRF_Alertrules_cne1.5+.yaml
 - PCRF_Alertrules_cne1.9+.yaml
- Name in the metadata section should be unique while applying more than one unique files. For example:

```
apiVersion: monitoring.coreos.com/v1
kind: PrometheusRule
metadata:
  creationTimestamp: null
  labels:
    role: cnc-alerting-rules
  name: occnp-pcf-alerting-rules
```

- If required, edit the threshold values of various alerts in the alert files before configuring the alerts.
- The Alert Manager and Prometheus tools should run in CNE namespace, for example, occne-infra.
- Use the following table to select the appropriate files on the basis of deployment mode and CNE version

Table 5-1 Alert Configuration

Deployment Mode	CNE 1.5+	CNE 1.9+
Converged Mode	Common_Alertrules_cne1.5+.yaml PCF_Alertrules_cne1.5+.yaml PCRF_Alertrules_cne1.5+.yaml	Common_Alertrules_cne1.9+.yaml PCF_Alertrules_cne1.9+.yaml PCRF_Alertrules_cne1.9+.yaml
PCF only	Common_Alertrules_cne1.5+.yaml PCF_Alertrules_cne1.5+.yaml	Common_Alertrules_cne1.9+.yaml PCF_Alertrules_cne1.9+.yaml
PCRF only	Common_Alertrules_cne1.5+.yaml PCRF_Alertrules_cne1.5+.yaml	Common_Alertrules_cne1.9+.yaml PCRF_Alertrules_cne1.9+.yaml

Configuring Alerts in Prometheus for CNE version from 1.5.0 up to 1.8.x

To configure alerts in Prometheus:

1. Copy the required files to the Bastion Host. Place the files in the `/var/occne/cluster/<cluster-name>/artifacts/alerts` directory on the OCCNE Bastion Host.

```
$ pwd /var/occne/cluster/stark/artifacts/alerts
$ ls
occne_alerts.yaml
$ vi PCF_Alertrules.yaml
$ ls PCF_Alertrules.yaml occne_alerts.yaml
```

2. To set the correct file permissions, run the following command:

```
$ chmod 644 PCF_Alertrules.yaml
```

3. To load the updated rules from the Bastion host in the file to the existing `occne-prometheus-alerts` Configmap, run the following command:

```
$ kubectl create configmap occne-prometheus-alerts --from-file=/var/occne/cluster/<cluster-name>/artifacts/alerts -o yaml --dry-run -n occne-infra |
kubectl replace -f -
$ kubectl get configmap -n occne-infra
```

4. Verify the alerts in the Prometheus GUI. To do so, select the Alerts tab, and view alert details by selecting any individual rule from the list.

Configuring Alerts in Prometheus for CNE 1.9.0 and later versions

To configure PCF alerts in Prometheus for CNE 1.9.0, perform the following steps:

1. Copy the the required file to the Bastion Host.
2. To create or replace the PrometheusRule CRD, run the following command:

```
$ kubectl apply -f Common_Alertrules_cne1.9+.yaml -n <namespace>
```

```
$ kubectl apply -f PCF_Alertrules_cne1.9+.yaml -n <namespace>
```

```
$ kubectl apply -f PCRF_Alertrules_cne1.9+.yaml -n <namespace>
```

Note

This is a sample command for Converged mode of deployment.

To verify if the CRD is created, run the following command:

```
kubectl get prometheusrule -n <namespace>
```

Example:

```
kubectl get prometheusrule -n occnp
```

3. Verify the alerts in the Prometheus GUI. To do so, select the Alerts tab, and view alert details by selecting any individual rule from the list.

Validating Alerts

After configuring the alerts in Prometheus server, a user can verify using the following procedure:

- Open the Prometheus server from your browser using the <IP>:<Port>
- Navigate to Status and then Rules
- Search Policy. Policy Alerts list is displayed.

If you are unable to see the alerts, verify if the alert file is correct and then try again.

Adding worker node name in metrics

To add the worker node name in metrics, perform the following steps:

1. Edit the configmap occne-prometheus-server in namespace - occne-infra.
2. Locate the the following job:

```
job_name: kubernetes-pods
kubernetes_sd_configs:
  role: pod
```

3. Add the following in the relabel_configs:

```
action: replace
source_labels:
  __meta_kubernetes_pod_node_name
target_label: kubernetes_pod_node_name
```

5.2 Configuring SNMP Notifier

This section describes the procedure to configure SNMP Notifier.

Configure the IP and port of the SNMP trap receiver in the SNMP Notifier using the following procedure:

1. Run the following command to edit the deployment:

```
$ kubectl edit deploy <snmp_notifier_deployment_name> -n <namespace>
```

Example:

```
$ kubectl edit deploy occne-snmp-notifier -n occne-infra
```

SNMP deployment yaml file is displayed.

2. Edit the SNMP destination in the deployment yaml file as follows:

```
--snmp.destination=<destination_ip>:<destination_port>
```

Example:

```
--snmp.destination=10.75.203.94:162
```

3. Save the file.

Checking SNMP Traps

Following is an example on how to capture the logs of the trap receiver server to view the generated SNMP traps:

```
$ docker logs <trapd_container_id>
```

Sample output:

Figure 5-1 Sample output for SNMP Trap

```
- Alert: SMEgressErrorRateAbove1Percent
  Summary: Transaction Error Rate detected above 1 Percent of Total Transactions at
  Description: Egress Transaction Error Rate at detected above 1 Percent"
2020-05-07 09:22:50 10.75.152.159 [UDP: [10.75.152.159]:29755->[172.17.0.2]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (24972700) 2 days, 21:22:07.00 SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.323.5.3.34.1.2.1023
SNMPv2-SMI::enterprises.323.5.3.34.1.2.1023.1 = STRING: "1.3.6.1.4.1.323.5.3.34.1.2.1023[alertname=KIBANA_DOWN,namespace=ocne-1
nfra,severity=major]" SNMPv2-SMI::enterprises.323.5.3.34.1.2.1023.2 = STRING: "major" SNMPv2-SMI::enterprises.323.5.3.34.1.2.1023.3 = STRING:
"Status: major"
```

MIB Files for Policy

There are two MIB files which are used to generate the traps. Update these files along with the Alert file in order to fetch the traps in their environment.

- `toplevel.mib`
This is the top level mib file, where the Objects and their data types are defined.
- `policy-alarm-mib.mib`
This file fetches objects from the top level mib file and these objects can be selected for display.

Note

MIB files are packaged along with Custom Templates. Download the file from MOS. For more information on downloading custom templates, see *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

5.3 List of Alerts

This section provides detailed information about the alert rules defined for Policy. It consists of the following three types of alerts:

1. **Common Alerts** - This category of alerts is common and required for all three modes of deployment.
2. **PCF Alerts** - This category of alerts is specific to PCF microservices and required for Converged and PCF only modes of deployment.

3. PCRF Alerts - This category of alerts is specific to PCRF microservices and required for Converged and PCRF only modes of deployment.

5.3.1 Common Alerts

This section provides information about alerts that are common for PCF and PCRF.

5.3.1.1 PodMemoryDoC

Description

Pod Resource Congestion status of {{\$labels.service}} service is DoC for Memory type

Summary

Pod Resource Congestion status of {{\$labels.service}} service is DoC for Memory type

Severity

Major

Condition

ocnp_pod_resource_congestion_state{type="memory"} == 1

OID

1.3.6.1.4.1.323.5.3.52.1.2.31

Metric Used

ocnp_pod_resource_congestion_state

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

Note

Threshold levels can be configured using the PCF_Alertrules.yaml file.

The alert gets cleared when the system is back to normal state.
For any additional guidance, contact My Oracle Support.

5.3.1.2 PodMemoryCongested

Description

Pod Resource Congestion status of {{\$labels.service}} service is congested for Memory type

Summary

Pod Resource Congestion status of {{\$labels.service}} service is congested for Memory type

Severity

Critical

Condition

ocnp_pod_resource_congestion_state{type="memory"} == 2

OID

1.3.6.1.4.1.323.5.3.52.1.2.32

Metric Used

occnp_pod_resource_congestion_state

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.3 POD_DANGER_OF_CONGESTION

Description

Pod Congestion status of {{labels.service}} service is DoC

Summary

Pod Congestion status of {{labels.service}} service is DoC

Severity

Major

Condition

occnp_pod_congestion_state == 1

OID

1.3.6.1.4.1.323.5.3.52.1.2.25

Metric Used

occnp_pod_congestion_state

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.4 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Description

RAA Rx fail count exceeds the critical threshold limit.

Summary

RAA Rx fail count exceeds the critical threshold limit.

Severity

CRITICAL

Condition

sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!="2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 90

OID

1.3.6.1.4.1.323.5.3.52.1.2.35

Metric Used

occnp_diam_response_local_total

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.5 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Description

RAA Rx fail count exceeds the major threshold limit.

Summary

RAA Rx fail count exceeds the major threshold limit.

