Oracle® Communications

Cloud Native Core, Converged Policy Troubleshooting Guide

Release 25.2.201
G49207-01
April 2026

Oracle Communications Cloud Native Core, Converged Policy Troubleshooting Guide, Release 25.2.201

G49207-01

Contents

Preface

Documentation Accessibility

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

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

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

Conventions

The following text conventions are used in this document:

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

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 Equipement
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 25.2.2xx.

Release 25.2.201 - G49207-01, April 2026

- Updated PCF Alerts section with the following alerts to support immediate report handling for AM-Data and UE-Policy-Set on N36 interface:
  - UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR
  - UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR
  - UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL
  - UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR
  - UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR
  - UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL
- Updated resolution steps of the Retry to CHF or UDR alternate route on timeout or error scenario in the UDR Connector Issues section.
- Updated resolution steps of the Inter-microservice communication failures scenario in the SM Service Issues section.

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 References

For more information, see the following documents:

- *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Converged Policy User Guide*
- *Oracle Communications Cloud Native Core, Converged Policy REST Specification Guide*
- *Oracle Communications Cloud Native Core, Converged Policy Design Guide*

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.

2.1 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.

2.1.1 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.

2.1.2 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?

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.

3.1 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>
   ```

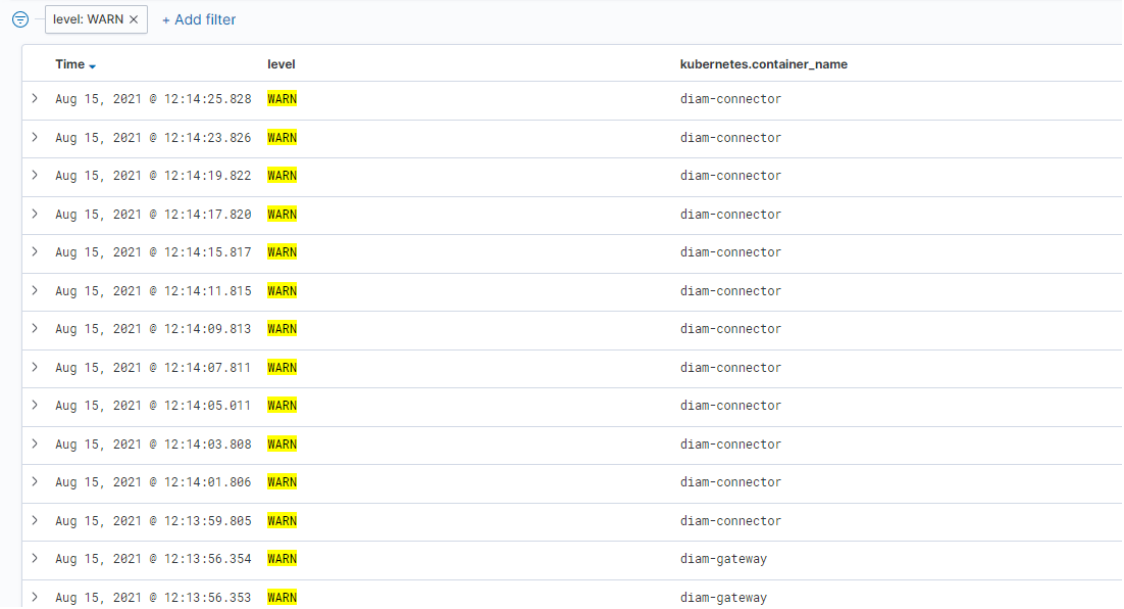
For more information on kubectl commands, see Kubernetes website.

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:



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": "DiuOSHsBX9U84vckBYSO",
  "_version": 1,
```

```
  "_score": null,
  "_source": {
    "stream": "stdout",
    "docker": {
      "container_id":
"fc7c3e68ba775ddca4e7f5d0603c8ba1bc414703e7d28f6177012893ca342a3b"
    },
    "kubernetes": {
      "container_name": "user-service",
      "namespace_name": "mdc3",
      "pod_name": "mdc3-cnpolicy-occnp-udr-connector-697f7f5b8b-9l2jz",
      "container_image": "titans-1-bastion-1:5000/occnp/oc-pcf-user:1.14.0-
nb-20210804",
      "container_image_id": "titans-1-bastion-1:5000/occnp/oc-pcf-
user@sha256:d66b1017fd8b1946744a2115bc088349c95f93db17626a20fbb11e25ff543f83",
      "pod_id": "f0b233bb-10a1-4b4c-9b77-f864659b9c3e",
      "host": "titans-1-k8s-node-2",
      "labels": {
        "application": "occnp",
        "engVersion": "1.14.0-nb-20210804",
        "microservice": "occnp_pcf_user",
        "mktgVersion": "1.0.0",
        "pod-template-hash": "697f7f5b8b",
        "vendor": "Oracle",
        "app_kubernetes_io/instance": "mdc3-cnpolicy",
        "app_kubernetes_io/managed-by": "Helm",
        "app_kubernetes_io/name": "user-service",
        "app_kubernetes_io/part-of": "occnp",
        "app_kubernetes_io/version": "1.0.0",
        "helm_sh/chart": "user-service-1.14.0-nb-20210804",
        "io_kompose_service": "mdc3-cnpolicy-occnp-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-occnp-config-mgmt:8000/pcf/nf-common-component/v1/nrf-client-
nfmanagement/nfProfileList\": Connect to mdc3-cnpolicy-occnp-config-mgmt:8000
[mdc3-cnpolicy-occnp-config-mgmt/10.233.53.78] failed: Connect timed out;
nested exception is org.apache.http.conn.ConnectTimeoutException: Connect to
mdc3-cnpolicy-occnp-config-mgmt:8000 [mdc3-cnpolicy-occnp-config-mgmt/
10.233.53.78] failed: Connect timed out",
```

```
      "message": "I/O error on GET request for \"http://mdc3-cnpolicy-occnp-
config-mgmt:8000/pcf/nf-common-component/v1/nrf-client-nfmanagement/
nfProfileList\": Connect to mdc3-cnpolicy-occnp-config-mgmt:8000 [mdc3-
cnpolicy-occnp-config-mgmt/10.233.53.78] failed: Connect timed out; nested
exception is org.apache.http.conn.ConnectTimeoutException: Connect to mdc3-
cnpolicy-occnp-config-mgmt:8000 [mdc3-cnpolicy-occnp-config-mgmt/
10.233.53.78] failed: Connect timed out",
      "name": "org.springframework.web.client.ResourceAccessException",
      "cause": {
        "commonElementCount": 14,
        "localizedMessage": "Connect to mdc3-cnpolicy-occnp-config-mgmt:8000
[mdc3-cnpolicy-occnp-config-mgmt/10.233.53.78] failed: Connect timed out",
        "message": "Connect to mdc3-cnpolicy-occnp-config-mgmt:8000 [mdc3-
cnpolicy-occnp-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.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"
        },
        "extendedStackTrace": "org.apache.http.conn.ConnectTimeoutException:
Connect to mdc3-cnpolicy-occnp-config-mgmt:8000 [mdc3-cnpolicy-occnp-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.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]\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.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-cnpolicy-occnp-config-mgmt:8000/pcf/nf-common-
component/v1/nrf-client-nfmanagement/nfProfileList\": Connect to mdc3-
cnpolicy-occnp-config-mgmt:8000 [mdc3-cnpolicy-occnp-config-mgmt/
10.233.53.78] failed: Connect timed out; nested exception is
org.apache.http.conn.ConnectTimeoutException: Connect to mdc3-cnpolicy-occnp-
config-mgmt:8000 [mdc3-cnpolicy-occnp-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$0(CmRestClient.java:54)
~[cne-common-0.0.8-SNAPSHOT-dev.jar!/:?]\n\tat
org.springframework.retry.support.RetryTemplate.doExecute(RetryTemplate.java:3
29) ~[spring-retry-1.3.1.jar!/:?]\n\tat
org.springframework.retry.support.RetryTemplate.execute(RetryTemplate.java:209
) ~[spring-retry-1.3.1.jar!/:?]\n\tat
ocpm.cne.common.cmclient.CmRestClient.get(CmRestClient.java:53) [cne-
common-0.0.8-SNAPSHOT-dev.jar!/:?]\n\tat
ocpm.cne.common.cmclient.CmRestClientTask.run(CmRestClientTask.java:32) [cne-
common-0.0.8-SNAPSHOT-dev.jar!/:?]\n\tat
org.springframework.scheduling.support.DelegatingErrorHandlingRunnable.run(Del
egatingErrorHandlingRunnable.java:54) [spring-
context-5.3.4.jar!/:5.3.4]\n\tat
java.util.concurrent.Executors$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-occnp-
```

```
config-mgmt:8000 [mdc3-cnpolicy-occnp-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.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\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.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"
    },
    "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-occnp-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": "pYKOSHsBgXqNeaK8Blhv",
  "_version": 1,
  "_score": null,
  "_source": {
    "stream": "stdout",
    "docker": {
      "container_id":
"d373ee8717f2c21ba1c06d7b78ba1d74b15239e044db24a98d8cbd7e0e0c70b6"
    },
    "kubernetes": {
      "container_name": "perf-info",
      "namespace_name": "mdc2",
      "pod_name": "mdc2-cnpolicy-performance-b9587f5cc-mxvp4",
```

```
      "container_image": "titans-1-bastion-1:5000/occnp/oc-perf-info:1.14.0-
rc.1",
      "container_image_id": "titans-1-bastion-1:5000/occnp/oc-perf-
info@sha256:c7b04350374a238aa4b05f1e5de50feeb65a45c09b48260b0639fb0771094975",
      "pod_id": "13f40f5f-dcea-4a1f-88bf-396520d360df",
      "host": "titans-1-k8s-node-11",
      "labels": {
        "application": "occnp",
        "engVersion": "1.14.0-rc.1",
        "microservice": "perf_info",
        "mktgVersion": "1.0.0",
        "pod-template-hash": "b9587f5cc",
        "vendor": "Oracle",
        "app_kubernetes_io/instance": "mdc2-cnpolicy",
        "app_kubernetes_io/managed-by": "Helm",
        "app_kubernetes_io/name": "perf-info",
        "app_kubernetes_io/part-of": "occnp",
        "app_kubernetes_io/version": "1.0.0",
        "helm_sh/chart": "perf-info-1.14.0-rc.1",
        "io_kompose_service": "mdc2-cnpolicy-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://occne-prometheus-server.occne-
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-cnpolicy-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.

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 3-1 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
kubernetes.labels.application	NF Application Name
kubernetes.labels.engVersion	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

Table 3-1 (Cont.) Log Attributes

Attribute	Description
kubernetes.pod_name	Pod Name
kubernetes.container_name	Container Name
Docker.container_id	Process ID internally assigned
kubernetes.labels.vendor	Vendor of product

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.

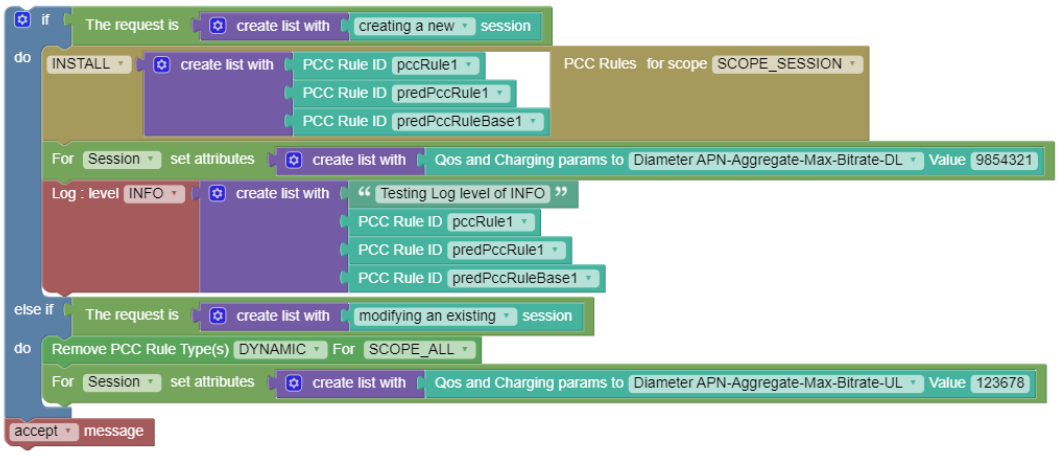
For more information on how to enable this feature, see the section "Subscriber Activity Logging" in *Oracle Communications Cloud Native Core, Converged Policy User's Guide*.

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",
    "reqeustId":"supi;
    imsi-60000000001",
    "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 **Configuration in CNE**.
> - For CNE versions prior to 23.2.0, follow Step b of **Configuration in CNE**.

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:
        -occnp
```

- 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

i. 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": "occnp" }]'
```

Example:

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

Sample output:

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

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: occnp
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: occnp
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 3-2 tcpdump

Options Tested	Description	Output	Capabilities

-D	Print the list of the network interfaces available on the system and on which *tcpdump* can capture packets.	`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]`
			NET_ADMIN, NET_RAW

-i	Listen on *interface*.	`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)	NET_ADMIN, NET_RAW
-w	Write the raw packets to file rather than parsing and printing them.	`tcpdump -w capture.pcap -i eth0`	NET_ADMIN, NET_RAW
-r	Read packets from *file* (which was created with the **-w** option).	`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	NET_ADMIN, NET_RAW

ip

Table 3-3 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 3-4 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:tproxy 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.defaul: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 3-4 (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:tproxy 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 outIcmp: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 tableIface 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 BMRUlo 65536 0 0 0 0 0 0 0 0 LRU	--

jq

Table 3-5 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 3-6 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 3-7 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 3-8 nmap

Options Tested	Description	Output	Capabilities

<ip>	Scan for Live hosts, Operating systems, packet filters, and open ports running on remote hosts.	`nmap 10.178.254.194`
		
		`Starting Nmap 6.40 ( http://nmap.org ) at 2020-09-29 05:54 UTCNmap 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 portsPORT STATE SERVICE22/tcp open ssh179/tcp open bgp6666/tcp open irc6667/tcp open irc30000/tcp open unknownNmap done: 1 IP address (1 host up) scanned in 0.04 seconds`
			--

Table 3-8 (Cont.) nmap

Options Tested	Description	Output	Capabilities

-v	Increase verbosity level.	`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`
			--

Table 3-8 (Cont.) nmap

Options Tested	Description	Output	Capabilities

-iL	Scan all the listed IP addresses in a file.	`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`
			--

dig

Table 3-9 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.	`dig 10.178.254.194` ***Note**: The IP should be reachable from inside the container.*	--
-x	Query DNS Reverse Look-up.	`dig -x 10.178.254.194`	--

3.4.1 Debug Tool Configuration Parameters

Following are the parameters used to configure debug tool.

CNE Parameters

Table 3-10 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 3-11 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 3-12 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 3-13 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 3-13 (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.

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.

4.1 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 preupgrade 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 logs -n <release-namespace> [options]
   ```

   Common options

   `-p`: Shows logs from the previous instance of a container that has crashed and restarted.

   `--since= <duration>` Returns logs newer than a relative duration
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:

   ```
   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.

- **Policy upgrade fails due to Helm upgrade failure during post-upgrade job for nrf-client-nfdiscovery**

  Helm upgrade can fail due to an exception in deleting the older release entry from common_configuration table for nrf-client-nfdiscovery service.

  Workaround:

  – Retry the upgrade, which will delete the older version's configuration enabling upgrade to go through.
  – If the retry fails, manually delete the older version entries from common_configuration table and retry the upgrade. This can bring up the services with newer version's configuration data.

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 behavior 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 replicasets. 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}
```

4.2 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.