Severity

MAJOR

Condition

$$\frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"RAA"}, \text{appId}=\text{"16777236"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"RAA"}, \text{appId}=\text{"16777236"}\}[5\text{m}]))} * 100 > 80 \text{ and }$$

$$\frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}=\text{"16777236"}, \text{msgType}=\text{"RAA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}=\text{"16777236"}, \text{msgType}=\text{"RAA"}\}[5\text{m}]))} * 100 \leq 90$$
OID

1.3.6.1.4.1.323.5.3.52.1.2.35

Metric Used

occnp_diam_response_local_total

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.6 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Description

RAA Rx fail count exceeds the minor threshold limit.

Summary

RAA Rx fail count exceeds the minor threshold limit.

Severity

MINOR

Condition

$$\frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}=\text{"16777236"}, \text{msgType}=\text{"RAA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}=\text{"16777236"}, \text{msgType}=\text{"RAA"}\}[5\text{m}]))} * 100 > 60 \text{ and }$$

$$\frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}=\text{"16777236"}, \text{msgType}=\text{"RAA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}=\text{"16777236"}, \text{msgType}=\text{"RAA"}\}[5\text{m}]))} * 100 \leq 90$$

$\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="RAA"}\}[5\text{m}])) * 100$
 ≤ 80

OID

1.3.6.1.4.1.323.5.3.52.1.2.35

Metric Used

occnp_diam_response_local_total

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.7 ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Description

ASA Rx fail count exceeds the critical threshold limit.

Summary

ASA Rx fail count exceeds the critical threshold limit.

Severity

CRITICAL

Condition

$\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA", \text{responseCode} \sim "2.*"}\}[5\text{m}])) /$
 $\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA"}\}[5\text{m}])) * 100$
 > 90

OID

1.3.6.1.4.1.323.5.3.52.1.2.66

Metric Used

occnp_diam_response_local_total

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.8 ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Description

ASA Rx fail count exceeds the major threshold limit.

Summary

ASA Rx fail count exceeds the major threshold limit.

Severity

MAJOR

Condition

$\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA", \text{responseCode} \sim "2.*"}\}[5\text{m}])) /$
 $\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA"}\}[5\text{m}])) * 100$
 > 80 and
 $\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA", \text{responseCode} \sim "2.*"}\}[5\text{m}])) /$

$\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA"}[5\text{m}])) * 100 \leq 90$

OID

1.3.6.1.4.1.323.5.3.52.1.2.66

Metric Used

occnp_diam_response_local_total

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.9 ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Description

ASA Rx fail count exceeds the minor threshold limit.

Summary

ASA Rx fail count exceeds the minor threshold limit.

Severity

MINOR

Condition

$\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA", \text{responseCode}!\sim"2.*"}[5\text{m}])) /$
 $\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA"}[5\text{m}])) * 100 > 60$ and
 $\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA", \text{responseCode}!\sim"2.*"}[5\text{m}])) /$
 $\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{appId}="16777236", \text{msgType}="ASA"}[5\text{m}])) * 100 \leq 80$

OID

1.3.6.1.4.1.323.5.3.52.1.2.66

Metric Used

occnp_diam_response_local_total

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.10 SCP_PEER_UNAVAILABLE

Description

Configured SCP peer is unavailable.

Summary

occnp_oc_egressgateway_peer_health_status != 0. SCP peer [{{ \$labels.peer }}] is unavailable.

Severity

Major

Condition

OID

1.3.6.1.4.1.323.5.3.52.1.2.60

Metric Used

occnp_oc_egressgateway_peer_health_status

Recommended Actions

This alert gets cleared when unavailable SCPs become available.
For any additional guidance, contact My Oracle Support.

5.3.1.11 SCP_PEER_SET_UNAVAILABLE

Description

None of the SCP peer available for configured peerset.

Summary

(occnp_oc_egressgateway_peer_count - occnp_oc_egressgateway_peer_available_count) != 0 and (occnp_oc_egressgateway_peer_count) > 0.

Severity

Critical

Condition

One of the SCPs has been marked unhealthy.

OID

1.3.6.1.4.1.323.5.3.52.1.2.61

Metric Used

oc_egressgateway_peer_count and oc_egressgateway_peer_available_count

Recommended Actions

NF clears the critical alarm when atleast one SCP peer in a peerset becomes available such that all other SCP peers in the given peerset are still unavailable.
For any additional guidance, contact My Oracle Support.

5.3.1.12 STALE_CONFIGURATION

Description

In last 10 minutes, the current service config_level does not match the config_level from the config-server.

Summary

In last 10 minutes, the current service config_level does not match the config_level from the config-server.

Severity

Major

Condition

```
(sum by(namespace) (topic_version{app_kubernetes_io_name="config-server",topicName="config.level"})) / (count by(namespace) (topic_version{app_kubernetes_io_name="config-server",topicName="config.level"})) != (sum by(namespace) (topic_version{app_kubernetes_io_name!="config-server",topicName="config.level"})) / (count by(namespace) (topic_version{app_kubernetes_io_name!="config-server",topicName="config.level"}))
```

OID

1.3.6.1.4.1.323.5.3.52.1.2.62

Metric Used

topic_version

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.13 POLICY_SERVICES_DOWN

Name in Alert Yaml File

PCF_SERVICES_DOWN

Description

{{labels.service}} service is not running!

Summary

{{labels.service}} is not running!

Severity

Critical

Condition

sum by(service, namespace, category)(appinfo_service_running{application="occnp",service!~".*altsvc-cache",vendor="Oracle"}) < 1

OID

1.3.6.1.4.1.323.5.3.36.1.2.1

Metric Used

appinfo_service_running

Recommended Actions

Alert gets triggered if PCF service is down.

For any additional guidance, contact My Oracle Support.

5.3.1.14 DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD

Name in Alert Yaml File

DiamTrafficRateAboveThreshold

Description

Diameter Connector Ingress traffic Rate is above threshold of Max MPS (current value is: {{ \$value }})

Summary

Traffic Rate is above 90 Percent of Max requests per second.

Severity

Major

Condition

The total Ingress traffic rate for Diameter connector has crossed the configured threshold of 900 TPS.

Default value of this alert trigger point in `Common_Alertrules.yaml` file is when Diameter Connector Ingress Rate crosses 90% of maximum ingress requests per second.

OID

1.3.6.1.4.1.323.5.3.36.1.2.6

Metric Used

ocpm_ingress_request_total

Recommended Actions

The alert gets cleared when the Ingress traffic rate falls below the threshold.

Note

Threshold levels can be configured using the `Common_Alertrules.yaml` file.

It is recommended to assess the reason for additional traffic. Perform the following steps to analyze the cause of increased traffic:

1. Refer **Ingress Gateway** section in Grafana to determine increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any additional guidance, contact My Oracle Support.

5.3.1.15 DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Name in Alert Yaml File

DiamIngressErrorRateAbove10Percent

Description

Transaction Error Rate detected above 10 Percent of Total on Diameter Connector (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 10 Percent of Total Transactions.

Severity

Critical

Condition

The number of failed transactions is above 10 percent of the total transactions on Diameter Connector.

OID

1.3.6.1.4.1.323.5.3.36.1.2.7

Metric Used

ocpm_ingress_response_total

Recommended Actions

The alert gets cleared when the number of failed transactions are below 10% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors. For instance:
`ocpm_ingress_response_total{servicename_3gpp="rx", response_code!="2.*"}`
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.1.16 DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Name in Alert Yaml File

DiamEgressErrorRateAbove1Percent

Description

Egress Transaction Error Rate detected above 1 Percent of Total on Diameter Connector (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 1 Percent of Total Transactions

Severity

Minor

Condition

The number of failed transactions is above 1 percent of the total Egress Gateway transactions on Diameter Connector.

OID

1.3.6.1.4.1.323.5.3.36.1.2.8

Metric Used

ocpm_egress_response_total

Recommended Actions

The alert gets cleared when the number of failed transactions are below 1% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the errors. For instance:
`ocpm_egress_response_total{servicename_3gpp="rx", response_code!="2.*"}`
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.1.17 UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Name in Alert Yaml File

PcfUdrIngressTrafficRateAboveThreshold

Description

User service Ingress traffic Rate from UDR is above threshold of Max MPS (current value is: {{ \$value }})

Summary

Traffic Rate is above 90 Percent of Max requests per second

Severity

Major

Condition

The total User Service Ingress traffic rate from UDR has crossed the configured threshold of 900 TPS.

Default value of this alert trigger point in `Common_Alertrules.yaml` file is when user service Ingress Rate from UDR crosses 90% of maximum ingress requests per second.

OID

1.3.6.1.4.1.323.5.3.36.1.2.9

Metric Used`ocpm_userservice_inbound_count_total{service_resource="udr-service"}`**Recommended Actions**

The alert gets cleared when the Ingress traffic rate falls below the threshold.

 Note

Threshold levels can be configured using the `Common_Alertrules.yaml` file.

It is recommended to assess the reason for additional traffic. Perform the following steps to analyze the cause of increased traffic:

1. Refer **Ingress Gateway** section in Grafana to determine increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any additional guidance, contact My Oracle Support.

5.3.1.18 UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Name in Alert Yaml File`PcfUdrEgressErrorRateAbove10Percent`**Description**

Egress Transaction Error Rate detected above 10 Percent of Total on User service (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 10 Percent of Total Transactions

Severity

Critical

Condition

The number of failed transactions from UDR is more than 10 percent of the total transactions.

OID

1.3.6.1.4.1.323.5.3.36.1.2.10

Metric Used`ocpm_udr_tracking_response_total{servicename_3gpp="nudr-dr",response_code!="2.*"}`

Recommended Actions

The alert gets cleared when the number of failure transactions falls below the configured threshold.

Note

Threshold levels can be configured using the `Common_Alertrules.yaml` file.

It is recommended to assess the reason for failed transactions. Perform the following steps to analyze the cause of increased traffic:

1. Refer **Egress Gateway** section in Grafana to determine increase in 4xx and 5xx error response codes.
2. Check **Egress Gateway** logs on Kibana to determine the reason for the errors.

For any additional guidance, contact My Oracle Support.

5.3.1.19 POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Name in Alert Yaml File

PolicyDsIngressTrafficRateAboveThreshold

Description

Ingress Traffic Rate is above threshold of Max MPS (current value is: {{ \$value }})

Summary

Traffic Rate is above 90 Percent of Max requests per second

Severity

Critical

Condition

The total PolicyDS Ingress message rate has crossed the configured threshold of 900 TPS. 90% of maximum Ingress request rate.
Default value of this alert trigger point in `Common_Alertrules.yaml` file is when PolicyDS Ingress Rate crosses 90% of maximum ingress requests per second.

OID

1.3.6.1.4.1.323.5.3.36.1.2.13

Metric Used

client_request_total

Note

This is a Kubernetes metric used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Recommended Actions

The alert gets cleared when the Ingress traffic rate falls below the threshold.

Note

Threshold levels can be configured using the `Common_Alertrules.yaml` file.

It is recommended to assess the reason for additional traffic. Perform the following steps to analyze the cause of increased traffic:

1. Refer **Ingress Gateway** section in Grafana to determine increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any additional guidance, contact My Oracle Support.

5.3.1.20 POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Name in Alert Yaml File

PolicyDsIngressErrorRateAbove10Percent

Description

Ingress Transaction Error Rate detected above 10 Percent of Total on PolicyDS service (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 10 Percent of Total Transactions

Severity

Critical

Condition

The number of failed transactions is above 10 percent of the total transactions for PolicyDS service.

OID

1.3.6.1.4.1.323.5.3.36.1.2.14

Metric Used

client_response_total

Recommended Actions

The alert gets cleared when the number of failed transactions are below 10% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors. For instance: `client_response_total{response!="2.*"}`
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.1.21 POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Name in Alert Yaml File

PolicyDsEgressErrorRateAbove1Percent

Description

Egress Transaction Error Rate detected above 1 Percent of Total on PolicyDS service (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 1 Percent of Total Transactions

Severity

Minor

Condition

The number of failed transactions is above 1 percent of the total transactions for PolicyDS service.

OID

1.3.6.1.4.1.323.5.3.36.1.2.15

Metric Used

server_response_total

Recommended Actions

The alert gets cleared when the number of failed transactions are below 10% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors. For instance:
server_response_total{response!~"2.*"}
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.1.22 UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Name in Alert Yaml File

PcfUdrIngressTimeoutErrorAboveMajorThreshold

Description

Ingress Timeout Error Rate detected above 10 Percent of Total towards UDR service (current value is: {{ \$value }})

Summary

Timeout Error Rate detected above 10 Percent of Total Transactions

Severity

Major

Condition

The number of failed transactions due to timeout is above 10 percent of the total transactions for UDR service.

OID

1.3.6.1.4.1.323.5.3.36.1.2.16

Metric Used

ocpm_udr_tracking_request_timeout_total{servicename_3gpp="nudur-dr"}

Recommended Actions

The alert gets cleared when the number of failed transactions due to timeout are below 10% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors. For instance:
`ocpm_udr_tracking_request_timeout_total{servicename_3gpp="nldr-dr"}`
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.1.23 DB_TIER_DOWN_ALERT

Name in Alert Yaml File

DBTierDownAlert

Description

DB cannot be reachable!

Summary

DB cannot be reachable!

Severity

Critical

Condition

Database is not available.

OID

1.3.6.1.4.1.323.5.3.36.1.2.18

Metric Used

`appinfo_category_running{category="database"}`

Recommended Actions

Alert gets triggered when database is not reachable.

For any additional guidance, contact My Oracle Support.

5.3.1.24 CPU_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Name in Alert Yaml File

CPUUsagePerServiceAboveMinorThreshold

Description

CPU usage for `{{ $labels.service }}` service is above 60

Summary

CPU usage for `{{ $labels.service }}` service is above 60

Severity

Minor

Condition

A service pod has reached the configured minor threshold (60%) of its CPU usage limits.

OID

1.3.6.1.4.1.323.5.3.36.1.2.19

Metric Used

container_cpu_usage_seconds_total

Note

This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. If the CPU utilization crosses the minor threshold then the alert shall be raised. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

Note

Threshold levels can be configured using the `PCF_Alert rules.yaml` file.

The alert gets cleared when the CPU utilization falls below the minor threshold or crosses the major threshold or when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.25 CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Name in Alert Yaml File

CPUUsagePerServiceAboveMajorThreshold

Description

CPU usage for {{labels.service}} service is above 80

Summary

CPU usage for {{labels.service}} service is above 80

Severity

Major

Condition

A service pod has reached the configured major threshold (80%) of its CPU usage limits.

OID

1.3.6.1.4.1.323.5.3.36.1.2.20

Metric Used

container_cpu_usage_seconds_total

Note

This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. If the CPU utilization crosses the major threshold then the alert shall be raised. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

Note

Threshold levels can be configured using the `PCF_Alertrules.yaml` file.

The alert gets cleared when the CPU utilization falls below the minor threshold or crosses the major threshold or when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.26 CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Name in Alert Yaml File

CPUUsagePerServiceAboveCriticalThreshold

Description

CPU usage for `{{labels.service}}` service is above 90

Summary

CPU usage for `{{labels.service}}` service is above 90

Severity

Critical

Condition

A service pod has reached the configured critical threshold (90%) of its CPU usage limits.

OID

1.3.6.1.4.1.323.5.3.36.1.2.21

Metric Used

`container_cpu_usage_seconds_total`

Note

This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. If the CPU utilization crosses the critical threshold then the alert shall be raised. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

Note

Threshold levels can be configured using the `PCF_Alertrules.yaml` file.

The alert gets cleared when the CPU utilization falls below the critical threshold or when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.27 MemoryUsagePerServiceAboveMinorThreshold

Table 5-2 MemoryUsagePerServiceAboveMinorThreshold

Field	Details
Description	Memory usage for <code>{{labels.service}}</code> service is above 60
Summary	Memory usage for <code>{{labels.service}}</code> service is above 60
Severity	Minor
Condition	A service pod has reached the configured minor threshold (60%) of its memory usage limits.
OID	1.3.6.1.4.1.323.5.3.36.1.2.22
Metric Used	container_memory_usage_bytes Note: This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.
Recommended Actions	The alert gets cleared when the memory utilization falls below the minor threshold or crosses the critical threshold, in which case MemoryUsagePerServiceAboveMajorThreshold alert shall be raised. Note: Threshold levels can be configured using the <code>PCF_Alertrules.yaml</code> file. For any additional guidance, contact My Oracle Support.

5.3.1.28 MEMORY_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Name in Alert Yaml File

MemoryUsagePerServiceAboveMajorThreshold

Description

Memory usage for `{{labels.service}}` service is above 80

Summary

Memory usage for `{{labels.service}}` service is above 80

Severity

Major

Condition

A service pod has reached the configured major threshold (80%) of its memory usage limits.

OID

1.3.6.1.4.1.323.5.3.36.1.2.23

Metric Used

container_memory_usage_bytes

Note

This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. If the memory utilization crosses the major threshold then the alert shall be raised. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

Note

Threshold levels can be configured using the `PCF_Alertrules.yaml` file.

The alert gets cleared when the memory utilization falls below the minor threshold or crosses the major threshold or when the system is back to normal state.
For any additional guidance, contact My Oracle Support.

5.3.1.29 MEMORY_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Name in Alert Yaml File

MemoryUsagePerServiceAboveCriticalThreshold

Description

Memory usage for {{ \$labels.service }} service is above 90

Summary

Memory usage for {{ \$labels.service }} service is above 90

Severity

Critical

Condition

A service pod has reached the configured critical threshold (90%) of its memory usage limits.

OID

1.3.6.1.4.1.323.5.3.36.1.2.24

Metric Used

container_memory_usage_bytes

Note

This is a Kubernetes used for instance availability monitoring. If the metric is not available, use similar metrics exposed by the monitoring system.