4.3 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.BsfConnect
or","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-smservice.pcf\",\"pcfDiamHost\":\"pcf-
smservice\",\"pcfDiamRealm\":\"pcf-smservice.svc\",\"snssai\":
{\"sst\":11,\"sd\":\"abc123\"}}","endOfBatch":false,"loggerFqcn":"org.apache.l
ogging.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.BsfConnect
or","message":"Receive Binding Reply from BSF: 406
NOT_ACCEPTABLE","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4
jLogger","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.S
mMetrics","message":"Pegging binding response metric. Dnn :dnn1, snssai : 11-
abc123, operationType : create ,mode : synchronous ,responseCode :
4xx","endOfBatch":false,"loggerFqcn":"org.apache.logging.slf4j.Log4jLogger","t
hreadId":37,"threadPriority":5,"messageTimestamp":"2021-05-24T08:29:01.946+000
0"}
```


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-occnp-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,
  "loggerFqcn": "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-a9b82fdeeef3


Error has been observed at the following site(s):
|_ checkpoint ? Request to POST http://my-cnpolicy-occnp-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-1
4","level":"ERROR","loggerName":"ocpm.pcf.service.sm.serviceconnector.BindingS
erviceConnector","message":"Failed to call Binding service for
      a8f8cf48-b889-44ee-95e6-a9b82fdeeef3 :

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","thre
adId":23640,"threadPriority":5,"messageTimestamp":"2021-06-01T11:46:09.166+000
0"}org.springframework.web.reactive.function.client.WebClientRequestException:
 Connection
      refused; nested exception is java.net.ConnectException: Connection
refusedat

org.springframework.web.reactive.function.client.ExchangeFunctions$DefaultExch
angeFunction.lambda$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-occnp-binding:8000/binding/v1/contextBinding/context-owner/PCF-SM
[DefaultWebClient]Stack trace:at

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

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

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

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

reactor.core.publisher.MonoIgnoreThen$ThenAcceptInner.onError(MonoIgnoreThen.j
ava:315)at

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

org.eclipse.jetty.reactive.client.internal.ResponseListenerProcessor.onComplet
e(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)a
t
org.eclipse.jetty.io.ManagedSelector.processConnect(ManagedSelector.java:335)a
t org.eclipse.jetty.io.ManagedSelector.access$1600(ManagedSelector.java:62)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.processSelected(ManagedS
elector.java:639)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.produce(ManagedSelector.
java:501)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)a
t org.eclipse.jetty.io.ManagedSelector.access$1600(ManagedSelector.java:62)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.processSelected(ManagedS
elector.java:639)at
org.eclipse.jetty.io.ManagedSelector$SelectorProducer.produce(ManagedSelector.
java:501)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)
```

Resolution Steps
To resolve this issue, perform the following steps:

1. Verify that the end point url (service FQDN/IP/PORT) is correctly specified for the target service in the application-config yaml or deployment file for the source service; if not, update.
2. Try again after restarting the source service pod.
3. Check the source service pod log to see if the call was successful.

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.SQLNonTransientConnectionException","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.Con
nectException: 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\n The 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.Con
nectException: 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.ja
va:1194)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.jav
a:1082)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.connect(HttpURLConnection.java:101
6)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getInputStream0(HttpURLConnection.
java:1600)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.j
ava: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.j
ava: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.getConfiguration
temByTopicWithRetry(ConfigServerConnectionWithRetry.java:313)
      [cne-common-1.11.0.jar!/:?]\n\tat

ocpm.cne.common.configclient.ConfigClient.getConfigurationItemByTopic(ConfigCl
ient.java:178)
      [cne-common-1.11.0.jar!/:?]\n\tat

ocpm.cne.common.configclient.ConfigClient.getConfigurationItemByTopic(ConfigCl
ient.java:149)
      [cne-common-1.11.0.jar!/:?]\n\tat

ocpm.cne.common.logging.level.PullLogLevelConfigTask.run(PullLogLevelConfigTas
k.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.ja
va:1194)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.jav
a:1082)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.connect(HttpURLConnection.java:101
6)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getInputStream0(HttpURLConnection.
```

```
java:1600)
        ~[?:?]\n\tat
sun.net.www.protocol.http.HttpURLConnection.getInputStream(HttpURLConnection.j
ava: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-occnp-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-occnp-
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-occnp-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,
  "loggerFqcn": "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-occnp-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-
occnp-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: RetryProfilebject
[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-
occnp-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":"W
ARN","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.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":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\":null,\"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\":null,\"title\":\"Service
Unavailable\",\"status\":503,\"detail\":\"Service
Unavailable\",\"instance\":null,\"cause\":null,\"invalidParams\":null},[]>",
  "endOfBatch": false,
  "loggerFqcn": "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","l
evel":"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/0:0:0:0:0:0:0:1] failed:
      Connection refused; nested exception is
org.apache.http.conn.HttpHostConnectException: Connect
      to localhost:5000 [localhost/127.0.0.1, localhost/0:0:0:0:0:0:0:1]
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/
0:0:0:0:0:0:0:1] failed:
      Connection refused; nested exception is
org.apache.http.conn.HttpHostConnectException: Connect
      to localhost:5000 [localhost/127.0.0.1, localhost/0:0:0:0:0:0:0:1]
failed: Connection

refused","name":"org.springframework.web.client.ResourceAccessException","caus
e":{"commonElementCount":14,"localizedMessage":"Connect
      to localhost:5000 [localhost/127.0.0.1, localhost/0:0:0:0:0:0:0:1]
```

```
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.Con
nectException: 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.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"},"extendedStackTrace":"org.apache.http.conn.HttpHost
ConnectException:
      Connect to localhost:5000 [localhost/127.0.0.1, localhost/
0:0:0:0:0:0:0:1] failed: Connection
      refused\n\tat

org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultH
ttpClientConnectionOperator.java:156)
      ~[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.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]\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(PlainCo
nnectionSocketFactory.java:75)
```

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.
4. If NRF returns an error message indicating incorrect or missing parameters, update the request parameters accordingly based on NRF's feedback. This may involve:
   - Adjusting filter values
   - Adding required query parameters
   - Correcting resource URIs

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":
{"epochSecond":1621844768,"nanoOfSecond":666347628},"thread":"UserService_Thre
adPool_7","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":103,"threadPriority":5,"messageTimestamp":"2021-05-24T08:26:08.66
6+0000"}{"instant":
{"epochSecond":1621844768,"nanoOfSecond":666674276},"thread":"UserService_Thre
adPool_7","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":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","t
hreadId":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-10000000002],
      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","t
hreadId":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","messag
e":"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,
  "loggerFqcn": "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,
  "loggerFqcn": "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.

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.

Upgrade failure with specific error in nrf-client-nfmanagement

If the upgrade procedure fails due to the below error in `nrf-client-nfmanagement-pre-upgrade` hooks:

```
Upgrade to same or higher versions is only supported. Can not proceed with
upgrade. Exiting...
```

Verify the release version in `ReleaseConfig` table in `nrf-client-nfmanagement`. If needed, manually update the version number following the below procedure:

> **Important**
>
> Perform this procedure in consultation with Oracle Engineering team.

If the release version in `ReleaseConfig` table is incorrect:

1. Backup `ReleaseConfig` table.

   ```
   mysqldump -u<privileged-user> –p<privileged-password> <release-db-name>
   ReleaseConfig > ReleaseConfig.sql
   ```

   Copy the backup to Bastion server.
2. Log in to MySQL pod.
3. Run the following command to manually update the `ReleaseConfig` table.

   ```
   use <release-db-name>;


   select * from ReleaseConfig where CfgKey='nrf-client-nfmanagement';
   ```

4. After the rollback procedure, if the `CfgValue` is as shown below:

   ```
   {"currentVersion":{"version":2300100,"jsonSchemaVersionMap":
   {}},"rollbackVersionSet":[{"version":2200304,"jsonSchemaVersionMap":{}},
   {"version":2300100,"jsonSchemaVersionMap":{}},
   {"version":2200401,"jsonSchemaVersionMap":{}}]}
   ```

upadte the `CfgValue`:

```
update ReleaseConfig set CfgValue='{"currentVersion":
{"version":2200304,"jsonSchemaVersionMap":{}},"rollbackVersionSet":
[{"version":2200304,"jsonSchemaVersionMap":{}},
{"version":2200401,"jsonSchemaVersionMap":{}}]}' where CfgKey='nrf-client-
nfmanagement';
```

5. Retry the upgrade procedure.

4.5 Bulk Import and Export Issues

This section describes the most common bulk import and export 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.

Bulk Import and Export – Partial Success Scenarios

Partial success messages encountered during bulk import/export operations can be ignored in the following scenarios, as they are aligned with recent updates.

1. Congestion Load Shedding Profile
When importing legacy congestion configuration data into version 25.1.100 or later, partial success can occur if the data contains a legacy congestion load shedding profile.

Reason: This behavior is expected due to migration changes in congestion configuration screens introduced in these versions. Partial success in this case can be ignored.

2. URSP Rules Import
Partial success can occur when importing URSP rules that include `MATCH_ALL` in combination with other `trafficDescriptorType` values.

Reason: `MATCH_ALL` cannot be combined with other `trafficDescriptorType` entries within a single rule. The system imports the valid entries and ignore any invalid combinations.

3. Policy Project Export
Partial success with an internal service error may occur during the export of the Policy Project or Bulk Export due to a referential integrity issue.

Reason: This issue arises when the Policy Project contains an empty URSP rule name in the policy project JSON file (For example, `<field name="ursp"></field>`).

Action: This issue is only observed during export and does not affect the import process. Ensure that no URSP rule names are left empty in the JSON configuration.

For example:

- Invalid: `<field name="ursp"></field>` (Empty URSP rule name)
- Valid: `<field name="ursp">ios001</field>` (Valid URSP rule name)

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.

You can configure alerts in Prometheus and `Alertrules.yaml` file.

The following table describes the various severity types of alerts generated by Policy:

Table 5-1 Alerts Levels or Severity Types

Alerts Levels / Severity Types	Definition
Critical	Indicates a severe issue that poses a significant risk to safety, security, or operational integrity. It requires immediate response to address the situation and prevent serious consequences. Raised for conditions can affect the service of Policy.
Major	Indicates a more significant issue that has an impact on operations or poses a moderate risk. It requires prompt attention and action to mitigate potential escalation. Raised for conditions can affect the service of Policy.
Minor	Indicates a situation that is low in severity and does not pose an immediate risk to safety, security, or operations. It requires attention but does not demand urgent action. Raised for conditions can affect the service of Policy.
Info or Warn (Informational)	Provides general information or updates that are not related to immediate risks or actions. These alerts are for awareness and do not typically require any specific response. WARN and INFO alerts may not impact the service of Policy.

For details on how to configure Policy alerts, see *Configuring Alerts* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

For details on how to configure SNMP Notifier, see *Configuring SNMP Notifier* section in *Oracle Communications Cloud Native Core, Converged Policy Installation, Upgrade, and Fault Recovery Guide*.

5.1 List of Alerts

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

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

5.1.1 Common Alerts

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

5.1.1.1 POD_CONGESTION_L1

Table 5-2 POD_CONGESTION_L1

Field	Details
Name in Alert Yaml File	PodCongestionL1
Description	Alert when cpu of pod is in CONGESTION_L1 state.
Summary	Alert when cpu of pod is in CONGESTION_L1 state.
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="cpu",container!~"bulwark|diam-gateway"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.71
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.2 POD_CONGESTION_L2

Table 5-3 POD_CONGESTION_L2

Field	Details
Name in Alert Yaml File	PodCongestionL2
Description	Alert when cpu of pod is in CONGESTION_L2 state.
Summary	Alert when cpu of pod is in CONGESTION_L2 state.
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="cpu"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.72
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.3 POD_PENDING_REQUEST_CONGESTION_L1

Table 5-4 POD_PENDING_REQUEST_CONGESTION_L1

Field	Details
Name in Alert Yaml File	PodPendingRequestCongestionL1
Description	Alert when queue of pod is in CONGESTION_L1 state.
Summary	Alert when queue of pod is in CONGESTION_L1 state.
Severity	critical
Expression	occnp_pod_resource_congestion_state{type="queue",container!~"bulwark|diam-gateway"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.73
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.4 POD_PENDING_REQUEST_CONGESTION_L2

Table 5-5 POD_PENDING_REQUEST_CONGESTION_L2

Field	Details
Name in Alert Yaml File	PodPendingRequestCongestionL2
Description	Alert when queue of pod is in CONGESTION_L2 state.
Summary	Alert when queue of pod is in CONGESTION_L2 state.
Severity	critical
Expression	occnp_pod_resource_congestion_state{type="queue"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.74
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.5 POD_CPU_CONGESTION_L1

Table 5-6 POD_CPU_CONGESTION_L1

Field	Details
Name in Alert Yaml File	PodCPUCongestionL1
Description	Alert when cpu of pod is in CONGESTION_L1 state.
Summary	Alert when cpu of pod is in CONGESTION_L1 state.Alert when pod is in CONGESTION_L1 state.
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="cpu",container!~"bulwark|diam-gateway"} == 2
OID	1.3.6.1.4.1.323.5.3.52.1.2.73
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.6 POD_CPU_CONGESTION_L2

Table 5-7 POD_CPU_CONGESTION_L2

Field	Details
Name in Alert Yaml File	PodCPUCongestionL2
Description	Alert when cpu of pod is in CONGESTION_L2 state.
Summary	Alert when cpu of pod is in CONGESTION_L2 state.
Severity	critical
Expression	occnp_pod_resource_congestion_state{type="cpu"} == 3
OID	1.3.6.1.4.1.323.5.3.52.1.2.74
Metric Used	occnp_pod_resource_congestion_state
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.7 Pod_Memory_DoC

Table 5-8 Pod_Memory_DoC

Field	Details
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
Expression	occnp_pod_resource_congestion_state{type="memory"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.31
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. **Note** Threshold levels can be configured using the `PCF_Alertrules.yaml` file. For any additional guidance, contact My Oracle Support.

5.1.1.8 Pod_Memory_Congested

Table 5-9 Pod_Memory_Congested

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

Table 5-9 (Cont.) Pod_Memory_Congested

Field	Details
Summary	Pod Resource Congestion status of {{$labels.service}} service is congested for Memory type
Severity	Critical
Expression	occnp_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. For any additional guidance, contact My Oracle Support.

5.1.1.9 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-10 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the critical threshold limit.
Summary	RAA Rx fail count exceeds the critical threshold limit.
Severity	CRITICAL
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.35
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.10 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-11 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the major threshold limit.
Summary	RAA Rx fail count exceeds the major threshold limit.
Severity	MAJOR
Expression	sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="RAA", appId="16777236"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.35
Metric Used	occnp_diam_response_local_total

Table 5-11 (Cont.) RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

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

5.1.1.11 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-12 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the minor threshold limit.
Summary	RAA Rx fail count exceeds the minor threshold limit.
Severity	MINOR
Expression	sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="RAA"}[5m])) * 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.

5.1.1.12 ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-13 ASA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA Rx fail count exceeds the critical threshold limit.
Summary	ASA Rx fail count exceeds the critical threshold limit.
Severity	CRITICAL
Expression	sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.66
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.13 ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-14 ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA Rx fail count exceeds the major threshold limit.

Table 5-14 (Cont.) ASA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Summary	ASA Rx fail count exceeds the major threshold limit.
Severity	MAJOR
Expression	sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.66
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.14 ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-15 ASA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA Rx fail count exceeds the minor threshold limit.
Summary	ASA Rx fail count exceeds the minor threshold limit.
Severity	MINOR
Expression	sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 <= 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.

5.1.1.15 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-16 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA Rx timeout count exceeds the minor threshold limit
Summary	ASA Rx timeout count exceeds the minor threshold limit
Severity	MINOR

Table 5-16 (Cont.) ASA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.67
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.16 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-17 ASA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA Rx timeout count exceeds the major threshold limit
Summary	ASA Rx timeout count exceeds the major threshold limit
Severity	sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 <= 90
Expression	MAJOR
OID	1.3.6.1.4.1.323.5.3.52.1.2.67
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.17 ASA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-18 ASA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA Rx timeout count exceeds the critical threshold limit
Summary	ASA Rx timeout count exceeds the critical threshold limit
Severity	CRITICAL
Expression	sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA",responseCode="timeout"}[5m])) / sum(rate(occnp_diam_response_local_total{appId="16777236",msgType="ASA"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.67
Metric Used	-

Table 5-18 (Cont.) ASA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

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

5.1.1.18 SCP_PEER_UNAVAILABLE

Table 5-19 SCP_PEER_UNAVAILABLE

Field	Details
Description	Configured SCP peer is unavailable.
Summary	Configured SCP peer is unavailable.
Severity	Major
Expression	occnp_oc_egressgateway_peer_health_status != 0. SCP peer [{{$labels.peer}}] is unavailable.
OID	1.3.6.1.4.1.323.5.3.52.1.2.60
Metric Used	occnp_oc_egressgateway_peer_health_status
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.19 SCP_PEER_SET_UNAVAILABLE

Table 5-20 SCP_PEER_SET_UNAVAILABLE

Field	Details
Description	None of the SCP peer available for configured peerset.
Summary	{{ $value }} SCP peers under peer set {{$labels.peerset}} are currently unavailable.
Severity	Critical
Expression	(occnp_oc_egressgateway_peer_count > 0 and (occnp_oc_egressgateway_peer_available_count) == 0)
OID	1.3.6.1.4.1.323.5.3.52.1.2.61
Metric Used	occnp_oc_egressgateway_peer_count and occnp_oc_egressgateway_peer_available_count
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.

5.1.1.20 STALE_CONFIGURATION

Table 5-21 STALE_CONFIGURATION

Field	Details
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

Table 5-21 (Cont.) STALE_CONFIGURATION

Field	Details
Expression	(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.

5.1.1.21 POLICY_SERVICES_DOWN

Table 5-22 POLICY_SERVICES_DOWN

Field	Details
Name in Alert Yaml File	PCF_SERVICES_DOWN
Description	{{$labels.service}} service is not running.
Summary	{{$labels.service}} service is not running.
Severity	Critical
Expression	None of the pods of the CNC Policy application are available.
OID	1.3.6.1.4.1.323.5.3.36.1.2.1
Metric Used	appinfo_service_running{vendor="Oracle", application="occnp", category!=""}!= 1
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.22 DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 5-23 DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
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
Expression	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

Table 5-23 (Cont.) DIAM_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
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.

5.1.1.23 DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 5-24 DIAM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Name in Alert Yaml File	DiamIngressErrorRateAbove10Percent
Description	Transaction Error Rate detected above 10 Percent of Total on Diameter Connector (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 10 Percent of Total Transactions.
Severity	Critical
Expression	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.

5.1.1.24 DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Table 5-25 DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
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

Table 5-25 (Cont.) DIAM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Severity	Minor
Expression	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.

5.1.1.25 UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 5-26 UDR_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
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
Expression	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.

5.1.1.26 UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 5-27 UDR_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
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
Expression	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.

5.1.1.27 POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 5-28 POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
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
Expression	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.

Table 5-28 (Cont.) POLICYDS_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
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.

5.1.1.28 POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 5-29 POLICYDS_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
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
Expression	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.

5.1.1.29 POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Table 5-30 POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
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

Table 5-30 (Cont.) POLICYDS_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Expression	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.

5.1.1.30 UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Table 5-31 UDR_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Field	Details
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
Expression	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="nudr-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="nudr-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.

5.1.1.31 DB_TIER_DOWN_ALERT

Table 5-32 DB_TIER_DOWN_ALERT

Field	Details
Name in Alert Yaml File	DBTierDownAlert

Table 5-32 (Cont.) DB_TIER_DOWN_ALERT

Field	Details
Description	DB cannot be reachable.
Summary	DB cannot be reachable.
Severity	Critical
Expression	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	For any additional guidance, contact My Oracle Support.

5.1.1.32 CPU_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Table 5-33 CPU_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Field	Details
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
Expression	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	The alert gets cleared when the CPU utilization falls below the minor threshold or crosses the major threshold, in which case CPUUsagePerServiceAboveMajorThreshold alert shall be raised. **Note**: Threshold levels can be configured using the `PCF_Alertrules.yaml` file. For any additional guidance, contact My Oracle Support.

5.1.1.33 CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Table 5-34 CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Field	Details
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
Expression	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.

Table 5-34 (Cont.) CPU_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The alert gets cleared when the CPU utilization falls below the major threshold or crosses the critical threshold, in which case CPUUsagePerServiceAboveCriticalThreshold alert shall be raised. **Note**: Threshold levels can be configured using the `PCF_Alertrules.yaml` file. For any additional guidance, contact My Oracle Support.

5.1.1.34 CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Table 5-35 CPU_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Field	Details
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
Expression	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	The alert gets cleared when the CPU utilization falls below the critical threshold. **Note**: Threshold levels can be configured using the `PCF_Alertrules.yaml` file. For any additional guidance, contact My Oracle Support.

5.1.1.35 MEMORY_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Table 5-36 MEMORY_USAGE_PER_SERVICE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	MemoryUsagePerServiceAboveMinorThreshold
Description	Memory usage for {{$labels.service}} service is above 60
Summary	Memory usage for {{$labels.service}} service is above 60
Severity	Minor
Expression	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 `PCF_Alertrules.yaml` file. For any additional guidance, contact My Oracle Support.

5.1.1.36 MEMORY_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Table 5-37 MEMORY_USAGE_PER_SERVICE_ABOVE_MAJOR_THRESHOLD

Field	Details
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
Expression	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	The alert gets cleared when the memory utilization falls below the major threshold or crosses the critical threshold, in which case MemoryUsagePerServiceAboveCriticalThreshold alert shall be raised. **Note**: Threshold levels can be configured using the `PCF_Alertrules.yaml` file. For any additional guidance, contact My Oracle Support.

5.1.1.37 MEMORY_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Table 5-38 MEMORY_USAGE_PER_SERVICE_ABOVE_CRITICAL_THRESHOLD

Field	Details
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
Expression	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	The alert gets cleared when the memory utilization falls below the critical threshold. **Note**: Threshold levels can be configured using the `PCF_Alertrules.yaml` file. For any additional guidance, contact My Oracle Support.

5.1.1.38 POD_CONGESTED

Table 5-39 POD_CONGESTED

Field	Details
Name in Alert Yaml File	PodCongested
Description	The pod congestion status is set to congested.

Table 5-39 (Cont.) POD_CONGESTED

Field	Details
Summary	Pod Congestion status of {{$labels.service}} service is congested
Severity	Critical
Expression	occnp_pod_congestion_state == 4
OID	1.3.6.1.4.1.323.5.3.36.1.2.26
Metric Used	occnp_pod_congestion_state
Recommended Actions	The alert gets cleared when the system is back to normal state. For any additional guidance, contact My Oracle Support.

5.1.1.39 POD_DANGER_OF_CONGESTION

Table 5-40 POD_DANGER_OF_CONGESTION

Field	Details
Description	The pod congestion status is set to Danger of Congestion.
Summary	Pod Congestion status of {{$labels.service}} service is DoC
Severity	Major
Expression	occnp_pod_resource_congestion_state == 1
OID	1.3.6.1.4.1.323.5.3.36.1.2.25
Metric Used	occnp_pod_congestion_state
Recommended Actions	The alert gets cleared when the system is back to normal state. For any additional guidance, contact My Oracle Support.

5.1.1.40 POD_PENDING_REQUEST_CONGESTED

Table 5-41 POD_PENDING_REQUEST_CONGESTED

Field	Details
Name in Alert Yaml File	PodPendingRequestCongested
Description	The pod congestion status is set to congested for PendingRequest.
Summary	Pod Resource Congestion status of {{$labels.service}} service is congested for PendingRequest type.
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="queue"} == 4
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	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.

5.1.1.41 POD_PENDING_REQUEST_DANGER_OF_CONGESTION

Table 5-42 POD_PENDING_REQUEST_DANGER_OF_CONGESTION

Field	Details
Description	The pod congestion status is set to DoC for pending requests.
Summary	Pod Resource Congestion status of {{$labels.service}} service is DoC for PendingRequest type.
Severity	Major
Expression	occnp_pod_resource_congestion_state{type="queue"} == 1
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	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.

5.1.1.42 POD_CPU_CONGESTED

Table 5-43 POD_CPU_CONGESTED

Field	Details
Name in Alert Yaml File	PodCPUCongested
Description	The pod congestion status is set to congested for CPU.
Summary	Pod Resource Congestion status of {{$labels.service}} service is congested for CPU type.
Severity	Critical
Expression	occnp_pod_resource_congestion_state{type="cpu"} == 4
OID	1.3.6.1.4.1.323.5.3.36.1.2.30
Metric Used	occnp_pod_resource_congestion_state{type="cpu"}
Recommended Actions	The alert gets cleared when the system CPU usage comes below the configured threshold value. For any additional guidance, contact My Oracle Support.

5.1.1.43 POD_CPU_DANGER_OF_CONGESTION

Table 5-44 POD_CPU_DANGER_OF_CONGESTION

Field	Details
Description	Pod Resource Congestion status of {{$labels.service}} service is DoC for CPU type.
Summary	Pod Resource Congestion status of {{$labels.service}} service is DoC for CPU type.
Severity	Major
Expression	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	occnp_pod_resource_congestion_state{type="cpu"}
Recommended Actions	The alert gets cleared when the system CPU usage comes below the configured threshold value. For any additional guidance, contact My Oracle Support.

5.1.1.44 SERVICE_OVERLOADED

Table 5-45 SERVICE_OVERLOADED

Field	Details
Description	Overload Level of {{$labels.service}} service is L1
Summary	Overload Level of {{$labels.service}} service is L1
Severity	Minor
Expression	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.

Table 5-46 SERVICE_OVERLOADED

Field	Details
Description	Overload Level of {{$labels.service}} service is L2
Summary	Overload Level of {{$labels.service}} service is L2
Severity	Major
Expression	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.

Table 5-47 SERVICE_OVERLOADED

Field	Details
Description	Overload Level of {{$labels.service}} service is L3
Summary	Overload Level of {{$labels.service}} service is L3
Severity	Critical
Expression	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.

5.1.1.45 SERVICE_RESOURCE_OVERLOADED

Alerts when service is in overload state due to memory usage

Table 5-48 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type

Table 5-48 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type
Severity	Minor
Expression	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.

Table 5-49 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type
Severity	Major
Expression	The overload level of the service is L2 due to 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.

Table 5-50 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type
Severity	Critical
Expression	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

Table 5-51 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type
Severity	Minor
Expression	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"}

Table 5-51 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
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.

Table 5-52 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type
Severity	Major