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. If the CPU utilization crosses the critical threshold then the alert shall be raised. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

Note

Threshold levels can be configured using the `PCF_Alertrules.yaml` file.

The alert gets cleared when the memory utilization falls below the critical threshold or when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.30 POD_CONGESTED

Name in Alert Yaml File

PodCongested

Description

Pod Congestion status of `{{labels.service}}` service is congested

Summary

Pod Congestion status of `{{labels.service}}` service is congested

Severity

Critical

Condition

The pod congestion status is set to congested.

OID

1.3.6.1.4.1.323.5.3.36.1.2.26

Metric Used

occpn_pod_congestion_state

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.31 POD_DANGER_OF_CONGESTION

Name in Alert Yaml File

PodDoC

Description

Pod Congestion status of `{{labels.service}}` service is DoC

Summary

Pod Congestion status of `{{labels.service}}` service is DoC

Severity

Major

Condition

The pod congestion status is set to Danger of Congestion.

OID

1.3.6.1.4.1.323.5.3.36.1.2.25

Metric Used

occnp_pod_congestion_state

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.32 POD_PENDING_REQUEST_CONGESTED

Name in Alert Yaml File

PodPendingRequestCongested

Description

Pod Resource Congestion status of {{\$labels.service}} service is congested for PendingRequest type

Summary

Pod Resource Congestion status of {{\$labels.service}} service is congested for PendingRequest type

Severity

Critical

Condition

The pod congestion status is set to congested for PendingRequest.

OID

1.3.6.1.4.1.323.5.3.36.1.2.28

Metric Used

occnp_pod_resource_congestion_state{type="queue"}

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the pending requests in the queue comes below the configured threshold value.

For any additional guidance, contact My Oracle Support.

5.3.1.33 POD_PENDING_REQUEST_DANGER_OF_CONGESTION

Name in Alert Yaml File

PodPendingRequestDoC

Description

Pod Resource Congestion status of {{\$labels.service}} service is DoC for PendingRequest type

Summary

Pod Resource Congestion status of {{\$labels.service}} service is DoC for PendingRequest type

Severity

Major

Condition

The pod congestion status is set to DoC for pending requests.

OID

1.3.6.1.4.1.323.5.3.36.1.2.27

Metric Used

occnp_pod_resource_congestion_state{type="queue"}

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the pending requests in the queue comes below the configured threshold value.

For any additional guidance, contact My Oracle Support.

5.3.1.34 POD_CPU_CONGESTED

Name in Alert Yaml File

PodCPUCongested

Description

Pod Resource Congestion status of {{\$labels.service}} service is congested for CPU type

Summary

Pod Resource Congestion status of {{\$labels.service}} service is congested for CPU type

Severity

Critical

Condition

The pod congestion status is set to congested for CPU.

OID

1.3.6.1.4.1.323.5.3.36.1.2.30

Metric Used

occnp_pod_resource_congestion_state{type="cpu"}

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the system CPU usage comes below the configured threshold value.

For any additional guidance, contact My Oracle Support.

5.3.1.35 POD_CPU_DANGER_OF_CONGESTION

Name in Alert Yaml File

PodCPUDoC

Description

Pod Resource Congestion status of {{\$labels.service}} service is DoC for CPU type

Summary

Pod Resource Congestion status of {{\$labels.service}} service is DoC for CPU type

Severity

Major

Condition

The pod congestion status is set to DoC for CPU.

OID

1.3.6.1.4.1.323.5.3.36.1.2.29

Metric Used

ocnp_pod_resource_congestion_state{type="cpu"}

Recommended Actions

Alert triggers based on the resource limit usage and load shedding configurations in congestion control. The CPU, Memory, and Queue usage can be referred using the Grafana Dashboard.

The alert gets cleared when the system CPU usage comes below the configured threshold value.

For any additional guidance, contact My Oracle Support.

5.3.1.36 SERVICE_OVERLOADED

Description

Overload Level of {{\$labels.service}} service is L1

Summary

Overload Level of {{\$labels.service}} service is L1

Severity

Minor

Condition

The overload level of the service is L1.

OID

1.3.6.1.4.1.323.5.3.36.1.2.40

Metric Used

load_level

Recommended Actions

The alert gets cleared when the system is back to normal state.

For any additional guidance, contact My Oracle Support.

Description

Overload Level of {{labels.service}} service is L2

Summary

Overload Level of {{labels.service}} service is L2

Severity

Major

Condition

The overload level of the service is L2.

OID

1.3.6.1.4.1.323.5.3.36.1.2.40

Metric Used

load_level

Recommended Actions

The alert gets cleared when the system is back to normal state.
For any additional guidance, contact My Oracle Support.

Description

Overload Level of {{labels.service}} service is L3

Summary

Overload Level of {{labels.service}} service is L3

Severity

Critical

Condition

The overload level of the service is L3.

OID

1.3.6.1.4.1.323.5.3.36.1.2.40

Metric Used

load_level

Recommended Actions

The alert gets cleared when the system is back to normal state.
For any additional guidance, contact My Oracle Support.

5.3.1.37 SERVICE_RESOURCE_OVERLOADED

Alerts when service is in overload state due to memory usage**Description**

{{labels.service}} service is L1 for {{labels.type}} type

Summary

{{labels.service}} service is L1 for {{labels.type}} type

Severity

Minor

Condition

The overload level of the service is L1 due to memory usage.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="memory"}

Recommended Actions

The alert gets cleared when the memory usage of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Description

{{ \$labels.service }} service is L2 for {{ \$labels.type }} type

Summary

{{ \$labels.service }} service is L2 for {{ \$labels.type }} type

Severity

Major

Condition

The overload level of the service is L2 due to memory usage.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="memory"}

Recommended Actions

The alert gets cleared when the memory usage of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Description

{{ \$labels.service }} service is L3 for {{ \$labels.type }} type

Summary

{{ \$labels.service }} service is L3 for {{ \$labels.type }} type

Severity

Critical

Condition

The overload level of the service is L3 due to memory usage.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="memory"}

Recommended Actions

The alert gets cleared when the memory usage of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Alerts when service is in overload state due to CPU usage**Description**

{{labels.service}} service is L1 for {{labels.type}} type

Summary

{{labels.service}} service is L1 for {{labels.type}} type

Severity

Minor

Condition

The overload level of the service is L1 due to CPU usage.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="cpu"}

Recommended Actions

The alert gets cleared when the CPU usage of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Description

{{labels.service}} service is L2 for {{labels.type}} type

Summary

{{labels.service}} service is L2 for {{labels.type}} type

Severity

Major

Condition

The overload level of the service is L2 due to CPU usage.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="cpu"}

Recommended Actions

The alert gets cleared when the CPU usage of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Description

{{labels.service}} service is L3 for {{labels.type}} type

Summary

{{labels.service}} service is L3 for {{labels.type}} type

Severity

Critical

Condition

The overload level of the service is L3 due to CPU usage.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="cpu"}

Recommended Actions

The alert gets cleared when the CPU usage of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Alerts when service is in overload state due to number of pending messages**Description**

{{\$labels.service}} service is L1 for {{\$labels.type}} type

Summary

{{\$labels.service}} service is L1 for {{\$labels.type}} type

Severity

Minor

Condition

The overload level of the service is L1 due to number of pending messages.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="svc_pending_count"}

Recommended Actions

The alert gets cleared when the number of pending messages of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Description

{{\$labels.service}} service is L2 for {{\$labels.type}} type

Summary

{{\$labels.service}} service is L2 for {{\$labels.type}} type

Severity

Major

Condition

The overload level of the service is L2 due to number of pending messages.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="svc_pending_count"}

Recommended Actions

The alert gets cleared when the number of pending messages of the service is back to normal state.
For any additional guidance, contact My Oracle Support.

Description

{{labels.service}} service is L3 for {{labels.type}} type

Summary

{{labels.service}} service is L3 for {{labels.type}} type

Severity

Critical

Condition

The overload level of the service is L3 due to number of pending messages.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="svc_pending_count"}

Recommended Actions

The alert gets cleared when the number of pending messages of the service is back to normal state.

For any additional guidance, contact My Oracle Support.

Alerts when service is in overload state due to number of failed requests**Description**

{{labels.service}} service is L1 for {{labels.type}} type

Summary

{{labels.service}} service is L1 for {{labels.type}} type

Severity

Minor

Condition

The overload level of the service is L1 due to number of failed requests.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="svc_failure_count"}

Recommended Actions

The alert gets cleared when the number of failed messages of the service is back to normal state.

For any additional guidance, contact My Oracle Support.

Description

{{labels.service}} service is L2 for {{labels.type}} type

Summary

{{labels.service}} service is L2 for {{labels.type}} type

Severity

Major

Condition

The overload level of the service is L2 due to number of failed requests.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="svc_failure_count"}

Recommended Actions

The alert gets cleared when the number of failed messages of the service is back to normal state.

For any additional guidance, contact My Oracle Support.

Description

{{ \$labels.service }} service is L3 for {{ \$labels.type }} type

Summary

{{ \$labels.service }} service is L3 for {{ \$labels.type }} type

Severity

Critical

Condition

The overload level of the service is L3 due to number of failed requests.

OID

1.3.6.1.4.1.323.5.3.36.1.2.41

Metric Used

service_resource_overload_level{type="svc_failure_count"}

Recommended Actions

The alert gets cleared when the number of failed messages of the service is back to normal state.

For any additional guidance, contact My Oracle Support.

5.3.1.38

SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD

Description

Notification Transaction Error exceeds the critical threshold limit for a given Subscriber Notification server

Summary

Transaction Error exceeds the critical threshold limit for a given Subscriber Notification server

Severity

Critical

Condition

The number of error responses for a given subscriber notification server exceeds the critical threshold of 1000.

OID

1.3.6.1.4.1.323.5.3.36.1.2.42

Metric Used

http_notification_response_total{responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Description

Notification Transaction Error exceeds the major threshold limit for a given Subscriber Notification server

Summary

Transaction Error exceeds the major threshold limit for a given Subscriber Notification server

Severity

Major

Condition

The number of error responses for a given subscriber notification server exceeds the major threshold value, that is, between 750 and 1000.

OID

1.3.6.1.4.1.323.5.3.36.1.2.42

Metric Used

http_notification_response_total{responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Description

Notification Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server

Summary

Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server

Severity

Minor

Condition

The number of error responses for a given subscriber notification server exceeds the minor threshold value, that is, between 500 and 750.

OID

1.3.6.1.4.1.323.5.3.36.1.2.42

Metric Used

http_notification_response_total{responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.39 SYSTEM_IMPAIRMENT_MAJOR

Description

Major Impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage

Summary

Major Impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage

Severity

Major

Condition

Major Impairment alert

OID

1.3.6.1.4.1.323.5.3.36.1.2.43

Metric Used

db_tier_replication_status

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.40 SYSTEM_IMPAIRMENT_CRITICAL

Description

Critical Impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage

Summary

Critical Impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage

Severity

Critical

Condition

Critical Impairment alert

OID

1.3.6.1.4.1.323.5.3.36.1.2.43

Metric Used

db_tier_replication_status

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.41 SYSTEM_OPERATIONAL_STATE_NORMAL

Description

System Operational State is now in normal state

Summary

System Operational State is now in normal state

Severity

Info

Condition

System Operational State is now in normal state

OID

1.3.6.1.4.1.323.5.3.36.1.2.44

Metric Used

system_operational_state == 1

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.42 SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN

Description

System Operational State is now in partial shutdown state

Summary

System Operational State is now in partial shutdown state

Severity

Info

Condition

System Operational State is now in partial shutdown state

OID

1.3.6.1.4.1.323.5.3.36.1.2.44

Metric Used

system_operational_state == 2

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.43 SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN

Description

System Operational State is now in complete shutdown state

Summary

System Operational State is now in complete shutdown state

Severity

Info

Condition

System Operational State is now in complete shutdown state

OID

1.3.6.1.4.1.323.5.3.36.1.2.44

Metric Used

system_operational_state == 3

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.44 TDF_CONNECTION_DOWN

Summary

TDF connection is down.

Description

TDF connection is down.

Severity

Critical

Condition

occnp_diam_conn_app_network{applicationName="Sd"} == 0

OID

1.3.6.1.4.1.323.5.3.52.1.2.48

Metric Used

occnp_diam_conn_app_network

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.45 DIAM_CONN_PEER_DOWN

Summary

Diameter connection to peer is down.

Description

Diameter connection to peer is down.

Severity

Major

Condition

(sum by (kubernetes_namespace,origHost)(occnp_diam_conn_network) == 0) and (sum by (kubernetes_namespace,origHost)(max_over_time(occnp_diam_conn_network[24h])) != 0)

OID

1.3.6.1.4.1.323.5.3.52.1.2.50

Metric Used

occnp_diam_conn_network

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.46 DIAM_CONN_NETWORK_DOWN

Summary

All the diameter network connections are down.

Description

All the diameter network connections are down.

Severity

Critical

Condition

sum by (kubernetes_namespace)(occnp_diam_conn_network) == 0

OID

1.3.6.1.4.1.323.5.3.52.1.2.51

Metric Used

occnp_diam_conn_network

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.47 DIAM_CONN_BACKEND_DOWN

Summary

All the diameter backend connections are down.

Description

All the diameter backend connections are down.

Severity

Critical

Condition

sum by (kubernetes_namespace)(occnp_diam_conn_backend) == 0

OID

1.3.6.1.4.1.323.5.3.52.1.2.52

Metric Used

occnp_diam_conn_network

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.48 PerfInfoActiveOverloadThresholdFetchFailed

Summary

The application fails to get the current active overload level threshold data.

DescriptionThe application raises this alert when it fails to fetch the current active overload level threshold data and `active_overload_threshold_fetch_failed == 1`.**Severity**

Major

Condition

active_overload_threshold_fetch_failed == 1

OID

1.3.6.1.4.1.323.5.3.52.1.2.53

Metric Used

active_overload_threshold_fetch_failed

Recommended Actions

The alert gets cleared when the application fetches the current active overload level threshold data.

For any additional guidance, contact My Oracle Support.

5.3.1.49 SLASYFailCountExceedsCriticalThreshold

Summary

SLA Sy fail count exceeds the critical threshold limit

Description

SLA Sy fail count exceeds the critical threshold limit

Severity

Critical

Condition

$\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}])) / \text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}\}[5\text{m}])) * 100 > 90$

OID

1.3.6.1.4.1.323.5.3.52.1.2.58

Metric Used

ocnp_diam_response_local_total

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present. If the user hasn't been added in the OCS configuration, then configure the user(s).

For any additional guidance, contact My Oracle Support.

5.3.1.50 SLASYFailCountExceedsMajorThreshold

Summary

SLA Sy fail count exceeds the major threshold limit

Description

SLA Sy fail count exceeds the major threshold limit

Severity

Critical

Condition

$\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}])) / \text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}\}[5\text{m}])) * 100 > 80$ and $\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}])) / \text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}\}[5\text{m}])) * 100 \leq 90$

OID

1.3.6.1.4.1.323.5.3.52.1.2.58

Metric Used

ocnp_diam_response_local_total

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present. If the user hasn't been added in the OCS configuration, then configure the user(s). For any additional guidance, contact My Oracle Support.

5.3.1.51 SLASYFailCountExceedsMinorThreshold

Summary

SLA Sy fail count exceeds the minor threshold limit

Description

SLA Sy fail count exceeds the minor threshold limit

Severity

Minor

Condition

$\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}])) / \text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}\}[5\text{m}])) * 100 > 60$ and $\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}])) / \text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"SLA"}\}[5\text{m}])) * 100 \leq 80$

OID

1.3.6.1.4.1.323.5.3.52.1.2.58

Metric Used

ocnp_diam_response_local_total

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present. If the user hasn't been added in the OCS configuration, then configure the user(s). For any additional guidance, contact My Oracle Support.

5.3.1.52 STASYFailCountExceedsCriticalThreshold

Summary

STA Sy fail count exceeds the critical threshold limit

Description

STA Sy fail count exceeds the critical threshold limit

Severity

Critical

Condition

$\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}])) / \text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}\}[5\text{m}])) * 100 > 90$

OID

1.3.6.1.4.1.323.5.3.52.1.2.59

Metric Used

ocnp_diam_response_local_total

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present. If the user hasn't been added in the OCS configuration, then configure the user(s). For any additional guidance, contact My Oracle Support.

5.3.1.53 STASYFailCountExceedsMajorThreshold**Summary**

STA Sy fail count exceeds the major threshold limit.

Description

STA Sy fail count exceeds the major threshold limit.

Severity

major

Condition

$$\frac{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}\}[5\text{m}]))} * 100 > 80 \text{ and } \frac{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}\}[5\text{m}]))} * 100 \leq 90$$
OID

1.3.6.1.4.1.323.5.3.52.1.2.59

Metric Used

ocnp_diam_response_local_total

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present. If the user hasn't been added in the OCS configuration, then configure the user(s). For any additional guidance, contact My Oracle Support.

5.3.1.54 STASYFailCountExceedsMinorThreshold**Summary**

STA Sy fail count exceeds the minor threshold limit

Description

STA Sy fail count exceeds the minor threshold limit

Severity

minor

Condition

$$\frac{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}\}[5\text{m}]))} * 100 > 60 \text{ and } \frac{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{ocnp_diam_response_local_total}\{\text{msgType}=\text{"STA"}\}[5\text{m}]))} * 100 \leq 80$$
OID

1.3.6.1.4.1.323.5.3.52.1.2.59

Metric Used

ocnp_diam_response_local_total

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present. If the user hasn't been added in the OCS configuration, then configure the user(s). For any additional guidance, contact My Oracle Support.

5.3.1.55 SMSC_CONNECTION_DOWN

Description

This alert is triggered when connection to SMSC host is down.