Expression	The overload level of the service is L2 due to CPU usage.
OID	1.3.6.1.4.1.323.5.3.36.1.2.41
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.

Table 5-53 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type
Severity	Critical
Expression	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

Table 5-54 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type
Severity	Minor
Expression	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.

Table 5-55 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type
Severity	Major
Expression	The overload level of the service is L2 due to 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.

Table 5-56 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type
Severity	Critical
Expression	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

Table 5-57 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L1 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L1 for {{$labels.type}} type.
Severity	Minor
Expression	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.

Table 5-58 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L2 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L2 for {{$labels.type}} type.
Severity	Major

Table 5-58 (Cont.) SERVICE_RESOURCE_OVERLOADED

Field	Details
Expression	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.

Table 5-59 SERVICE_RESOURCE_OVERLOADED

Field	Details
Description	{{$labels.service}} service is L3 for {{$labels.type}} type.
Summary	{{$labels.service}} service is L3 for {{$labels.type}} type.
Severity	Critical
Expression	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.

5.1.1.46 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD

Table 5-60 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the critical threshold limit for a given Subscriber Notification server
Summary	Transaction Error exceeds the critical threshold limit for a given Subscriber Notification server
Severity	Critical
Expression	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.

Table 5-61 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the major threshold limit for a given Subscriber Notification server
Summary	Transaction Error exceeds the major threshold limit for a given Subscriber Notification server

Table 5-61 (Cont.) SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Severity	Major
Expression	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.

Table 5-62 SUBSCRIBER_NOTIFICATION_ERROR_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	Notification Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server
Summary	Transaction Error exceeds the minor threshold limit for a given Subscriber Notification server
Severity	Minor
Expression	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.

5.1.1.47 SYSTEM_IMPAIRMENT_MAJOR

Table 5-63 SYSTEM_IMPAIRMENT_MAJOR

Field	Details
Description	Major impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage must be more than 80% for 10 minutes.
Summary	Major impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage must be more than 80% for 10 minutes.
Severity	Major
Expression	(db_tier_replication_status{role="failed"} == 0) or (db_tier_replication_status{role="active"} == 0) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="standby"})) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="failed"})) or (avg_over_time(db_tier_binlog_used_bytes_percentage[5m])>= 80)
OID	1.3.6.1.4.1.323.5.3.52.1.2.43
Metric Used	db_tier_replication_status and db_tier_binlog_used_bytes_percentage
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.48 SYSTEM_IMPAIRMENT_CRITICAL

Table 5-64 SYSTEM_IMPAIRMENT_CRITICAL

Field	Details
Description	Critical impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage must be more than 80% for 30 minutes.
Summary	Critical impairment alert raised for REPLICATION_FAILED or REPLICATION_CHANNEL_DOWN or BINLOG_STORAGE usage must be more than 80% for 30 minutes.
Severity	Critical
Expression	(db_tier_replication_status{role="failed"} == 0) or (db_tier_replication_status{role="active"} == 0) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="standby"})) or (count by (site_name) (db_tier_replication_status) == count by (site_name) (db_tier_replication_status{role="failed"})) or (avg_over_time(db_tier_binlog_used_bytes_percentage[5m])>= 80)
OID	1.3.6.1.4.1.323.5.3.52.1.2.43
Metric Used	db_tier_replication_status and db_tier_binlog_used_bytes_percentage
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.49 SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN

Table 5-65 SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN

Field	Details
Description	System Operational State is now in partial shutdown state.
Summary	System Operational State is now in partial shutdown state.
Severity	Major
Expression	system_operational_state == 2
OID	1.3.6.1.4.1.323.5.3.37.1.2.17
Metric Used	system_operational_state == 2
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.50 SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN

Table 5-66 SYSTEM_OPERATIONAL_COMPLETE_SHUTDOWN

Field	Details
Description	System Operational State is now in complete shutdown state
Summary	System Operational State is now in complete shutdown state
Severity	Critical
Expression	system_operational_state == 3
OID	1.3.6.1.4.1.323.5.3.37.1.2.17
Metric Used	system_operational_state

Table 5-66 (Cont.) SYSTEM_OPERATIONAL_COMPLETE_SHUTDOWN

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

5.1.1.51 TDF_CONNECTION_DOWN

Table 5-67 TDF_CONNECTION_DOWN

Field	Details
Description	TDF connection is down.
Summary	TDF connection is down.
Severity	Critical
Expression	occnp_diam_conn_app_network{applicationName="Sd"} == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.48
Metric Used	occnp_diam_conn_app_network
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.52 DIAM_CONN_PEER_DOWN

Table 5-68 DIAM_CONN_PEER_DOWN

Field	Details
Description	Diameter connection to peer {{ $labels.peerHost }} is down.
Summary	Diameter connection to peer is down.
Severity	Major
Expression	Diameter connection to peer peerHost in given namespace is down.
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.

5.1.1.53 DIAM_CONN_NETWORK_DOWN

Table 5-69 DIAM_CONN_NETWORK_DOWN

Field	Details
Description	All the diameter network connections are down.
Summary	All the diameter network connections are down.
Severity	Critical
Expression	sum by (kubernetes_namespace)(occnp_diam_conn_network) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.51
Metric Used	occnp_diam_conn_network
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.54 DIAM_CONN_BACKEND_DOWN

Table 5-70 DIAM_CONN_BACKEND_DOWN

Field	Details
Description	All the diameter backend connections are down.
Summary	All the diameter backend connections are down.
Severity	Critical
Expression	sum by (kubernetes_namespace)(occnp_diam_conn_backend) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.52
Metric Used	occnp_diam_conn_network
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.55 PerfInfoActiveOverloadThresholdFetchFailed

Table 5-71 PerfInfoActiveOverloadThresholdFetchFailed

Field	Details
Description	The application fails to get the current active overload level threshold data.
Summary	The application fails to get the current active overload level threshold data.
Severity	Major
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	For any additional guidance, contact My Oracle Support.

5.1.1.56 SLA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-72 SLA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	SLA Sy fail count exceeds the critical threshold limit
Summary	SLA Sy fail count exceeds the critical threshold limit
Severity	Critical
Condition	sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.58
Metric Used	occnp_diam_response_local_total
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.

5.1.1.57 SLA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-73 SLA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	SLA Sy fail count exceeds the major threshold limit
Summary	SLA Sy fail count exceeds the major threshold limit
Severity	Major
Condition	sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.58
Metric Used	occnp_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.

5.1.1.58 SLA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-74 SLA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	SLA Sy fail count exceeds the minor threshold limit
Summary	SLA Sy fail count exceeds the minor threshold limit
Severity	Minor
Condition	sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="SLA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SLA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.58
Metric Used	occnp_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.

5.1.1.59 STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-75 STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	STA Sy fail count exceeds the critical threshold limit.

Table 5-75 (Cont.) STA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Summary	STA Sy fail count exceeds the critical threshold limit.
Severity	Critical
Condition	The failure rate of Sy STA responses is more than 90% of the total responses.
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.59
Metric Used	occnp_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.

5.1.1.60 STA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-76 STA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	STA Sy fail count exceeds the major threshold limit.
Summary	STA Sy fail count exceeds the major threshold limit.
Severity	Major
Condition	The failure rate of Sy STA responses is more than 80% and less and or equal to 90% of the total responses.
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.59
Metric Used	occnp_diam_response_local_total
Recommended Actions	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.

5.1.1.61 STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-77 STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	STA Sy fail count exceeds the minor threshold limit.

Table 5-77 (Cont.) STA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Summary	STA 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	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777302"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.59
Metric Used	occnp_diam_response_local_total
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.

5.1.1.62 SMSC_CONNECTION_DOWN

Table 5-78 STASYFailCountExceedsCritcalThreshold

Field	Details
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)(occnp_active_smsc_conn_count) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.63
Metric Used	occnp_active_smsc_conn_count
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.

5.1.1.63 STA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-79 STASYFailCountExceedsCritcalThreshold

Field	Details
Description	STA Rx fail count exceeds the critical threshold limit.
Summary	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.

Table 5-79 (Cont.) STASYFailCountExceedsCritcalThreshold

Field	Details
Expression	sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.64
Metric Used	occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}
Recommended Actions	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.

5.1.1.64 STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-80 STA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	STA Rx fail count exceeds the major threshold limit.
Summary	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(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA", appId="16777236"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.64
Metric Used	occnp_diam_response_local_total{msgType="STA", appId="16777236", responseCode!~"2.*"}
Recommended Actions	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.

5.1.1.65 STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-81 STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	STA Rx fail count exceeds the minor threshold limit.

Table 5-81 (Cont.) STA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Summary	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.

5.1.1.66 SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-82 SNA_SY_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	SNA Sy fail count exceeds the critical threshold limit
Summary	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.

5.1.1.67 SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-83 SNA_SY_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	SNA Sy fail count exceeds the major threshold limit
Summary	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	sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 > 80 and sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 <= 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.65
Metric Used	occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}
Recommended Actions	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.

5.1.1.68 SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-84 SNA_SY_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	SNA Sy fail count exceeds the minor threshold limit
Summary	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	sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 > 60 and sum(rate(occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="SNA"}[5m])) * 100 <= 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.65
Metric Used	occnp_diam_response_local_total{msgType="SNA", responseCode!~"2.*"}
Recommended Actions	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.

5.1.1.69 STALE_DIAMETER_REQUEST_CLEANUP_MINOR

Table 5-85 STALE_DIAMETER_REQUEST_CLEANUP_MINOR

Field	Details
Description	This alerts is triggered when more than 10 % of the received Diameter requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	
Severity	Minor
Expression	
OID	
Metric Used	• ocpm_stale_diam_request_cleanup_total • occnp_diam_request_local_total
Recommended Actions	

5.1.1.70 STALE_DIAMETER_REQUEST_CLEANUP_MAJOR

Table 5-86 STALE_DIAMETER_REQUEST_CLEANUP_MAJOR

Field	Details
Description	This alert is triggered when more than 20 % of the received Diameter requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	
Severity	Major
Expression	
OID	
Metric Used	• ocpm_late_arrival_rejection_total • occnp_diam_request_local_total
Recommended Actions	

5.1.1.71 STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL

Table 5-87 STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	This alert is triggered when more than 30 % of the received Diameter requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	
Severity	Critical
Expression	
OID	
Metric Used	• ocpm_late_arrival_rejection_total • occnp_diam_request_local_total
Recommended Actions	

5.1.1.72 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

Table 5-88 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

Field	Details
Description	Certificate expiry in less than 6 months.
Summary	Certificate expiry in less than 6 months.
Severity	Minor
Condition	dgw_tls_cert_expiration_seconds - time() <= 15724800
OID	1.3.6.1.4.1.323.5.3.52.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.73 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR

Table 5-89 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR

Field	Details
Description	Certificate expiry in less than 3 months.
Summary	Certificate expiry in less than 3 months.
Severity	Major
Condition	dgw_tls_cert_expiration_seconds - time() <= 7862400
OID	1.3.6.1.4.1.323.5.3.52.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.74 DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

Table 5-90 DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

Field	Details
Description	Certificate expiry in less than 1 month.
Summary	Certificate expiry in less than 1 month.
Severity	Critical
Condition	dgw_tls_cert_expiration_seconds - time() <= 2592000
OID	1.3.6.1.4.1.323.5.3.52.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.75 DGW_TLS_CONNECTION_FAILURE

Table 5-91 DGW_TLS_CONNECTION_FAILURE

Field	Details
Description	Alert for TLS connection establishment.
Summary	TLS Connection failure when Diam gateway is an initiator.
Severity	Major
Condition	sum by (namespace,reason) (occnp_diam_failed_conn_network) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.81
Metric Used	occnp_diam_failed_conn_network
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.76 POLICY_CONNECTION_FAILURE

Table 5-92 POLICY_CONNECTION_FAILURE

Field	Details
Description	Connection failure on Egress and Ingress Gateways for incoming and outgoing connections.
Summary	Connection failure on Egress and Ingress Gateways for incoming and outgoing connections.
Severity	Major
Expression	sum(increase(occnp_oc_ingressgateway_connection_failure_total[5m]) >0 or (occnp_oc_ingressgateway_connection_failure_total unless occnp_oc_ingressgateway_connection_failure_total offset 5m)) by (namespace,app, error_reason) > 0 or sum(increase(occnp_oc_egressgateway_connection_failure_total[5m]) >0 or (occnp_oc_egressgateway_connection_failure_total unless occnp_oc_egressgateway_connection_failure_total offset 5m)) by (namespace,app, error_reason) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.76
Metric Used	occnp_oc_ingressgateway_connection_failure_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.77 AUDIT_NOT_RUNNING

Table 5-93 AUDIT_NOT_RUNNING

Field	Details
Description	Audit has not been running for at least 1 hour.
Summary	Audit has not been running for at least 1 hour.
Severity	CRITICAL
Expression	(absent_over_time(data_repository_invocations_seconds_count{method="getQueued TablesToAudit"}[1h]) == 1) OR (sum(increase(data_repository_invocations_seconds_count{method="getQueuedTabl esToAudit"}[1h])) == 0)
OID	1.3.6.1.4.1.323.5.3.52.1.2.78
Metric Used	data_repository_invocations_seconds_count
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.78 DIAMETER_POD_ERROR_RESPONSE_MINOR

Table 5-94 DIAMETER_POD_ERROR_RESPONSE_MINOR

Field	Details
Description	At least 1% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Summary	At least 1% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Severity	MINOR
Condition	(topk(1,((sort_desc(sum by (pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])))/ (sum by (pod) (rate(ocbsf_diam_response_network_total[2m])))) * 100))) >=1
OID	1.3.6.1.4.1.323.5.3.52.1.2.79
Metric Used	ocbsf_diam_response_network_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.79 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Table 5-95 DIAMETER_POD_ERROR_RESPONSE_MAJOR

Field	Details
Description	At least 5% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Summary	At least 5% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER.
Severity	MAJOR
Expression	(topk(1,((sort_desc(sum by (pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])))/ (sum by (pod) (rate(ocbsf_diam_response_network_total[2m])))) * 100))) >=5
OID	1.3.6.1.4.1.323.5.3.52.1.2.79

Table 5-95 (Cont.) DIAMETER_POD_ERROR_RESPONSE_MAJOR

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

5.1.1.80 DIAMETER_POD_ERROR_RESPONSE_CRITICAL

Table 5-96 DIAMETER_POD_ERROR_RESPONSE_CRITICAL

Field	Details
Description	At least 10% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER
Summary	At least 10% of the Diam Response connection requests failed with error DIAMETER_UNABLE_TO_DELIVER
Severity	CRITICAL
Expression	(topk(1,((sort_desc(sum by (pod) (rate(ocbsf_diam_response_network_total{responseCode="3002"}[2m])))/ (sum by (pod) (rate(ocbsf_diam_response_network_total[2m]))))) * 100))) >=10
OID	1.3.6.1.4.1.323.5.3.52.1.2.79
Metric Used	ocbsf_diam_response_network_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.81 LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Table 5-97 LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	lockAcquisitionExceedsCriticalThreshold
Description	The lock requests fails to acquire the lock count exceeds the critical threshold limit. The (current value is: {{ $value }})
Summary	Keys used in Bulwark lock request which are already in locked state detected above 75 Percent of Total Transactions.
Severity	Critical
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >=75
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total

Table 5-97 (Cont.) LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, above 75% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 75%.

5.1.1.82 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Table 5-98 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	lockAcquisitionExceedsMajorThreshold
Description	The lock requests fails to acquire the lock count exceeds the major threshold limit. The (current value is: {{ $value }})
Summary	Keys used in Bulwark lock request which are already in locked state detected above 50 Percent of Total Transactions.
Severity	Major

Table 5-98 (Cont.) LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, between 50% and 75% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 50%. If the rate exceeds 75%, a higher severity alert will trigger.

5.1.1.83 LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Table 5-99 LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	lockAcquisitionExceedsMinorThreshold
Description	The lock requests fails to acquire the lock count exceeds the minor threshold limit. The (current value is: {{ $value }})
Summary	Keys used in Bulwark lock request which are already in locked state detected above 20 Percent of Total Transactions.
Severity	Minor
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >=20 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total

Table 5-99 (Cont.) LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Field	Details
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, between 20% and 50% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 20%. If the rate exceeds 50%, a higher severity alert will trigger.

5.1.1.84 CERTIFICATE_EXPIRY_MINOR

Table 5-100 CERTIFICATE_EXPIRY_MINOR

Field	Details
Description	Certificate expiry in less than 6 months
Summary	Certificate expiry in less than 6 months
Severity	MINOR
Condition	security_cert_x509_expiration_seconds - time() <= 15724800
OID	1.3.6.1.4.1.323.5.3.52.1.2.77

Table 5-100 (Cont.) CERTIFICATE_EXPIRY_MINOR

Field	Details
Metric Used	-
Recommended Actions	-

5.1.1.85 CERTIFICATE_EXPIRY_MAJOR

Table 5-101 CERTIFICATE_EXPIRY_MAJOR

Field	Details
Description	Certificate expiry in less than 3 months
Summary	Certificate expiry in less than 3 months
Severity	MAJOR
Condition	security_cert_x509_expiration_seconds - time() <= 7862400
OID	1.3.6.1.4.1.323.5.3.52.1.2.77
Metric Used	-
Recommended Actions	-

5.1.1.86 CERTIFICATE_EXPIRY_CRITICAL

Table 5-102 CERTIFICATE_EXPIRY_CRITICAL

Field	Details
Description	Certificate expiry in less than 1 months
Summary	Certificate expiry in less than 1 months
Severity	CRITICAL
Condition	security_cert_x509_expiration_seconds - time() <= 2592000
OID	1.3.6.1.4.1.323.5.3.52.1.2.77
Metric Used	-
Recommended Actions	-

5.1.1.87 PERF_INFO_ACTIVE_OVERLOADTHRESHOLD_DATA_PRESENT

Table 5-103 PERF_INFO_ACTIVE_OVERLOADTHRESHOLD_DATA_PRESENT

Field	Details
Description	
Summary	
Severity	MINOR
Condition	active_overload_threshold_fetch_failed == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.53
Metric Used	
Recommended Actions	

5.1.1.88 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Table 5-104 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Description	More than 10% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 10% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MINOR
Condition	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m])))/(sum by (namespace) (rate(ocpm_userservice_inbound_count_total{service_resource="udr-service"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.85
Metric Used	-
Recommended Actions	-

5.1.1.89 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Table 5-105 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Description	More than 20% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 20% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MAJOR
Condition	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m])))/(sum by (namespace) (rate(ocpm_userservice_inbound_count_total{service_resource="udr-service"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m]))) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.85
Metric Used	-
Recommended Actions	-

5.1.1.90 UDR_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Table 5-106 UDR_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	More than 30% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 30% of incoming requests towards UDR-connector is rejected due to request being stale on arrival or during processing by the connector

Table 5-106 (Cont.) UDR_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Severity	CRITICAL