Summary

Connection to SMSC peer {{\$labels.smscName}} is down in notifier service pod {{\$labels.pod}}

Severity

Major

Condition

sum by(namespace, pod, smscName)(ocnp_active_smsc_conn_count) == 0

OID

1.3.6.1.4.1.323.5.3.52.1.2.63

Metric Used

ocnp_active_smsc_conn_count

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.1.56 STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Summary

STA Rx fail count exceeds the critical threshold limit.

Description

STA Rx fail count exceeds the critical threshold limit.

Severity

Critical

Condition

The failure rate of Rx STA responses is more than 90% of the total responses.

Expression

sum(rate(ocnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(ocnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 > 90

OID

1.3.6.1.4.1.323.5.3.52.1.2.64

Metric Used

ocnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present.

Check that the session and user hasn't been removed in the OCS configuration, then configure the user(s).

For any additional guidance, contact My Oracle Support.

5.3.1.57 STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD**Summary**

STA Rx fail count exceeds the major threshold limit

Description

STA Rx fail count exceeds the major threshold limit

Severity

Major

Condition

The failure rate of Rx STA responses is more than 80% and less and or equal to 90% of the total responses.

Expression

```
sum(rate(ocnp_diam_response_local_total{msgType="STA", appId="16777236",
responseCode!~"2.*"}[5m])) / sum(rate(ocnp_diam_response_local_total{msgType="STA",
appId="16777236"}[5m])) * 100 > 80 and
sum(rate(ocnp_diam_response_local_total{msgType="STA", appId="16777236",
responseCode!~"2.*"}[5m])) / sum(rate(ocnp_diam_response_local_total{msgType="STA",
appId="16777236"}[5m])) * 100 <= 90
```

OID

1.3.6.1.4.1.323.5.3.52.1.2.64

Metric Used

ocnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}

Recommended Actions

Check the connectivity between diam-gw pod(s) & AF and ensure connectivity is present.

Check that the session and user is valid and hasn't been removed in the Policy database, then configure the user(s).

For any additional guidance, contact My Oracle Support.

5.3.1.58 STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD**Summary**

STA Rx fail count exceeds the minor threshold limit

Description

STA Rx fail count exceeds the minor threshold limit

Severity

Minor

Condition

The failure rate of Rx STA responses is more than 60% and less and or equal to 80% of the total responses.

Expression

```
sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236",
responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA",
appId="16777236"}[5m])) * 100 > 60 and
sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236",
responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA",
appId="16777236"}[5m])) * 100 <= 80
```

OID

1.3.6.1.4.1.323.5.3.52.1.2.64

Metric Used

occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}

Recommended Actions

Check the connectivity between diam-gw pod(s) & AF and ensure connectivity is present.
Check that the session and user is valid and hasn't been removed in the Policy database, then configure the user(s).
For any additional guidance, contact My Oracle Support.

5.3.1.59 SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Summary

SNA Sy fail count exceeds the critical threshold limit

Description

SNA Sy fail count exceeds the critical threshold limit

Severity

Critical

Condition

The failure rate of Sy SNA responses is more than 90% of the total responses.

Expression

```
sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) /
sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 > 90
```

OID

1.3.6.1.4.1.323.5.3.52.1.2.65

Metric Used

occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present.
Check that the session and user hasn't been removed in the OCS configuration, then configure the user(s).
For any additional guidance, contact My Oracle Support.

5.3.1.60 SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Summary

SNA Sy fail count exceeds the major threshold limit

Description

SNA Sy fail count exceeds the major threshold limit

Severity

Major

Condition

The failure rate of Sy SNA responses is more than 80% and less and or equal to 90% of the total responses.

Expression

$$\frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}\}[5\text{m}]))} * 100 > 80 \text{ and } \frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}\}[5\text{m}]))} * 100 \leq 90$$
OID

1.3.6.1.4.1.323.5.3.52.1.2.65

Metric Used

occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present.

Check that the session and user hasn't been removed in the OCS configuration, then configure the user(s).

For any additional guidance, contact My Oracle Support.

5.3.1.61 SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Summary

SNA Sy fail count exceeds the minor threshold limit

Description

SNA Sy fail count exceeds the minor threshold limit

Severity

Minor

Condition

The failure rate of Sy STA responses is more than 60% and less and or equal to 80% of the total responses.

Expression

$$\frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}\}[5\text{m}]))} * 100 > 60 \text{ and } \frac{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}, \text{responseCode!}\sim\text{"2.*"}\}[5\text{m}]))}{\text{sum}(\text{rate}(\text{occnp_diam_response_local_total}\{\text{msgType}=\text{"SNA"}\}[5\text{m}]))} * 100 \leq 80$$
OID

1.3.6.1.4.1.323.5.3.52.1.2.65

Metric Used

occnp_diam_response_local_total{msgType="STA", responseCode!~"2.*"}

Recommended Actions

Check the connectivity between diam-gw pod(s) and OCS server and ensure connectivity is present.

Check that the session and user hasn't been removed in the OCS configuration, then configure the user(s).

For any additional guidance, contact My Oracle Support.

5.3.2 PCF Alerts

This section provides information on PCF alerts.

5.3.2.1 INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD

Name in Alert Yaml File

IngressErrorRateAbove10PercentPerPod

Description

Ingress Error Rate above 10 Percent in {{ \$labels.kubernetes_name }} in {{ \$labels.kubernetes_namespace }}

Summary

Transaction Error Rate in {{ \$labels.kubernetes_node }} (current value is: {{ \$value }})

Severity

Critical

Condition

The total number of failed transactions per pod is above 10 percent of the total transactions.

OID

1.3.6.1.4.1.323.5.3.36.1.2.2

Metric Used

ocpm_ingress_response_total

Recommended Actions

The alert gets cleared when the number of failed transactions are below 10% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors.
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.2.2 SM_TRAFFIC_RATE_ABOVE_THRESHOLD

Name in Alert Yaml File

SMTrafficRateAboveThreshold

Description

SM service Ingress traffic Rate is above threshold of Max MPS (current value is: {{ \$value }})

Summary

Traffic Rate is above 90 Percent of Max requests per second

Severity

Major

OID

1.3.6.1.4.1.323.5.3.36.1.2.3

Condition

The total SM service Ingress traffic rate has crossed the configured threshold of 900 TPS. Default value of this alert trigger point in PCF_Alertrules.yaml file is when SM service Ingress Rate crosses 90% of maximum ingress requests per second.

Metric Used

ocpm_ingress_request_total{servicename_3gpp="npcf-smpolicycontrol"}

Recommended Actions

The alert gets cleared when the Ingress traffic rate falls below the threshold.

 Note

Threshold levels can be configured using the PCF_Alertrules.yaml file.

It is recommended to assess the reason for additional traffic. Perform the following steps to analyze the cause of increased traffic:

1. Refer **Ingress Gateway** section in Grafana to determine increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any additional guidance, contact My Oracle Support.

5.3.2.3 SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Name in Alert Yaml File

SMIngressErrorRateAbove10Percent

Description

Transaction Error Rate detected above 10 Percent of Total on SM service (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 10 Percent of Total Transactions

Severity

Critical

Condition

The number of failed transactions is above 10 percent of the total transactions.

OID

1.3.6.1.4.1.323.5.3.36.1.2.4

Metric Used

ocpm_ingress_response_total

Recommended Actions

The alert gets cleared when the number of failed transactions are below 10% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors. For instance:
`ocpm_ingress_response_total{servicename_3gpp="npcf-smpolicycontrol",response_code!="2.*"}`
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.2.4 SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Name in Alert Yaml File

SMEgressErrorRateAbove1Percent

Description

Egress Transaction Error Rate detected above 1 Percent of Total Transactions (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 1 Percent of Total Transactions

Severity

Minor

Condition

The number of failed transactions is above 1 percent of the total transactions.

OID

1.3.6.1.4.1.323.5.3.36.1.2.5

Metric Used

ocpm_egress_response_total

Recommended Actions

The alert gets cleared when the number of failed transactions are below 1% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors. For instance:
`ocpm_egress_response_total{servicename_3gpp="npcf-smpolicycontrol",response_code!="2.*"}`
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.2.5 PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Name in Alert Yaml File

PcfChfIngressTrafficRateAboveThreshold

Description

User service Ingress traffic Rate from CHF is above threshold of Max MPS (current value is: {{ \$value }})

Summary

Traffic Rate is above 90 Percent of Max requests per second

Severity

Major

Condition

The total User Service Ingress traffic rate from CHF has crossed the configured threshold of 900 TPS.

Default value of this alert trigger point in PCF_Alertrules.yaml file is when user service Ingress Rate from CHF crosses 90% of maximum ingress requests per second.

OID

1.3.6.1.4.1.323.5.3.36.1.2.11

Metric Used

ocpm_userservice_inbound_count_total{service_resource="chf-service"}

Recommended Actions

The alert gets cleared when the Ingress traffic rate falls below the threshold.

Note

Threshold levels can be configured using the PCF_Alertrules.yaml file.

It is recommended to assess the reason for additional traffic. Perform the following steps to analyze the cause of increased traffic:

1. Refer **Ingress Gateway** section in Grafana to determine increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any additional guidance, contact My Oracle Support.

5.3.2.6 PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Name in Alert Yaml File

PcfChfEgressErrorRateAbove10Percent

Description

Egress Transaction Error Rate detected above 10 Percent of Total on User service (current value is: {{ \$value }})

Summary

Transaction Error Rate detected above 10 Percent of Total Transactions

Severity

Critical

Condition

The number of failed transactions from UDR is more than 10 percent of the total transactions.

OID

1.3.6.1.4.1.323.5.3.36.1.2.12

Metric Used

ocpm_chf_tracking_response_total{servicename_3gpp="nchf-spendinglimitcontrol",response_code!~"2.*"}

Recommended Actions

The alert gets cleared when the number of failure transactions falls below the configured threshold.

Note

Threshold levels can be configured using the `PCF_Alert rules.yaml` file.

It is recommended to assess the reason for failed transactions. Perform the following steps to analyze the cause of increased traffic:

1. Refer **Egress Gateway** section in Grafana to determine increase in 4xx and 5xx error response codes.
2. Check **Egress Gateway** logs on Kibana to determine the reason for the errors.

For any additional guidance, contact My Oracle Support.

5.3.2.7 PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Name in Alert Yaml File

PcfChfIngressTimeoutErrorAboveMajorThreshold

Description

Ingress Timeout Error Rate detected above 10 Percent of Total towards CHF service (current value is: {{ \$value }})

Summary

Timeout Error Rate detected above 10 Percent of Total Transactions

Severity

Major

Condition

The number of failed transactions due to timeout is above 10 percent of the total transactions for CHF service.

OID

1.3.6.1.4.1.323.5.3.36.1.2.17

Metric Used

ocpm_chf_tracking_request_timeout_total{servicename_3gpp="nchf-spendinglimitcontrol"}

Recommended Actions

The alert gets cleared when the number of failed transactions due to timeout are below 10% of the total transactions.

To assess the reason for failed transactions, perform the following steps:

1. Check the service specific metrics to understand the service specific errors. For instance:
ocpm_chf_tracking_request_timeout_total{servicename_3gpp="nchf-spendinglimitcontrol"}
2. The service specific errors can be further filtered for errors specific to a method such as GET, PUT, POST, DELETE, and PATCH.

For any additional guidance, contact My Oracle Support.

5.3.2.8 PCF_PENDING_BINDING_SITE_TAKEOVER

Table 5-3 PCF_PENDING_BINDING_SITE_TAKEOVER

Field	Details
Description	The site takeover configuration has been activated
Summary	The site takeover configuration has been activated
Severity	CRITICAL
Condition	sum by (application, container, namespace) (changes(ocnp_pending_binding_site_takeover_total[2m])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.45
Metric Used	ocnp_pending_binding_site_takeover_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.3.2.9 PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Table 5-4 PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Field	Details
Description	The Pending Operation table threshold has been reached.
Summary	The Pending Operation table threshold has been reached.
Severity	CRITICAL
Condition	sum by (application, container, namespace) (changes(ocnp_threshold_limit_reached_total[2m])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.46
Metric Used	ocnp_threshold_limit_reached_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.3.2.10 PCF_PENDING_BINDING_RECORDS_COUNT

Table 5-5 PCF_PENDING_BINDING_RECORDS_COUNT

Field	Details
Description	An attempt to internally recreate a PCF binding has been triggered by PCF
Summary	An attempt to internally recreate a PCF binding has been triggered by PCF
Severity	MINOR
Condition	sum by (application, container, namespace) (changes(ocnp_pending_operation_records_count[10s])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.47
Metric Used	ocnp_pending_operation_records_count

Table 5-5 (Cont.) PCF_PENDING_BINDING_RECORDS_COUNT

Field	Details
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.3.2.11 TDF_CONNECTION_DOWN

Description

TDF connection is down.

Summary

TDF connection is down.

Severity

Critical

Condition

Diameter gateway raises an alert any time there is a disconnection with TDF peer node that is configured.

OID

1.3.6.1.4.1.323.5.3.52.1.2.48

Metric Used

ocncp_diam_conn_app_network{applicationName="Sd"} == 0

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.2.12 AUTONOMOUS_SUBSCRIPTION_FAILURE

Description

Autonomous subscription failed for a configured Slice Load Level

Summary

Autonomous subscription failed for a configured Slice Load Level

Severity

Critical

Condition

The number of failed Autonomous Subscription for a configured Slice Load Level in nwdaf-agent is greater than zero.

OID

1.3.6.1.4.1.323.5.3.52.1.2.49

Metric Used

subscription_failure{requestType="autonomous"}

Recommended Actions

The alert gets cleared when the failed Autonomous Subscription is corrected.

To clear the alert, perform the following steps:

1. Delete the Slice Load Level configuration.
2. Re-provision the Slice Load Level configuration.

For any additional guidance, contact My Oracle Support.

5.3.2.13 AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Table 5-6 AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Description	AM Notification Error Rate detected above 1 Percent of Total (current value is: {{ \$value }})
Summary	AM Notification Error Rate detected above 1 Percent of Total (current value is: {{ \$value }})
Severity	MINOR
Condition	(sum(rate(http_out_conn_response_total{pod=~".*amservice.*",responseCode!~"2.*",servicename3gpp="npcf-am-policy-control"}[1d])) / sum(rate(http_out_conn_response_total{pod=~".*amservice.*",servicename3gpp="npcf-am-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.54
Metric Used	http_out_conn_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.3.2.14 AM_AR_ERROR_RATE_ABOVE_1_PERCENT

Table 5-7 AM_AR_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Description	Alternate Routing Error Rate detected above 1 Percent of Total on AM Service (current value is: {{ \$value }})
Summary	Alternate Routing Error Rate detected above 1 Percent of Total on AM Service (current value is: {{ \$value }})
Severity	MINOR
Condition	(sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*amservice.*",responseCode!~"2.*",servicename3gpp="npcf-am-policy-control"}[1d])) / sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*amservice.*",servicename3gpp="npcf-am-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.55
Metric Used	ocpm_ar_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.3.2.15 UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Table 5-8 UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Description	UE Notification Error Rate detected above 1 Percent of Total (current value is: {{ \$value }})

Table 5-8 (Cont.) UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Summary	UE Notification Error Rate detected above 1 Percent of Total (current value is: {{ \$value }})
Severity	MINOR
Condition	(sum(rate(http_out_conn_response_total{pod=~".*ueservice.*",responseCode!~"2.*",servicename3gpp="npcf-ue-policy-control"}[1d])) / sum(rate(http_out_conn_response_total{pod=~".*ueservice.*",servicename3gpp="npcf-ue-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.56
Metric Used	http_out_conn_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.3.2.16 UE_AR_ERROR_RATE_ABOVE_1_PERCENT

Table 5-9 UE_AR_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Description	Alternate Routing Error Rate detected above 1 Percent of Total on UE Service (current value is: {{ \$value }})
Summary	Alternate Routing Error Rate detected above 1 Percent of Total on UE Service (current value is: {{ \$value }})
Severity	MINOR
Condition	(sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*ueservice.*",responseCode!~"2.*",servicename3gpp="npcf-ue-policy-control"}[1d])) / sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*ueservice.*",servicename3gpp="npcf-ue-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.57
Metric Used	ocpm_ar_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.3.3 PCRF Alerts

This section provides information about PCRF alerts.

5.3.3.1 PreUnreachableExceedsThreshold

PRE_UNREACHABLE_EXCEEDS_CRITICAL_THRESHOLD

Description

PRE fail count exceeds the critical threshold limit.

Summary

Alert PRE unreachable NS:{{ \$labels.kubernetes_namespace }}, PODNAME: {{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

PRE fail count exceeds the critical threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.9

Metric Used

http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD**Description**

PRE fail count exceeds the major threshold limit.

Summary

Alert PRE unreachable NS:{{ \$labels.kubernetes_namespace }}, PODNAME: {{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

PRE fail count exceeds the major threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.9

Metric Used

http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD**Description**

PRE fail count exceeds the minor threshold limit.

Summary

Alert PRE unreachable NS:{{ \$labels.kubernetes_namespace }}, PODNAME: {{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

PRE fail count exceeds the minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.9

Metric Used

http_out_conn_response_total{container="pcrf-core", responseCode!="2.*", serviceResource="PRE"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.2 PcrfDown

Description

PCRF Service is down

Summary

Alert PCRF_DOWN NS:{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

None of the pods of the PCRF service are available.