Condition	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="UDR-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m])))/(sum by (namespace) (rate(ocpm_userservice_inbound_count_total{service_resource="udr-service"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="UDR-C"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.85
Metric Used	-
Recommended Actions	-

5.1.1.91 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Table 5-107 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Description	More than 10% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 10% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MINOR
Condition	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m])))/(sum by (namespace) (rate(ocpm_userservice_inbound_count_total{service_resource="chf-service"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.86
Metric Used	-
Recommended Actions	-

5.1.1.92 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Table 5-108 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Description	More than 20% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 20% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	MAJOR
Condition	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m])))/(sum by (namespace) (rate(ocpm_userservice_inbound_count_total{service_resource="chf-service"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m]))) * 100 > 20

Table 5-108 (Cont.) CHF_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.86
Metric Used	-
Recommended Actions	-

5.1.1.93 CHF_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Table 5-109 CHF_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	More than 30% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Summary	More than 30% of incoming requests towards CHF-connector is rejected due to request being stale on arrival or during processing by the connector
Severity	CRITICAL
Condition	(sum by (namespace) (rate(occnp_late_processing_rejection_total{mode="CHF-C"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m])))/(sum by (namespace) (rate(ocpm_userservice_inbound_count_total{service_resource="chf-service"}[5m])) + sum by (namespace) (rate(occnp_late_arrival_rejection_total{mode="CHF-C"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.86
Metric Used	-
Recommended Actions	-

5.1.1.94 EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Table 5-110 EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Field	Details
Description	This alarm is raised when OCNADD is not reachable.
Summary	'kubernetes_namespace: {{$labels.kubernetes_namespace}}, timestamp: {{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}{{ end }} BSF Egress Gateway Data Director unreachable'
Severity	Major
Condition	This alarm is raised when data director is not reachable from Egress Gateway.
OID	1.3.6.1.4.1.323.5.3.37.1.2.48
Metric Used	oc_egressgateway_dd_unreachable
Recommended Actions	Alert gets cleared automatically when the connection with data director is established.

5.1.1.95 INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Table 5-111 INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Field	Details
Description	This alarm is raised when OCNADD is not reachable.
Summary	'kubernetes_namespace: {{$labels.kubernetes_namespace}}, timestamp: {{ with query "time()" }}{{ . | first | value | humanizeTimestamp }}{{ end }} BSF Ingress Gateway Data Director unreachable'
Severity	Major
Condition	This alarm is raised when data director is not reachable from Ingress Gateway.
OID	1.3.6.1.4.1.323.5.3.37.1.2.47
Metric Used	oc_ingressgateway_dd_unreachable
Recommended Actions	Alert gets cleared automatically when the connection with data director is established.

5.1.1.96 STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Table 5-112 STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	This alert is triggered when more than 30 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	-
Severity	Critical
Expression	-
OID	-
Metric Used	• ocpm_late_processing_rejection_total • occnp_diam_request_local_total
Recommended Actions	-

5.1.1.97 STALE_HTTP_REQUEST_CLEANUP_MAJOR

Table 5-113 STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Description	This alert is triggered when more than 20 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	-
Severity	Major
Expression	-
OID	-

Table 5-113 (Cont.) STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Metric Used	• ocpm_late_processing_rejection_total • occnp_diam_request_local_total
Recommended Actions	-

5.1.1.98 STALE_HTTP_REQUEST_CLEANUP_MINOR

Table 5-114 STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Description	This alert is triggered when more than 10 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	-
Severity	Minor
Expression	-
OID	-
Metric Used	• ocpm_late_processing_rejection_total • occnp_diam_request_local_total
Recommended Actions	-

5.1.1.99 STALE_BINDING_REQUEST_REJECTION_CRITICAL

Table 5-115 STALE_BINDING_REQUEST_REJECTION_CRITICAL

Field	Details
Description	This alert is triggered when more than 30 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	'{{ $value }} % of requests are being discarded by binding svc due to request being stale either on arrival or during processing.'summary: "More than 30% of the Binding requests failed with error TIMED_OUT_REQUEST"
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total {microservice=~".*binding"}[5m]))+sum by (namespace) rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m])))/(sum by (namespace) (rate(ocpm_binding_inbound_request_total{microservice=~".*binding"} [5m]))+sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.87
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_binding_inbound_request_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.100 STALE_BINDING_REQUEST_REJECTION_MAJOR

Table 5-116 STALE_BINDING_REQUEST_REJECTION_MAJOR

Field	Details
Description	This alert is triggered when more than 20 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	'{{ $value }} % of requests are being discarded by binding svc due to request being stale either on arrival or during processing.'summary: "More than 20% of the Binding requests failed with error TIMED_OUT_REQUEST"
Severity	Major
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total {microservice=~".*binding"}[5m]))+sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m])))/(sum by (namespace) (rate(ocpm_binding_inbound_request_total {microservice=~".*binding"} [5m]))+sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m]))) * 100 >= 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.87
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_binding_inbound_request_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.101 STALE_BINDING_REQUEST_REJECTION_MINOR

Table 5-117 STALE_BINDING_REQUEST_REJECTION_MINOR

Field	Details
Description	This alert is triggered when more than 10 % of the received HTTP requests are cancelled due to them being stale (received too late, or took too much time to process them).
Summary	'{{ $value }} % of requests are being discarded by binding service due to request being stale either on arrival or during processing.' summary: "More than 10% of the Binding requests failed with error TIMED_OUT_REQUEST"
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total {microservice=~".*binding"}[5m]))+sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"} [5m])))/(sum by (namespace) (rate(ocpm_binding_inbound_request_total {microservice=~".*binding"} [5m]))+sum by (namespace) (rate(occnp_late_arrival_rejection_total{microservice=~".*binding"}[5m]))) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.87
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_binding_inbound_request_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.1.102 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Table 5-118 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Description	At least 10 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Summary	At least 10 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Severity	Minor
Expression	-
OID	-
Metric Used	• `occnp_late_arrival_rejection_total` • `occnp_late_processing_rejection_total` • `ocpm_userservice_inbound_count_total`
Recommended Actions	-

5.1.1.103 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Table 5-119 UDR_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Description	At least 20 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Summary	At least 20 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Severity	Major
Expression	-
OID	-
Metric Used	• `occnp_late_arrival_rejection_total` • `occnp_late_processing_rejection_total` • `ocpm_userservice_inbound_count_total`
Recommended Actions	-

5.1.1.104 UDR_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Table 5-120 UDR_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	At least 30 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Summary	At least 30 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Severity	Critical
Expression	-
OID	-

Table 5-120 (Cont.) UDR_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_userservice_inbound_count_total
Recommended Actions	-

5.1.1.105 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Table 5-121 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MINOR

Field	Details
Description	At least 10 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Summary	At least 10 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Severity	Minor
Expression	-
OID	-
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_userservice_inbound_count_total
Recommended Actions	-

5.1.1.106 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Table 5-122 CHF_C_STALE_HTTP_REQUEST_CLEANUP_MAJOR

Field	Details
Description	At least 20 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Summary	At least 20 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Severity	Major
Expression	-
OID	-
Metric Used	• occnp_late_arrival_rejection_total • occnp_late_processing_rejection_total • ocpm_userservice_inbound_count_total
Recommended Actions	-

5.1.1.107 CHF_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Table 5-123 CHF_C_STALE_HTTP_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	At least 30 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Summary	At least 30 % of the received HTTP requests are cancelled per operation type due to them being stale (received too late, or took too much time to process them).
Severity	Critical
Expression	-
OID	-
Metric Used	• `occnp_late_arrival_rejection_total` • `occnp_late_processing_rejection_total` • `ocpm_userservice_inbound_count_total`
Recommended Actions	-

5.1.1.108 UPDATE_NOTIFY_TIMEOUT_ABOVE_70_PERCENT

Table 5-124 UPDATE_NOTIFY_TIMEOUT_ABOVE_70_PERCENT

Field	Details
Description	Number of Update Notify failed because a timeout is equal to or above 70% in a given time period.
Summary	Number of Update Notify failed because a timeout is equal to or above 70% in a given time period.
Severity	Critical
Condition	(sum by (namespace) (rate(**ocpm_handle_update_notify_timeout_for_rx_collision_total**{operationType="update_notify", microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(**occnp_http_out_conn_response_total**{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 70
OID	-
Metric Used	-
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.109 UPDATE_NOTIFY_TIMEOUT_ABOVE_50_PERCENT

Table 5-125 UPDATE_NOTIFY_TIMEOUT_ABOVE_50_PERCENT

Field	Details
Description	Number of Update Notify that failed because a timeout is equal to or above 50% but less than 70% in a given time period.

Table 5-125 (Cont.) UPDATE_NOTIFY_TIMEOUT_ABOVE_50_PERCENT

Field	Details
Summary	Number of Update Notify that failed because a timeout is equal to or above 50% but less than 70% in a given time period.
Severity	Major
Condition	(sum by (namespace) (rate(**ocpm_handle_update_notify_timeout_for_rx_collision_total**{operationType="update_notify", microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(**occnp_http_out_conn_response_total**{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 50 < 70
OID	-
Metric Used	-
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.110 UPDATE_NOTIFY_TIMEOUT_ABOVE_30_PERCENT

Table 5-126 UPDATE_NOTIFY_TIMEOUT_ABOVE_30_PERCENT

Field	Details
Description	Number of Update Notify that failed because a timeout is equal to or above 30% but less than 50% of total Rx sessions.
Summary	Number of Update Notify that failed because a timeout is equal to or above 30% but less than 50% of total Rx sessions.
Severity	Minor
Condition	(sum by (namespace) (rate(**ocpm_handle_update_notify_timeout_for_rx_collision_total**{operationType="update_notify", microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(**occnp_http_out_conn_response_total**{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 30 < 50
OID	-
Metric Used	-
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.111 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MINOR

Table 5-127 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MINOR

Field	Details
Description	If 30% to 50% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Summary	If 30% to 50% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Severity	Minor
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY",response!~"2.*"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY"}[5m]))) * 100 > 30 <= 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.129
Metric Used	occnp_policy_data_resubscription_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.112 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MAJOR

Table 5-128 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_MAJOR

Field	Details
Description	If 50% to 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Summary	If 50% to 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY",response!~"2.*"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY"}[5m]))) * 100 > 50 <= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.129
Metric Used	occnp_policy_data_resubscription_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.113 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_CRITICAL

Table 5-129 POLICYDS_PREEXPIRY_RESUBSCRIBE_FAILURE_CRITICAL

Field	Details
Description	If 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Summary	If 70% of subscriptions which are in PRE_EXPIRY period fail to resubscribe, this alert will be raised.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY",response!~"2.*"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_response_total{expiryStatus="PRE_EXPIRY"}[5m]))) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.129
Metric Used	occnp_policy_data_resubscription_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.114 POLICYDS_EXPIRED_SUBSCRIPTION

Table 5-130 POLICYDS_EXPIRED_SUBSCRIPTION

Field	Details
Description	If more than 10% of audited subscriptions are expired, this alert will be raised.
Summary	If more than 10% of audited subscriptions are expired, this alert will be raised.
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_request_total{expiryStatus="EXPIRED"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_policy_data_resubscription_request_total[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.130
Metric Used	occnp_policy_data_resubscription_request_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.1.115 LDAP_PEER_CONNECTION_LOST

Table 5-131 LDAP_PEER_CONNECTION_LOST

Field	Details
Name in Alert Yaml File	LDAP_PEER_CONNECTION_LOST

Table 5-131 (Cont.) LDAP_PEER_CONNECTION_LOST

Field	Details
Description	This alert is triggered when the LDAP Gateway loses connection to its LDAP peer(s). It is based on the value of the occnp_ldap_conn_total metric falling to zero. The connection re-attempt and alert clearance behavior is governed by a new configuration parameter, LDAP_CONNECTION_REVERT_DELAY.
Summary	LDAP Gateway loses connection to its LDAP peer(s).
Severity	major
Expression	sum by (namespace,peer)(occnp_ldap_conn_total) == 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.113
Metric Used	occnp_ldap_conn_total
Recommended Actions	• Verify that the LDAP server is running and connectivity between the PCF and LDAP peers is available. • If LDAP is reachable, check the configured **LDAP_CONNECTION_REVERT_DELAY** value since reconnection attempts and alert clearance depend on this setting.

5.1.1.116 IGW_POD_PROTECTION_DOC_STATE

Table 5-132 IGW_POD_PROTECTION_DOC_STATE

Field	Details
Description	The Ingress Gateway is in Danger_of_Congestion Level for the pod {{$labels.pod}} in namespace {{$labels.namespace}} (current congestion level: {{ $value }} %)
Summary	Ingress Gateway pod congestion state in Danger_of_Congestion Level.
Severity	Minor
Expression	oc_ingressgateway_congestion_system_state{microservice=~".*ingress-gateway"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.123
Metric Used	oc_ingressgateway_congestion_system_state
Recommended Actions	The alert is cleared when the pod CPU consumption dropped below the configured abatement value for the DOC level.

5.1.1.117 IGW_POD_PROTECTION_CONGESTED_STATE

Table 5-133 IGW_POD_PROTECTION_CONGESTED_STATE

Field	Details
Description	The Ingress Gateway is in Congested Level for the pod {{$labels.pod}} in namespace {{$labels.namespace}} (current congestion level: {{ $value }} %)
Summary	Ingress Gateway pod congestion state in Congested level.
Severity	Critical
Expression	sum(oc_ingressgateway_congestion_system_state{app_kubernetes_io_name="occnp-ingress-gateway"}) by (pod) == 4
OID	1.3.6.1.4.1.323.5.3.52.1.2.123
Metric Used	oc_ingressgateway_congestion_system_state

Table 5-133 (Cont.) IGW_POD_PROTECTION_CONGESTED_STATE

Field	Details
Recommended Actions	The alert is cleared when the pod CPU consumption dropped below the configured abatement value for the Congested level.

5.1.2 PCF Alerts

This section provides information on PCF alerts.

5.1.2.1 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Table 5-134 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Description	UDR returning with POST subscribe response but without user data for SM as part of immediate reporting occurring above 10% for service {{$labels.microservice}} in {{$labels.namespace}} (current value: {{ $value }} %)
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Severity	Minor
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.127
Metric Used	occnp_immrep_response_total

Table 5-134 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing SM user data check is based on: * `service_subresource = "sm-data"` (indicates the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `imm_reports_present = "false"` (indicates no SM user data was returned from UDR as part of the Immediate Reporting capability) – If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response without SM user data as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (e.g., `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved, inform the UDR operators to verify whether the Immediate Reporting feature is working and negotiated from their end.

Table 5-134 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.2 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Table 5-135 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.127
Metric Used	occnp_immrep_response_total

Table 5-135 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing SM user data check is based on: * `service_subresource = "sm-data"` (to indicate the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no SM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response **without** user data for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and still no SM user data is retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end.

Table 5-135 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.3 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Table 5-136 UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Description	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.127
Metric Used	occnp_immrep_response_total

Table 5-136 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing AM user data check is based on: * `service_subresource = "sm-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no SM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response **without** user data for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in the request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end.

Table 5-136 (Cont.) UDR_SM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.4 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Table 5-137 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Minor
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	occnp_immrep_response_total
Metric Used	1.3.6.1.4.1.323.5.3.52.1.2.128

Table 5-137 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation check is based on: * `service_subresource = "sm-data"` (to indicate the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end.

Table 5-137 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.5 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Table 5-138 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Major
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Table 5-138 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The failed feature negotiation check is based on: * `service_subresource = "sm-data"` (to indicate the UDR POST was to get SM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in the request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end.

Table 5-138 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
	Recovery: 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.6 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Table 5-139 UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Description	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Summary	More than 30% of the traffic, UDR returned with POST subscribe response but without user data for SM as part of immediate reporting.
Severity	Critical
Expression	(sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (microservice, namespace) (rate(occnp_immrep_response_total{service_subresource="sm-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.128
Metric Used	occnp_immrep_response_total

Table 5-139 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "sm-data"` (indicates the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `immediate_report_pcc = "false"` (indicates that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for SM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and SM user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is

Table 5-139 (Cont.) UDR_SM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
	working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.7 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MINOR

Table 5-140 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MINOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 10% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Summary	The Diameter requests are being discarded due to timeout processing occurring above 10% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Severity	Minor
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total{microservice=diam-connector}[5m]))) / (sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER", microservice=diam-connector}[5m]))) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.88
Metric Used	• `occnp_diam_request_local_total` • `occnp_stale_diam_request_cleanup_total`
Recommended Actions	The alert gets cleared when the number of stale requests is below 10% of the total requests. To troubleshoot and resolve the issue, perform the following steps: 1. Identify the root cause of the timeout processing by reviewing the logs for the pod {{$labels.pod}} and service {{$labels.microservice}} in {{$labels.namespace}}. 2. Verify the performance and resource utilization (CPU, memory) of the pod and make sure it has sufficient resources to process the requests in a timely manner. 3. Review the configuration settings of the Diameter connector and check timeout settings if necessary. 4. Ensure that the backend services that the Diameter connector communicates with are healthy and responsive. For further assistance, contact My Oracle Support.

5.1.2.8 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MAJOR

Table 5-141 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_MAJOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 20% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Summary	The Diameter requests are being discarded due to timeout processing occurring above 20% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Severity	Major