OID

1.3.6.1.4.1.323.5.3.44.1.2.33

Metric Used

appinfo_service_running{service=~".*pcrf-core"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.3 CCAFailCountExceedsThreshold

CCA Fail Count Exceeds Critical Threshold**Description**

CCA fail count exceeds the critical threshold limit

Summary

Alert CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The failure rate of CCA messages has exceeded the configured threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.13

Metric Used

occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!="2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

CCA Fail Count Exceeds Major Threshold**Description**

CCA fail count exceeds the major threshold limit

Summary

Alert CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:

```
{{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:
{{ $labels.instance }} REL:{{ $labels.release }}
```

Severity

Major

Condition

The failure rate of CCA messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.13

Metric Used

occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

CCA Fail Count Exceeds Minor Threshold**Description**

CCA fail count exceeds the minor threshold limit

Summary

Alert CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS:

```
{{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:
{{ $labels.instance }} REL:{{ $labels.release }}
```

Severity

Minor

Condition

The failure rate of CCA messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.13

Metric Used

occnp_diam_response_local_total{msgType=~"CCA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.4 AAFAilCountExceedsThreshold

AAA Fail Count Exceeds Critical Threshold**Description**

AAA fail count exceeds the critical threshold limit

Summary

Alert AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The failure rate of AAA messages has exceeded the critical threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.34

Metric Used

occpn_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

AAA Fail Count Exceeds Major Threshold**Description**

AAA fail count exceeds the major threshold limit

Summary

Alert AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The failure rate of AAA messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.34

Metric Used

occpn_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

AAA Fail Count Exceeds Minor Threshold**Description**

AAA fail count exceeds the minor threshold limit

Summary

Alert AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The failure rate of AAA messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.34

Metric Used

occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.5 RAARxFailCountExceedsThreshold

RAA Rx Fail Count Exceeds Critical Threshold**Description**

RAA Rx fail count exceeds the critical threshold limit

Summary

Alert RAA_Rx_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The failure rate of RAA Rx messages has exceeded the configured threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.35

Metric Used

occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Rx Fail Count Exceeds Major Threshold**Description**

RAA Rx fail count exceeds the major threshold limit

Summary

Alert RAA_Rx_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The failure rate of RAA Rx messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.35

Metric Used

ocnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!="2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Rx Fail Count Exceeds Minor Threshold**Description**

RAA Rx fail count exceeds the minor threshold limit

Summary

Alert RAA_Rx_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The failure rate of RAA Rx messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.35

Metric Used

ocnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!="2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.6 RAAGxFailCount ExceedsThreshold

RAA Gx Fail Count Exceeds Critical Threshold**Description**

RAA Gx fail count exceeds the critical threshold limit

Summary

Alert RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The failure rate of RAA Gx messages has exceeded the configured threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.18

Metric Used

ocnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!="2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Gx Fail Count Exceeds Major Threshold

Description

RAA Gx fail count exceeds the major threshold limit

Summary

Alert RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The failure rate of RAA Gx messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.18

Metric Used

ocnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Gx Fail Count Exceeds Minor Threshold

Description

RAA Gx fail count exceeds the minor threshold limit

Summary

Alert RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The failure rate of RAA Gx messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.18

Metric Used

ocnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.7 ASAFailCountExceedsThreshold

ASA Fail Count Exceeds Critical Threshold

Description

ASA fail count exceeds the critical threshold limit

Summary

Alert ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The failure rate of ASA messages has exceeded the configured threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.17

Metric Used

ocnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

ASA Fail Count Exceeds Major Threshold**Description**

ASA fail count exceeds the major threshold limit

Summary

Alert ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The failure rate of ASA messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.17

Metric Used

ocnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

ASA Fail Count Exceeds Minor Threshold**Description**

ASA fail count exceeds the minor threshold limit

Summary

Alert ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The failure rate of ASA messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.17

Metric Used

occnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.8 ASATimeoutCountExceedsThreshold

ASA Timeout Count Exceeds Critical Threshold

Description

ASA timeout count exceeds the critical threshold limit

Summary

Alert ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The timeout rate of ASA messages has exceeded the configured threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.31

Metric Used

occnp_diam_response_local_total{msgType="ASA", responseCode="timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

ASA Timeout Count Exceeds Major Threshold

Description

ASA timeout count exceeds the major threshold limit

Summary

Alert ASA_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The timeout rate of ASA messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.31

Metric Used

occnp_diam_response_local_total{msgType="ASA", responseCode!~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

ASA Timeout Count Exceeds Minor Threshold**Description**

ASA timeout count exceeds the minor threshold limit

Summary

Alert ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The timeout rate of ASA messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.31

Metric Used

occnp_diam_response_local_total{msgType="ASA", responseCode!~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.9 RAARxTimeoutCountExceedsThreshold

RAA Rx Timeout Count Exceeds Critical Threshold**Description**

RAA Rx timeout count exceeds the critical threshold limit

Summary

Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The timeout rate of RAA Rx messages has exceeded the configured threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.36

Metric Used

occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!
~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Rx Timeout Count Exceeds Major Threshold**Description**

RAA Rx timeout count exceeds the major threshold limit

Summary

Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The timeout rate of RAA Rx messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.36

Metric Used

occpn_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!
~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Rx Timeout Count Exceeds Minor Threshold**Description**

RAA Rx timeout count exceeds the minor threshold limit

Summary

Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The timeout rate of RAA Rx messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.36.1.2.36

Metric Used

occpn_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!
~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.10 RAARxTimeoutCountExceedsThreshold

RAA Gx Timeout Count Exceeds Critical Threshold

Description

RAA Gx timeout count exceeds the critical threshold limit

Summary

Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS:
{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The timeout rate of RAA Gx messages has exceeded the configured threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.32

Metric Used

occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!
~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Gx Timeout Count Exceeds Major Threshold

Description

RAA Gx timeout count exceeds the major threshold limit

Summary

Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS:
{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The timeout rate of RAA Gx messages has exceeded the configured major threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.32

Metric Used

occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!
~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

RAA Gx Timeout Count Exceeds Minor Threshold

Description

RAA Gx timeout count exceeds the minor threshold limit

Summary

Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS:
{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The timeout rate of RAA Gx messages has exceeded the configured minor threshold limit.

OID

1.3.6.1.4.1.323.5.3.44.1.2.32

Metric Used

occpn_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!
~"timeout"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.11 ResponseErrorRateAbovePercent

Response Error Rate Exceeds Critical Percent

Description

CCA, AAA, RAA, ASA and STA error rate combined is above 10 percent

Summary

Alert RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS:
{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The combined failure rate of CCA, AAA, RAA, ASA, and STA messages is more than 10% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.37

Metric Used

occpn_diam_response_local_total{ responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Response Error Rate Exceeds Major Percent

Description

CCA, AAA, RAA, ASA and STA error rate combined is above 5 percent

Summary

Alert RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The combined failure rate of CCA, AAA, RAA, ASA, and STA messages is more than 5% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.37

Metric Used

occnp_diam_response_local_total{ responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Response Error Rate Exceeds Minor Percent

Description

CCA, AAA, RAA, ASA and STA error rate combined is above 1 percent

Summary

Alert RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The combined failure rate of CCA, AAA, RAA, ASA, and STA messages is more than 1% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.37

Metric Used

occnp_diam_response_local_total{ responseCode!~"2.*"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.12 RxResponseErrorRateAbovePercent

Rx Response Error Rate Above Critical Percent

Description

Rx error rate combined is above 10 percent

Summary

Alert Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS:
{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The failure rate of Rx responses is more than 10% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.38

Metric Used

occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Rx Response Error Rate Above Major Percent

Description

Rx error rate combined is above 5 percent

Summary

Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS:
{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The failure rate of Rx responses is more than 5% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.38

Metric Used

occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Rx Response Error Rate Above Minor Percent

Description

Rx error rate combined is above 1 percent

Summary

Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS:
 {{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
 {{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The failure rate of Rx responses is more than 1% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.38

Metric Used

occpn_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

5.3.3.13 GxResponseErrorRateAbovePercent

Gx Response Error Rate Above Critical Percent

Description

Gx error rate combined is above 10 percent

Summary

Alert Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS:
 {{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
 {{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Critical

Condition

The failure rate of Gx responses is more than 10% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.39

Metric Used

occpn_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Gx Response Error Rate Above Major Percent

Description

Gx error rate combined is above 5 percent

Summary

Alert Gx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS:
 {{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
 {{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Major

Condition

The failure rate of Gx responses is more than 5% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.39

Metric Used

occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}

Recommended Actions

For any additional guidance, contact My Oracle Support.

Gx Response Error Rate Above Minor Percent**Description**

Gx error rate combined is above 1 percent

Summary

Alert Gx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS:

{{ \$labels.kubernetes_namespace }}, PODNAME:{{ \$labels.kubernetes_pod_name }}, INST:
{{ \$labels.instance }} REL:{{ \$labels.release }}

Severity

Minor

Condition

The failure rate of Gx responses is more than 1% of the total responses.

OID

1.3.6.1.4.1.323.5.3.36.1.2.39

Metric Used

occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}

Recommended Actions

For any additional guidance, contact My Oracle Support.