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total{microservice=diam-connector}[5m]))) / (sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER", microservice=diam-connector}[5m]))) * 100 >= 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.88
Metric Used	• `occnp_diam_request_local_total` • `occnp_stale_diam_request_cleanup_total`
Recommended Actions	The alert gets cleared when the number of stale requests is below 20% of the total requests. To troubleshoot and resolve the issue, perform the following steps: 1. Identify the root cause of the timeout processing by reviewing the logs for the pod {{$labels.pod}} and service {{$labels.microservice}} in {{$labels.namespace}}. 2. Verify the performance and resource utilization (CPU, memory) of the pod and make sure it has sufficient resources to process the requests in a timely manner. 3. Review the configuration settings of the Diameter connector and check timeout settings if necessary. 4. Ensure that the backend services that the Diameter connector communicates with are healthy and responsive. For further assistance, contact My Oracle Support.

5.1.2.9 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL

Table 5-142 STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 30% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Summary	The Diameter requests are being discarded due to timeout processing occurring above 30% inside pod {{$labels.pod}} for service {{$labels.microservice}} in {{$labels.namespace}}
Severity	Critical
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total{microservice=diam-connector}[5m]))) / (sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER", microservice=diam-connector}[5m]))) * 100 >= 30

Table 5-142 (Cont.) STALE_DIAMETER_CONNECTOR_REQUEST_CLEANUP_CRITICAL

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.88
Metric Used	• `occnp_diam_request_local_total` • `occnp_stale_diam_request_cleanup_total`
Recommended Actions	The alert gets cleared when the number of stale requests is below 30% of the total requests. To troubleshoot and resolve the issue, perform the following steps: 1. Identify the root cause of the timeout processing by reviewing the logs for the pod {{$labels.pod}} and service {{$labels.microservice}} in {{$labels.namespace}}. 2. Verify the performance and resource utilization (CPU, memory) of the pod and make sure it has sufficient resources to process the requests in a timely manner. 3. Review the configuration settings of the Diameter connector and check timeout settings if necessary. 4. Ensure that the backend services that the Diameter connector communicates with are healthy and responsive. For further assistance, contact My Oracle Support.

5.1.2.10 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_CRITICAL_THRESHOLD

Table 5-143 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	Number of revalidation responses indicated that the binding was missing, but restored from BSF. Overall valid sessions being audited is equal to or above 70% of the total revalidation responses.
Summary	Number of revalidation responses indicated that the binding was missing, but restored from BSF. Overall valid sessions being audited is equal to or above 70% of the total revalidation responses.
Severity	Critical
Condition	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code="2xx",action="restored"} [5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.89
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.11 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MAJOR_THRESHOLD

Table 5-144 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	Number of revalidation responses indicated that the binding was missing, but restored from BSF. Overall valid sessions being audited is equal or above 50% but less than 70% of total revalidation responses.
Summary	Number of revalidation responses indicated that the binding was missing, but restored from BSF. Overall valid sessions being audited is equal or above 50% but less than 70% of total revalidation responses.
Severity	Major
Condition	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code="2xx",action="restored"} [5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.89
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.12 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD

Table 5-145 SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	Number of revalidation responses indicated that the binding was missing, but restored from BSF. Overall valid sessions being audited is equal or above 30% but less than 50% of total revalidation responses.
Summary	Number of revalidation responses indicated that the binding was missing, but restored from BSF. Overall valid sessions being audited is equal or above 30% but less than 50% of total revalidation responses.
Severity	Minor

Table 5-145 (Cont.)
SESSION_BINDING_MISSING_FROM_BSF_EXCEEDS_MINOR_THRESHOLD

Field	Details
Condition	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx",action="restored"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding",response_code="2xx"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.89
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.13 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_CRITICAL_THRESHOLD

Table 5-146 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	Number of unsuccessful revalidation responses with error received from BSF, while in PCF the binding association is valid sessions is equal or above 70% of total revalidation responses.
Summary	Number of unsuccessful revalidation responses with error received from BSF, while in PCF the binding association is valid sessions is equal or above 70% of total revalidation responses.
Severity	Critical
Condition	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code!~"2.*"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.90
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	Verify the health condition of BSF Management Service. For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.14 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MAJOR_THRESHOLD

Table 5-147 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	Number of unsuccessful revalidation responses with error received from BSF, while in PCF the binding association is valid sessions is equal to or above 50% but less than 70% of total revalidation responses.
Summary	Number of unsuccessful revalidation responses with error received from BSF, while in PCF the binding association is valid sessions is equal to or above 50% but less than 70% of total revalidation responses.
Severity	Major
Condition	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code!~"2.*"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.90
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	Verify the health condition of BSF Management Service. For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.15 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MINOR_THRESHOLD

Table 5-148 SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	Number of unsuccessful revalidation responses with error received from BSF, while in PCF the binding association is valid sessions is equal to or above 30% but less than 50% of total revalidation responses.

Table 5-148 (Cont.) SESSION_BINDING_REVALIDATION_WITH_BSF_FAILURE_EXCEEDS_MINOR_THRESHOLD

Field	Details
Summary	Number of unsuccessful revalidation responses with error received from BSF, while in PCF the binding association is valid sessions is equal to or above 30% but less than 50% of total revalidation responses.
Severity	Minor
Condition	(sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding", response_code!~"2.*"}[5m])) /sum by (namespace) (rate(occnp_session_binding_revalidation_response_total{microservice=~".*binding"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.90
Metric Used	occnp_session_binding_revalidation_response_total
Recommended Actions	Verify the health condition of BSF Management Service. For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.16 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT

Table 5-149 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Description	when {{ $value }} % of primary key lookup fails during PA create in namespace {{$labels.namespace}}
Summary	Primary Key lookup failed is equal or above 10% but less than 50% of total PA create.
Severity	Minor
Expression	sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total{status="failed"}[30m])) / sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total[30m])) * 100 >= 10 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.124
Metric Used	occnp_optimized_smpolicyassociation_lookup_query_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.17 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT

Table 5-150 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Description	when {{ $value }} % of primary key lookup fails during PA create in namespace {{$labels.namespace}}
Summary	Primary Key lookup failed is equal or above 50% but less than 75% of total PA create.
Severity	Major
Expression	sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total{status="failed"}[30m])) / sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total[30m])) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.124
Metric Used	occnp_optimized_smpolicyassociation_lookup_query_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.18 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

Table 5-151 N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Description	when {{ $value }} % of primary key lookup fails during PA create in namespace {{$labels.namespace}}
Summary	Primary Key lookup failed is equal or above 75% of total PA create
Severity	Critical
Expression	sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total{status="failed"}[30m])) / sum by (namespace) (increase(occnp_optimized_smpolicyassociation_lookup_query_total[30m])) * 100 >= 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.124
Metric Used	occnp_optimized_smpolicyassociation_lookup_query_total

Table 5-151 (Cont.)
N7_OPTIMIZED_LOOKUP_ERROR_RATE_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.19 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MINOR

Table 5-152 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MINOR

Field	Details
Description	{{ $value }}% of incoming request towards pcf_sm service are rejected due to enhanced overload control mechanism
Summary	At least 10% of the received Requests have been rejected due to Overload state of pcf-sm service in namespace {{$labels.namespace}}
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_enhanced_overload_reject_total{microservice=~".*pcf_sm"}[2m])) / (sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0) + (sum by (namespace) (rate(session_oam_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0)))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.125
Metric Used	occnp_enhanced_overload_reject_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.20 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR

Table 5-153 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR

Field	Details
Description	{{ $value }}% of incoming request towards pcf_sm service are rejected due to enhanced overload control mechanism
Summary	At least 20% of the received Requests have been rejected due to Overload state of pcf-sm service in namespace {{$labels.namespace}}
Severity	Major

Table 5-153 (Cont.) SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_MAJOR

Field	Details
Expression	(sum by (namespace) (rate(occnp_enhanced_overload_reject_total{microservice=~".*pcf_sm"}[2m])) / (sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0) + (sum by (namespace) (rate(session_oam_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0)))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.125
Metric Used	occnp_enhanced_overload_reject_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.21 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_CRITICAL

Table 5-154 SM_SVC_REQ_ENHANCED_OVERLOAD_REJECTION_CRITICAL

Field	Details
Description	{{ $value }}% of incoming request towards pcf_sm service are rejected due to enhanced overload control mechanism
Summary	At least 30% of the received Requests have been rejected due to Overload state of pcf-sm service in namespace {{$labels.namespace}}.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_enhanced_overload_reject_total{microservice=~".*pcf_sm"}[2m])) / (sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0) + (sum by (namespace) (rate(session_oam_request_total{microservice=~".*pcf_sm"}[2m]) or occnp_enhanced_overload_reject_total * 0)))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.125
Metric Used	occnp_enhanced_overload_reject_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.1.2.22 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Table 5-155 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timer capacity has been occupied for n1n2 transfer failure notification
Summary	More than 70% of timer capacity has been occupied for n1n2 transfer failure notification
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2TransferFailure"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.107
Metric Used	occnp_timer_capacity

Table 5-155 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer failure notification reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer failure notification and possibly enable re-transmission. **Cause:** This alert indicates sustained high utilization of the UE N1N2 Transfer Failure Notification timer pool. The occnp_timer_capacity gauge tracks the current number of outstanding timers per timerName, updated every timer scan. • These timers are created when the UE cannot deliver URSP rules and the system initiates a reattempt flow using backoff with a timer. High utilization suggests many failures are triggering the N1N2 transfer failure notification flow. • The alert notifies when utilization for timerName "UE_N1N2TransferFailure" exceeds 70% of a baseline capacity of 360,000. Dimensions: timerName: UE_N1N2TransferFailure namespace: as per Prometheus label used in aggregation siteId: underlying metric label; rule aggregates with max by (namespace) **Diagnostic Information:** 1. **Validate the alert metric:** Inspect occnp_timer_capacity{timerName="UE_N1N2TransferFailure"} in Prometheus/Grafana (and /actuator/prometheus) and review trends around the alert window. 2. **Correlate with triggering failures:** Check for spikes in N1N2 transfer failure notifications and URSP delivery failures within the same time window. 3. **Review logs around the alert window:** In PCF-UE and related components/egress, look for errors leading to N1N2 transfer failure notifications; align timestamps with the alert period. 4. **Verify retransmission/backoff settings:** Ensure retransmission is enabled; confirm backoff parameters are appropriate (not overly conservative). 5. **Check downstream/egress health:** Validate connectivity and response health for AMF or upstream endpoints; look for elevated error rates/timeouts. 6. **Confirm processing throughput:** Verify rate_per_second for this timerName, worker thread health, and pod readiness/liveness; ensure backlog is draining. 7. **Watch for capacity rejections:** Observe occnp_timer_create_failure_total{timerName="UE_N1N2TransferFailure", errorCause="TIMER_CAPACITY_EXCEEDS"} for signs of hard-cap hits. **Recovery:** 1. **Resolve underlying failures:**

Table 5-155 (Cont.) AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MINOR_THRESHOLD

Field	Details
	Work with upstream/AMF and correct misconfigurations causing the flow to trigger N1N2 transfer failure notifications at high rates. 2. **Enable or optimize retransmission:** Turn on retransmission if disabled; tune backoff to improve success while avoiding downstream overload. 3. **Increase draining capacity:** Temporarily raise rate_per_second and/or scale pods to drain outstanding timers faster. 4. **Adjust capacity if needed:** Temporarily increase the registered timer_capacity baseline for this timerName while addressing root causes. 5. **Reduce new load temporarily:** Throttle or defer non-critical timer creates for this timerName until utilization drops. 6. **Monitor until recovered:** Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold.

5.1.2.23 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Table 5-156 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for n1n2 transfer failure notification
Summary	More than 80% of timer capacity has been occupied for n1n2 transfer failure notification
Severity	Major
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2TransferFailure"})/360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.107
Metric Used	occnp_timer_capacity

Table 5-156 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer failure notification reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer failure notification and possibly enable re-transmission. **Cause:** This alert indicates sustained high utilization of the UE N1N2 Transfer Failure Notification timer pool. The occnp_timer_capacity gauge tracks the current number of outstanding timers per timerName, updated every timer scan. - These timers are created when the UE cannot deliver URSP rules and the system initiates a reattempt flow using backoff with a timer. High utilization suggests many failures are triggering the N1N2 transfer failure notification flow. - The alert notifies when utilization for timerName "UE_N1N2TransferFailure" exceeds 80% of a baseline capacity of 360000. Dimensions: timerName : UE_N1N2TransferFailure namespace : as per Prometheus label used in aggregation siteId : underlying metric label; rule aggregates with max by (namespace) **Diagnostic Information :** 1. **Validate the alert metric:** Inspect occnp_timer_capacity{timerName="UE_N1N2TransferFailure"} in Prometheus/Grafana (and /actuator/prometheus) and review trends around the alert window. 2. **Correlate with triggering failures:** Check for spikes in N1N2 transfer failure notifications and URSP delivery failures within the same time window. 3. **Review logs around the alert window:** In PCF-UE and related components/egress, look for errors leading to N1N2 transfer failure notifications; align timestamps with the alert period. 4. **Verify retransmission/backoff settings:** Ensure retransmission is enabled; confirm backoff parameters are appropriate (not overly conservative). 5. **Check downstream/egress health:** Validate connectivity and response health for AMF or upstream endpoints; look for elevated error rates/timeouts. 6. **Confirm processing throughput:** Verify rate_per_second for this timerName, worker thread health, and pod readiness/liveness; ensure backlog is draining. 7. **Watch for capacity rejections:** Observe occnp_timer_create_failure_total{timerName="UE_N1N2TransferFailure",errorCause="TIMER_CAPACITY_EXCEEDS"} for signs of hard-cap hits. **Recovery :**

Table 5-156 (Cont.) AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_MAJOR_THRESHOLD

Field	Details
	1. **Resolve underlying failures:** Work with upstream/AMF and correct misconfigurations causing the flow to trigger N1N2 transfer failure notifications at high rates. 2. **Enable or optimize retransmission:** Turn on retransmission if disabled; tune backoff to improve success while avoiding downstream overload. 3. **Increase draining capacity:** Temporarily raise rate_per_second and/or scale pods to drain outstanding timers faster. 4. **Adjust capacity if needed:** Temporarily increase the registered timer_capacity baseline for this timerName while addressing root causes. 5. **Reduce new load temporarily:** Throttle or defer non-critical timer creates for this timerName until utilization drops. 6. **Monitor until recovered:** Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold.

5.1.2.24 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Table 5-157 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD
Description	More than 90% of timer capacity has been occupied for n1n2 transfer failure notification
Summary	More than 90% of timer capacity has been occupied for n1n2 transfer failure notification
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2TransferFailure"})/360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.107
Metric Used	occnp_timer_capacity

Table 5-157 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer failure notification reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer failure notification and possibly enable re-transmission. **Cause:** This alert indicates sustained high utilization of the UE N1N2 Transfer Failure Notification timer pool. The occnp_timer_capacity gauge tracks the current number of outstanding timers per timerName, updated every timer scan. - These timers are created when the UE cannot deliver URSP rules and the system initiates a reattempt flow using backoff with a timer. High utilization suggests many failures are triggering the N1N2 transfer failure notification flow. - The alert notifies when utilization for timerName "UE_N1N2TransferFailure" exceeds 90% of a baseline capacity of 360000. Dimensions: timerName : UE_N1N2TransferFailure namespace : as per Prometheus label used in aggregation siteId : underlying metric label; rule aggregates with max by (namespace) **Diagnostic Information :** 1. **Validate the alert metric:** Inspect occnp_timer_capacity{timerName="UE_N1N2TransferFailure"} in Prometheus/Grafana (and /actuator/prometheus) and review trends around the alert window. 2. **Correlate with triggering failures:** Check for spikes in N1N2 transfer failure notifications and URSP delivery failures within the same time window. 3. **Review logs around the alert window:** In PCF-UE and related components/egress, look for errors leading to N1N2 transfer failure notifications; align timestamps with the alert period. 4. **Verify retransmission/backoff settings:** Ensure retransmission is enabled; confirm backoff parameters are appropriate (not overly conservative). 5. **Check downstream/egress health:** Validate connectivity and response health for AMF or upstream endpoints; look for elevated error rates/timeouts. 6. **Confirm processing throughput:** Verify rate_per_second for this timerName, worker thread health, and pod readiness/liveness; ensure backlog is draining. 7. **Watch for capacity rejections:** Observe occnp_timer_create_failure_total{timerName="UE_N1N2TransferFailure",errorCause="TIMER_CAPACITY_EXCEEDS"} for signs of hard-cap hits. **Recovery :**

Table 5-157 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_ABOVE_CRITICAL_THRESHOLD

Field	Details
	1. **Resolve underlying failures:** Work with upstream/AMF and correct misconfigurations causing the flow to trigger N1N2 transfer failure notifications at high rates. 2. **Enable or optimize retransmission:** Turn on retransmission if disabled; tune backoff to improve success while avoiding downstream overload. 3. **Increase draining capacity:** Temporarily raise rate_per_second and/or scale pods to drain outstanding timers faster. 4. **Adjust capacity if needed:** Temporarily increase the registered timer_capacity baseline for this timerName while addressing root causes. 5. **Reduce new load temporarily:** Throttle or defer non-critical timer creates for this timerName until utilization drops. 6. **Monitor until recovered:** Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold.

5.1.2.25 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD

Table 5-158 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timers capacity has been occupied for amf discovery.
Summary	More than 70% of timers capacity has been occupied for amf discovery.
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_AMFDiscovery"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.95
Metric Used	occnp_timer_capacity

Table 5-158 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to AMF discovery reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with NRF discovery and possibly enable direct or indirect alternate routing from NRF client. **Cause:** More than 70% of timer capacity has been occupied for AMF discovery. The `occnp_timer_capacity` metric records the current timer count. These timers are created when the User Equipment (UE) cannot deliver URSP rules, retries with a back-off, and creates a timer. This alert is triggered when capacity for timers corresponding to AMF Discovery reaches a certain percent (over 70%) of the total 360K capacity. **Diagnostic Information:** • **High Rate of UE Failures**: Many User Equipment (UE) devices are unable to deliver URSP (User Route Selection Policy) rules, causing increased retries and timer creation for AMF discovery. • **Network Function (NRF or AMF) Issues**: Problems or instability with the AMF (Access and Mobility Management Function) or related NRF (Network Repository Function) components might prevent successful discovery or rule delivery, resulting in more timer retries. • **Resource Bottlenecks**: Network resource constraints or congestion could delay or prevent successful URSP rule delivery, again resulting in repeated retries and high timer usage. • **Excessively Short Timer Values**: If the back-off or retry timers are set too short, UEs may repeat attempts too rapidly, compounding timer consumption. **Recovery:** • Review the logs and monitor for trends in UE failures with AMF discovery. • Consider enabling direct or indirect alternate routing from the NRF-client to mitigate timer capacity issues. • Investigate any recent configuration or software changes, check for network health (especially AMF and NRF), and verify timer-related configurations. • If the issue persists, please check with Support team.

5.1.2.26 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD

Table 5-159 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for amf discovery.
Summary	More than 80% of timer capacity has been occupied for amf discovery.
Severity	Major

Table 5-159 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_MAJOR_THRESHOLD

Field	Details
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_AMFDiscovery"})/ 360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.95
Metric Used	occnp_timer_capacity
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to AMF discovery reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with NRF discovery and possibly enable direct or indirect alternate routing from NRF client. **Cause:** More than 80% of timer capacity has been occupied for AMF discovery. The `occnp_timer_capacity` metric records the current timer count. These timers are created when the User Equipment (UE) cannot deliver URSP rules, retries with a back-off, and creates a timer. This alert is triggered when capacity for timers corresponding to AMF Discovery reaches a certain percent (over 80%) of the total 360K capacity. **Diagnostic Information:** • **High Rate of UE Failures**: Many User Equipment (UE) devices are unable to deliver URSP (User Route Selection Policy) rules, causing increased retries and timer creation for AMF discovery. • **Network Function (NRF or AMF) Issues**: Problems or instability with the AMF (Access and Mobility Management Function) or related NRF (Network Repository Function) components might prevent successful discovery or rule delivery, resulting in more timer retries. • **Resource Bottlenecks**: Network resource constraints or congestion could delay or prevent successful URSP rule delivery, again resulting in repeated retries and high timer usage. • **Excessively Short Timer Values**: If the back-off or retry timers are set too short, UEs may repeat attempts too rapidly, compounding timer consumption. **Recovery:** • Review the logs and monitor for trends in UE failures with AMF discovery. • Consider enabling direct or indirect alternate routing from the NRF-client to mitigate timer capacity issues. • Investigate any recent configuration or software changes, check for network health (especially AMF and NRF), and verify timer-related configurations. • If the issue persists, please check with Support team.

5.1.2.27 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Table 5-160 AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Table 5-160 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_AMF_DISCOVERY_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	More than 90% of timer capacity has been occupied for amf discovery.
Summary	More than 90% of timer capacity has been occupied for amf discovery.
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_AMFDiscovery"})/ 360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.95
Metric Used	occnp_timer_capacity
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to AMF discovery reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with NRF discovery and possibly enable direct or indirect alternate routing from NRF client. **Cause:** More than 90% of timer capacity has been occupied for AMF discovery. The `occnp_timer_capacity` metric records the current timer count. These timers are created when the User Equipment (UE) cannot deliver URSP rules, retries with a back-off, and creates a timer. This alert is triggered when capacity for timers corresponding to AMF Discovery reaches a certain percent (over 90%) of the total 360K capacity. **Diagnostic Information:** • **High Rate of UE Failures**: Many User Equipment (UE) devices are unable to deliver URSP (User Route Selection Policy) rules, causing increased retries and timer creation for AMF discovery. • **Network Function (NRF or AMF) Issues**: Problems or instability with the AMF (Access and Mobility Management Function) or related NRF (Network Repository Function) components might prevent successful discovery or rule delivery, resulting in more timer retries. • **Resource Bottlenecks**: Network resource constraints or congestion could delay or prevent successful URSP rule delivery, again resulting in repeated retries and high timer usage. • **Excessively Short Timer Values**: If the back-off or retry timers are set too short, UEs may repeat attempts too rapidly, compounding timer consumption. **Recovery:** • Review the logs and monitor for trends in UE failures with AMF discovery. • Consider enabling direct or indirect alternate routing from the NRF-client to mitigate timer capacity issues. • Investigate any recent configuration or software changes, check for network health (especially AMF and NRF), and verify timer-related configurations. • If the issue persists, please check with Support team.

5.1.2.28 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD

Table 5-161 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timer capacity has been occupied for n1n2 subscribe.
Summary	More than 70% of timer capacity has been occupied for n1n2 subscribe.
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageSubscribe"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.96
Metric Used	occnp_timer_capacity

Table 5-161 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 subscribe reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 subscription or on the AMF side and possibly enable the direct/indirect alternate routing. **Cause:** More than 70% of timer capacity has been occupied for N1N2 subscription. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after back-off, and creates a new timer. This alert is triggered when timer capacity for N1N2 subscription exceeds 70% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Subscription Flows:** Multiple User Equipment (UE) devices may be repeatedly failing to complete N1N2 subscription actions, resulting in retries and new timer creations. • **Persistent Delivery or Communication Issues:** Failures in delivering URSP rules or problems communicating with the AMF or other network functions might cause UEs to retrigger the N1N2 subscription flow. • **Underlying AMF or Network Instability:** Instability, health issues, or misconfigurations in the AMF (Access and Mobility Management Function) could prevent successful subscription completion, leading to increased timers. • **High Traffic Volume or Spikes:** Unexpectedly high volumes of N1N2 subscription requests can cause a large number of timers to be in use concurrently. • **Resource Limitations or Performance Bottlenecks:** Processing delays or resource bottlenecks (CPU, memory, network) within the UE-service or supporting backend could slow down or block subscription handling, causing timers to accumulate. • **Improper Timer or Retry Configuration:** Short retry intervals or misconfigured back-off could lead to rapid, repeated subscription attempts and excessive timer usage. **Recovery:** • Review logs and N1N2 subscription flow metrics for unusual error patterns. • Investigate AMF and related network function health and recent changes. • Check configuration for timer parameters and adjust if necessary. • Monitor for spikes in traffic or unusual load patterns. • If the issue persists, please check with Support team.

5.1.2.29 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD

Table 5-162 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for n1n2 subscribe.
Summary	More than 80% of timer capacity has been occupied for n1n2 subscribe.
Severity	Major
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageSubscribe"})/360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.96
Metric Used	occnp_timer_capacity

Table 5-162 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 subscribe reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 subscription or on the AMF side and possibly enable the direct/indirect alternate routing. **Cause:** More than 80% of timer capacity has been occupied for N1N2 subscription. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after back-off, and creates a new timer. This alert is triggered when timer capacity for N1N2 subscription exceeds 80% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Subscription Flows:** Multiple User Equipment (UE) devices may be repeatedly failing to complete N1N2 subscription actions, resulting in retries and new timer creations. • **Persistent Delivery or Communication Issues:** Failures in delivering URSP rules or problems communicating with the AMF or other network functions might cause UEs to retrigger the N1N2 subscription flow. • **Underlying AMF or Network Instability:** Instability, health issues, or misconfigurations in the AMF (Access and Mobility Management Function) could prevent successful subscription completion, leading to increased timers. • **High Traffic Volume or Spikes:** Unexpectedly high volumes of N1N2 subscription requests can cause a large number of timers to be in use concurrently. • **Resource Limitations or Performance Bottlenecks:** Processing delays or resource bottlenecks (CPU, memory, network) within the UE-service or supporting backend could slow down or block subscription handling, causing timers to accumulate. • **Improper Timer or Retry Configuration:** Short retry intervals or misconfigured back-off could lead to rapid, repeated subscription attempts and excessive timer usage. **Recovery:** • Review logs and N1N2 subscription flow metrics for unusual error patterns. • Investigate AMF and related network function health and recent changes. • Check configuration for timer parameters and adjust if necessary. • Monitor for spikes in traffic or unusual load patterns. • If the issue persists, please check with Support team.

5.1.2.30 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD

Table 5-163 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD
Description	More than 90% of timer capacity has been occupied for n1n2 subscribe.
Summary	More than 90% of timer capacity has been occupied for n1n2 subscribe.
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageSubscribe"})/360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.96
Metric Used	occnp_timer_capacity

Table 5-163 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_SUBSCRIBE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 subscribe reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 subscription or on the AMF side and possibly enable the direct/indirect alternate routing. **Cause:** More than 90% of timer capacity has been occupied for N1N2 subscription. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after back-off, and creates a new timer. This alert is triggered when timer capacity for N1N2 subscription exceeds 90% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Subscription Flows:** Multiple User Equipment (UE) devices may be repeatedly failing to complete N1N2 subscription actions, resulting in retries and new timer creations. • **Persistent Delivery or Communication Issues:** Failures in delivering URSP rules or problems communicating with the AMF or other network functions might cause UEs to retrigger the N1N2 subscription flow. • **Underlying AMF or Network Instability:** Instability, health issues, or misconfigurations in the AMF (Access and Mobility Management Function) could prevent successful subscription completion, leading to increased timers. • **High Traffic Volume or Spikes:** Unexpectedly high volumes of N1N2 subscription requests can cause a large number of timers to be in use concurrently. • **Resource Limitations or Performance Bottlenecks:** Processing delays or resource bottlenecks (CPU, memory, network) within the UE-service or supporting backend could slow down or block subscription handling, causing timers to accumulate. • **Improper Timer or Retry Configuration:** Short retry intervals or misconfigured back-off could lead to rapid, repeated subscription attempts and excessive timer usage. **Recovery:** • Review logs and N1N2 subscription flow metrics for unusual error patterns. • Investigate AMF and related network function health and recent changes. • Check configuration for timer parameters and adjust if necessary. • Monitor for spikes in traffic or unusual load patterns. If the issue persists, please check with Support team.

5.1.2.31 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD

Table 5-164 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD
Description	More than 70% of timer capacity has been occupied for n1n2 transfer.
Summary	More than 70% of timer capacity has been occupied for n1n2 transfer.
Severity	Minor
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageTransfer"})/360000) * 100 > 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.97
Metric Used	occnp_timer_capacity

Table 5-164 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer subscribe reaches 70% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer and possibly enable direct/ indirect alternate routing. **Cause:** More than 70% of timer capacity has been occupied for N1N2 transfer. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after a back-off, and creates a new timer. This alert is triggered when the timer capacity for N1N2 transfer exceeds 70% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Transfer Flows:** Many User Equipment (UE) devices are failing to complete N1N2 transfer operations successfully. Each failure leads to retries and the creation of new timers. • **Delivery or Communication Issues:** Persistent network issues preventing successful URSP rule delivery or failures in communication between the UE, AMF (Access and Mobility Management Function), or other relevant network functions can result in repeated N1N2 transfer attempts. • **Resource Constraints or Performance Bottlenecks:** Limited processing resources, high latency, or overload conditions (e.g., CPU/memory/network contention) can slow down or block the completion of transfer requests, causing timers to accumulate. • **High Volume of Requests:** An increased volume of N1N2 transfer requests due to network events or abnormal UE behavior can lead to a rapid consumption of available timer capacity. • **Improper Timer Configuration:** Short back-off intervals or aggressive retry settings can cause repeated rapid reattempts, increasing the number of concurrent timers. • **AMF or Other NF Instability:** Outages or instability in the AMF or related network functions may cause requests to go unprocessed, triggering continual retries from UEs. **Recovery:** • Review recent logs and metrics related to N1N2 transfer failures. • Investigate the health status of the AMF and other supporting NFs. • Check resource utilization and adjust timer back-off/retry configuration if needed. • Look for recent network changes or spikes in request volume. If the issue persists, please check with Support team.

5.1.2.32 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD

Table 5-165 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD
Description	More than 80% of timer capacity has been occupied for n1n2 transfer.
Summary	More than 80% of timer capacity has been occupied for n1n2 transfer.
Severity	Major
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageTransfer"})/360000) * 100 > 80
OID	1.3.6.1.4.1.323.5.3.52.1.2.97
Metric Used	occnp_timer_capacity

Table 5-165 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer subscribe reaches 80% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer and possibly enable direct/ indirect alternate routing. **Cause:** More than 80% of timer capacity has been occupied for N1N2 transfer. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after a back-off, and creates a new timer. This alert is triggered when the timer capacity for N1N2 transfer exceeds 80% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Transfer Flows:** Many User Equipment (UE) devices are failing to complete N1N2 transfer operations successfully. Each failure leads to retries and the creation of new timers. • **Delivery or Communication Issues:** Persistent network issues preventing successful URSP rule delivery or failures in communication between the UE, AMF (Access and Mobility Management Function), or other relevant network functions can result in repeated N1N2 transfer attempts. • **Resource Constraints or Performance Bottlenecks:** Limited processing resources, high latency, or overload conditions (e.g., CPU/memory/network contention) can slow down or block the completion of transfer requests, causing timers to accumulate. • **High Volume of Requests:** An increased volume of N1N2 transfer requests due to network events or abnormal UE behavior can lead to a rapid consumption of available timer capacity. • **Improper Timer Configuration:** Short back-off intervals or aggressive retry settings can cause repeated rapid reattempts, increasing the number of concurrent timers. • **AMF or Other NF Instability:** Outages or instability in the AMF or related network functions may cause requests to go unprocessed, triggering continual retries from UEs. **Recovery:** • Review recent logs and metrics related to N1N2 transfer failures. • Investigate the health status of the AMF and other supporting NFs. • Check resource utilization and adjust timer back-off/retry configuration if needed. • Look for recent network changes or spikes in request volume. If the issue persists, please check with Support team.

5.1.2.33 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD

Table 5-166 AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD
Description	More than 90% of timer capacity has been occupied for n1n2 transfer.
Summary	More than 90% of timer capacity has been occupied for n1n2 transfer.
Severity	Critical
Expression	(max by (namespace) (occnp_timer_capacity{timerName="UE_N1N2MessageTransfer"})/360000) * 100 > 90
OID	1.3.6.1.4.1.323.5.3.52.1.2.97
Metric Used	occnp_timer_capacity

Table 5-166 (Cont.)
AUDIT_TIMER_CAPACITY_FOR_UE_N1N2_TRANSFER_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_timer_capacity` metric is pegged during each timer scan, providing the current timers count. These timers were created when UE was not able to deliver the URSP rules and reattempt with back off. In this scenario an alert is triggered when the timers capacity corresponding to N1N2 transfer subscribe reaches 90% of the maximum rate limit of 360K. In this case the operator can troubleshoot and identify the reasons for failures with the flow triggering N1N2 transfer and possibly enable direct/ indirect alternate routing. **Cause:** More than 90% of timer capacity has been occupied for N1N2 transfer. The `occnp_timer_capacity` metric tracks the current count of active timers. These timers are created when the User Equipment (UE) fails to deliver URSP rules, retries after a back-off, and creates a new timer. This alert is triggered when the timer capacity for N1N2 transfer exceeds 90% of the total 360K capacity. **Diagnostic Information:** • **Frequent UE Failures in N1N2 Transfer Flows:** Many User Equipment (UE) devices are failing to complete N1N2 transfer operations successfully. Each failure leads to retries and the creation of new timers. • **Delivery or Communication Issues:** Persistent network issues preventing successful URSP rule delivery or failures in communication between the UE, AMF (Access and Mobility Management Function), or other relevant network functions can result in repeated N1N2 transfer attempts. • **Resource Constraints or Performance Bottlenecks:** Limited processing resources, high latency, or overload conditions (e.g., CPU/memory/network contention) can slow down or block the completion of transfer requests, causing timers to accumulate. • **High Volume of Requests:** An increased volume of N1N2 transfer requests due to network events or abnormal UE behavior can lead to a rapid consumption of available timer capacity. • **Improper Timer Configuration:** Short back-off intervals or aggressive retry settings can cause repeated rapid reattempts, increasing the number of concurrent timers. • **AMF or Other NF Instability:** Outages or instability in the AMF or related network functions may cause requests to go unprocessed, triggering continual retries from UEs. **Recovery:** • Review recent logs and metrics related to N1N2 transfer failures. • Investigate the health status of the AMF and other supporting NFs. • Check resource utilization and adjust timer back-off/retry configuration if needed. • Look for recent network changes or spikes in request volume. If the issue persists, please check with Support team.

5.1.2.34 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 5-167 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of n1n2 subscribe reattempt failed.

Table 5-167 (Cont.) UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Summary	More than 25% of n1n2 subscribe reattempt failed.
Severity	Minor
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",operationType="subscribe",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",operationType="subscribe"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.99
Metric Used	http_out_conn_response_total, http_out_conn_request_total
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 subscribe. If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 subscription is failing or if the AMF that request are going to is unhealthy. **Cause:** An elevated percentage of reattempt failures has been detected for UE N1N2 subscriptions. The `http_out_conn_response_total` metric increments whenever the PCF-UE receives a response for outbound messages, specifically tracking reattempts where the operation type is "subscribe" and the response code is not in the 2xx (success) range. This alert triggers when more than 25% of such reattempts fail over a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** The target AMF may be experiencing outages, heavy load, or is otherwise unhealthy, causing it to reject or fail to respond to subscription requests. • **Network Issues or Communication Failures:** Network congestion, routing problems, or transient communication errors may prevent successful delivery of N1N2 subscription requests or receipt of responses. • **Configuration Errors:** Misconfiguration of endpoints (such as incorrect URLs, authentication, or authorization settings) may cause subscription requests to be rejected or fail. • **High Load or Resource Exhaustion:** If the AMF or intermediate network components are overloaded or have run out of necessary resources (e.g., memory, threads, process slots), reattempted requests may be rejected. • **Timeouts or Latency Issues:** Prolonged delays in response times could cause requests to time out, leading to apparent failures. **Recovery:** • Review logs and error codes for patterns or specific failure reasons. • Check the health and recent activity of the AMF(s) and relevant network paths. • Examine configuration settings related to N1N2 subscriptions and ensure they are correct. • Investigate any spikes in load or indications of resource bottlenecks. • Correlate with recent changes or deployments in the environment. If the issue persists, please check with Support team.

5.1.2.35 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 5-168 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of n1n2 subscribe reattempt failed.
Summary	More than 50% of n1n2 subscribe reattempt failed.
Severity	Major
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",operationType="subscribe",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",operationType="subscribe"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.99
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Table 5-168 (Cont.) UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 subscribe.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 subscription is failing or if the AMF that request are going to is unhealthy. **Cause:** An elevated percentage of reattempt failures has been detected for UE N1N2 subscriptions. The `http_out_conn_response_total` metric increments whenever the PCF-UE receives a response for outbound messages, specifically tracking reattempts where the operation type is "subscribe" and the response code is not in the 2xx (success) range. This alert triggers when more than 50% of such reattempts fail over a 5-minute period. **Diagnostic Information:** **AMF (Access and Mobility Management Function) Unavailability or Instability:** The target AMF may be experiencing outages, heavy load, or is otherwise unhealthy, causing it to reject or fail to respond to subscription requests. **Network Issues or Communication Failures:** Network congestion, routing problems, or transient communication errors may prevent successful delivery of N1N2 subscription requests or receipt of responses. **Configuration Errors:** Misconfiguration of endpoints (such as incorrect URLs, authentication, or authorization settings) may cause subscription requests to be rejected or fail. **High Load or Resource Exhaustion:** If the AMF or intermediate network components are overloaded or have run out of necessary resources (e.g., memory, threads, process slots), reattempted requests may be rejected. • **Timeouts or Latency Issues:**Prolonged delays in response times could cause requests to time out, leading to apparent failures. **Recovery:** • Review logs and error codes for patterns or specific failure reasons. • Check the health and recent activity of the AMF(s) and relevant network paths. • Examine configuration settings related to N1N2 subscriptions and ensure they are correct. • Investigate any spikes in load or indications of resource bottlenecks. • Correlate with recent changes or deployments in the environment. If the issue persists, please check with Support team.

5.1.2.36 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 5-169 UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of n1n2 subscribe reattempt failed.
Summary	More than 75% of n1n2 subscribe reattempt failed.
Severity	Critical

Table 5-169 (Cont.) UE_N1N2_SUBSCRIBE_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",operationType="subscribe",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",operationType="subscribe"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.99
Metric Used	http_out_conn_response_total, http_out_conn_request_total
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 subscribe.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 subscription is failing or if the AMF that request are going to is unhealthy. **Cause:** An elevated percentage of reattempt failures has been detected for UE N1N2 subscriptions. The `http_out_conn_response_total` metric increments whenever the PCF-UE receives a response for outbound messages, specifically tracking reattempts where the operation type is "subscribe" and the response code is not in the 2xx (success) range. This alert triggers when more than 75% of such reattempts fail over a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** The target AMF may be experiencing outages, heavy load, or is otherwise unhealthy, causing it to reject or fail to respond to subscription requests. • **Network Issues or Communication Failures:** Network congestion, routing problems, or transient communication errors may prevent successful delivery of N1N2 subscription requests or receipt of responses. • **Configuration Errors:** Misconfiguration of endpoints (such as incorrect URLs, authentication, or authorization settings) may cause subscription requests to be rejected or fail. • **High Load or Resource Exhaustion:** If the AMF or intermediate network components are overloaded or have run out of necessary resources (e.g., memory, threads, process slots), reattempted requests may be rejected. • **Timeouts or Latency Issues:**Prolonged delays in response times could cause requests to time out, leading to apparent failures. **Recovery:** • Review logs and error codes for patterns or specific failure reasons. • Check the health and recent activity of the AMF(s) and relevant network paths. • Examine configuration settings related to N1N2 subscriptions and ensure they are correct. • Investigate any spikes in load or indications of resource bottlenecks. • Correlate with recent changes or deployments in the environment. If the issue persists, please check with Support team.

5.1.2.37 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 5-170 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of n1n2 transfer reattempt failed.
Summary	More than 25% of n1n2 transfer reattempt failed.
Severity	Minor
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.100
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Table 5-170 (Cont.) UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 transfer.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 message transfer is failing or if the AMF that request are going to is unhealthy. **Cause:** An increased percentage of reattempt failures has been detected for UE N1N2 message transfers. The `http_out_conn_response_total` metric increments when the PCF-UE receives a response for messages being sent out of the Network Function (NF), specifically monitoring reattempts of the "transfer" operation where the response code is not 2xx (success). This alert is triggered when over 25% of such reattempts result in failure within a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** If the target AMF is down, overloaded, or behaving unpredictably, message transfer requests (especially retries) are more likely to fail. • **Network Path Issues:** Transient or persistent network failures, high latency, or packet loss between the PCF-UE and the target network function can disrupt the successful transfer of N1N2 messages. • **Configuration Errors:** Misconfiguration in endpoints, credentials, or other protocol parameters can cause messages to be consistently rejected or fail to deliver. • **System Resource Constraints:** Resource exhaustion (CPU, memory, file descriptors, etc.) on either the PCF-UE or the AMF could prevent successful handling of transfer requests. • **Timeouts and Slow Processing:** Delayed responses or timeouts can be interpreted as failures, particularly if the operation times out consistently during high load or due to backend issues. **Recovery:** • Review and analyze failure logs and returned error codes. • Check the operational health and resource status of the AMF and other involved NFs. • Validate network connectivity and latency between all relevant components. • Inspect configuration and recent changes for potential misalignments. • Correlate the timing of increased failures with network incidents, maintenance windows, or new deployments. If the issue persists, please check with Support team.

5.1.2.38 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 5-171 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of n1n2 transfer reattempt failed.
Summary	More than 50% of n1n2 transfer reattempt failed.
Severity	Major

Table 5-171 (Cont.) UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.100
Metric Used	http_out_conn_response_total, http_out_conn_request_total
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 transfer.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 message transfer is failing or if the AMF that request are going to is unhealthy. **Cause:** An increased percentage of reattempt failures has been detected for UE N1N2 message transfers. The `http_out_conn_response_total` metric increments when the PCF-UE receives a response for messages being sent out of the Network Function (NF), specifically monitoring reattempts of the "transfer" operation where the response code is not 2xx (success). This alert is triggered when over 50% of such reattempts result in failure within a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** If the target AMF is down, overloaded, or behaving unpredictably, message transfer requests (especially retries) are more likely to fail. • **Network Path Issues:** Transient or persistent network failures, high latency, or packet loss between the PCF-UE and the target network function can disrupt the successful transfer of N1N2 messages. • **Configuration Errors:** Misconfiguration in endpoints, credentials, or other protocol parameters can cause messages to be consistently rejected or fail to deliver. • **System Resource Constraints:** Resource exhaustion (CPU, memory, file descriptors, etc.) on either the PCF-UE or the AMF could prevent successful handling of transfer requests. • **Timeouts and Slow Processing:** Delayed responses or timeouts can be interpreted as failures, particularly if the operation times out consistently during high load or due to backend issues. **Recovery:** • Review and analyze failure logs and returned error codes. • Check the operational health and resource status of the AMF and other involved NFs. • Validate network connectivity and latency between all relevant components. • Inspect configuration and recent changes for potential misalignments. • Correlate the timing of increased failures with network incidents, maintenance windows, or new deployments. If the issue persists, please check with Support team.

5.1.2.39 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 5-172 UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of n1n2 transfer reattempt failed.
Summary	More than 75% of n1n2 transfer reattempt failed.
Severity	Critical
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2MessageTransfer", operationType="transfer"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.100
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Table 5-172 (Cont.) UE_N1N2_TRANSFER_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of reattempt failure for ue n1n2 transfer.If there is an increase of failure, operator can revise the reason why the flow triggering n1n2 message transfer is failing or if the AMF that request are going to is unhealthy. **Cause:** An increased percentage of reattempt failures has been detected for UE N1N2 message transfers. The `http_out_conn_response_total` metric increments when the PCF-UE receives a response for messages being sent out of the Network Function (NF), specifically monitoring reattempts of the "transfer" operation where the response code is not 2xx (success). This alert is triggered when over 75% of such reattempts result in failure within a 5-minute period. **Diagnostic Information:** • **AMF (Access and Mobility Management Function) Unavailability or Instability:** If the target AMF is down, overloaded, or behaving unpredictably, message transfer requests (especially retries) are more likely to fail. • **Network Path Issues:** Transient or persistent network failures, high latency, or packet loss between the PCF-UE and the target network function can disrupt the successful transfer of N1N2 messages. • **Configuration Errors:** Misconfiguration in endpoints, credentials, or other protocol parameters can cause messages to be consistently rejected or fail to deliver. • **System Resource Constraints:** Resource exhaustion (CPU, memory, file descriptors, etc.) on either the PCF-UE or the AMF could prevent successful handling of transfer requests. • **Timeouts and Slow Processing:** Delayed responses or timeouts can be interpreted as failures, particularly if the operation times out consistently during high load or due to backend issues. **Recovery:** • Review and analyze failure logs and returned error codes. • Check the operational health and resource status of the AMF and other involved NFs. • Validate network connectivity and latency between all relevant components. • Inspect configuration and recent changes for potential misalignments. • Correlate the timing of increased failures with network incidents, maintenance windows, or new deployments. If the issue persists, please check with Support team.

5.1.2.40 SM_STALE_REQUEST_PROCESSING_REJECT_MINOR

Table 5-173 SM_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Name in Alert Yaml File	SM_STALE_REQUEST_PROCESSING_REJECT_MINOR
Description	More than 10% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Summary	More than 10% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Severity	Minor

Table 5-173 (Cont.) SM_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Expression	(sum by (namespace,pod) (rate(occnp_late_processing_rejection_total{microservice=~"occnp_pcf_sm"}[5m])))/ (sum by (namespace,pod) (rate(ocpm_ingress_request_total{microservice=~"occnp_pcf_sm"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.101
Metric Used	occnp_late_processing_rejection_total, ocpm_ingress_request_total
Recommended Actions	The metric **occnp_late_processing_rejection_total** is pegged when Late Processing finds a stale session. **Cause:** The metric **occnp_late_processing_rejection_total** is incremented when the SM Service determines that a request has become stale. For example, if a request includes the following header parameters: • `sbiSenderTimestamp3GPP='2025-11-03T09:48:01.000Z'` (sender timestamp) • `sbiMaxRSPTime3GPP='3000'` (maximum response time in milliseconds) In this scenario, if there is a delay in receiving a response from the external Network Function (NF), a stale check is later performed. If the request is deemed stale during this check, it is counted in the metric. When more than 10% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT, then this alarm will be raised. **Diagnostic Information:** • **Validate Timestamps:** Ensure that system clocks are synchronized (e.g., via NTP). • **Analyze Latency:** Use tracing or metric data to identify bottlenecks in response time—look for patterns in external NF response delays. • **Review Configurations:** Confirm that max response times (`sbiMaxRSPTime3GPP`) are correctly set as per the service contract. • **Scale System Resources**: Check for resource constraints (CPU, memory, bandwidth) and scale up your system or services as needed to handle the incoming request load within the allowed response time. **Recovery:** Once the recommended diagnostic actions are implemented and responses from the external NF are received within the expected timeframe, the percentage of rejected messages will begin to decline, ultimately clearing the alert.

5.1.2.41 SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Table 5-174 SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Name in Alert Yaml File	SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR
Description	More than 20% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Summary	More than 20% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Severity	Major

Table 5-174 (Cont.) SM_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Expression	(sum by (namespace,pod) (rate(occnp_late_processing_rejection_total{microservice=~"occnp_pcf_sm"}[5m])))/ (sum by (namespace,pod) (rate(ocpm_ingress_request_total{microservice=~"occnp_pcf_sm"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.101
Metric Used	occnp_late_processing_rejection_total, ocpm_ingress_request_total
Recommended Actions	The metric **occnp_late_processing_rejection_total** is pegged when Late Processing finds a stale session. **Cause:** The metric **occnp_late_processing_rejection_total** is incremented when the SM Service determines that a request has become stale. For example, if a request includes the following header parameters: • `sbiSenderTimestamp3GPP='2025-11-03T09:48:01.000Z'` (sender timestamp) • `sbiMaxRSPTime3GPP='3000'` (maximum response time in milliseconds) In this scenario, if there is a delay in receiving a response from the external Network Function (NF), a stale check is later performed. If the request is deemed stale during this check, it is counted in the metric. When more than 20% and less than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT, then this alarm will be raised. **Diagnostic Information:** • **Validate Timestamps:** Ensure that system clocks are synchronized (e.g., via NTP). • **Analyze Latency:** Use tracing or metric data to identify bottlenecks in response time—look for patterns in external NF response delays. • **Review Configurations:** Confirm that max response times (`sbiMaxRSPTime3GPP`) are correctly set as per the service contract. • **Scale System Resources**: Check for resource constraints (CPU, memory, bandwidth) and scale up your system or services as needed to handle the incoming request load within the allowed response time. **Recovery:** Once the recommended diagnostic actions are implemented and responses from the external NF are received within the expected timeframe, the percentage of rejected messages will begin to decline, ultimately clearing the alert.

5.1.2.42 SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Table 5-175 SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Name in Alert Yaml File	SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL
Description	More than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Summary	More than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT due to request being stale
Severity	Critical

Table 5-175 (Cont.) SM_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Expression	(sum by (namespace,pod) (rate(occnp_late_processing_rejection_total{microservice=~"occnp_pcf_sm"}[5m])))/ (sum by (namespace,pod) (rate(ocpm_ingress_request_total{microservice=~"occnp_pcf_sm"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.101
Metric Used	occnp_late_processing_rejection_total, ocpm_ingress_request_total
Recommended Actions	The metric **occnp_late_processing_rejection_total** is pegged when Late Processing finds a stale session. **Cause:** The metric **occnp_late_processing_rejection_total** is incremented when the SM Service determines that a request has become stale. For example, if a request includes the following header parameters: • `sbiSenderTimestamp3GPP='2025-11-03T09:48:01.000Z'` (sender timestamp) • `sbiMaxRSPTime3GPP='3000'` (maximum response time in milliseconds) In this scenario, if there is a delay in receiving a response from the external Network Function (NF), a stale check is later performed. If the request is deemed stale during this check, it is counted in the metric. When more than 30% of the Ingress requests failed with error 504 GATEWAY_TIMEOUT, then this alarm will be raised. **Diagnostic Information:** • **Validate Timestamps:** Ensure that system clocks are synchronized (e.g., via NTP). • **Analyze Latency:** Use tracing or metric data to identify bottlenecks in response time—look for patterns in external NF response delays. • **Review Configurations:** Confirm that max response times (`sbiMaxRSPTime3GPP`) are correctly set as per the service contract. • **Scale System Resources**: Check for resource constraints (CPU, memory, bandwidth) and scale up your system or services as needed to handle the incoming request load within the allowed response time. **Recovery:** Once the recommended diagnostic actions are implemented and responses from the external NF are received within the expected timeframe, the percentage of rejected messages will begin to decline, ultimately clearing the alert.

5.1.2.43 UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Table 5-176 UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Description	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Summary	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Severity	Major

Table 5-176 (Cont.) UE_STALE_REQUEST_PROCESSING_REJECT_MAJOR

Field	Details
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.104
Metric Used	`occnp_late_processing_rejection_total`
Recommended Actions	Metric `occnp_late_processing_rejection_total` is pegged when requests being processed become stale**.** **Cause:** More than 20% of incoming requests to the ue-service have been rejected because they became stale during processing. The service flags a request as stale when its processing exceeds an acceptable time window. **Diagnostic Information:** • **High System Load or Resource Contention:** The ue-service or its backend components may be overloaded (e.g., CPU, memory, I/O), delaying request processing. • **Inefficient Request Handling or Bottlenecks:** There may be inefficiencies or slow operations within the service logic, such as database queries, API calls, or complex computations causing extended processing times. • **Network Latency or Downstream Delays:** High network latency or slow responses from dependent services or databases could increase the time required to process requests. • **Increased Volume of Requests:** A spike in incoming requests can overwhelm the service, leading to request queues and increased wait times. **Recovery:** • Monitor system and service resource utilization. • Review recent changes to workload, configuration, or deployments. • Tune timeouts and thresholds appropriately based on observed service latency. • Analyze logs to pinpoint where delays are occurring in the request processing workflow. If the issue persists, please check with Support team.

5.1.2.44 UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Table 5-177 UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Description	This alert is triggered when more than 30% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Summary	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.104

Table 5-177 (Cont.) UE_STALE_REQUEST_PROCESSING_REJECT_CRITICAL

Field	Details
Metric Used	`occnp_late_processing_rejection_total`
Recommended Actions	Metric `occnp_late_processing_rejection_total` is pegged when requests being processed become stale**.** **Cause:** More than 30% of incoming requests to the ue-service have been rejected because they became stale during processing. The service flags a request as stale when its processing exceeds an acceptable time window. **Diagnostic Information:** • **High System Load or Resource Contention:** The ue-service or its backend components may be overloaded (e.g., CPU, memory, I/O), delaying request processing. • **Inefficient Request Handling or Bottlenecks:** There may be inefficiencies or slow operations within the service logic, such as database queries, API calls, or complex computations causing extended processing times. • **Network Latency or Downstream Delays:** High network latency or slow responses from dependent services or databases could increase the time required to process requests. • **Increased Volume of Requests:** A spike in incoming requests can overwhelm the service, leading to request queues and increased wait times. **Recovery:** • Monitor system and service resource utilization. • Review recent changes to workload, configuration, or deployments. • Tune timeouts and thresholds appropriately based on observed service latency. • Analyze logs to pinpoint where delays are occurring in the request processing workflow. If the issue persists, please check with Support team.

5.1.2.45 UE_STALE_REQUEST_PROCESSING_REJECT_MINOR

Table 5-178 UE_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Description	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Summary	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to request going stale, while being processed by the service.
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_late_processing_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace) (rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.104
Metric Used	`occnp_late_processing_rejection_total`

Table 5-178 (Cont.) UE_STALE_REQUEST_PROCESSING_REJECT_MINOR

Field	Details
Recommended Actions	Metric `occnp_late_processing_rejection_total` is pegged when requests being processed become stale. **Cause:** More than 10% of incoming requests to the ue-service have been rejected because they became stale during processing. The service flags a request as stale when its processing exceeds an acceptable time window. **Diagnostic Information:** • **High System Load or Resource Contention:** The ue-service or its backend components may be overloaded (e.g., CPU, memory, I/O), delaying request processing. • **Inefficient Request Handling or Bottlenecks:** There may be inefficiencies or slow operations within the service logic, such as database queries, API calls, or complex computations causing extended processing times. • **Network Latency or Downstream Delays:** High network latency or slow responses from dependent services or databases could increase the time required to process requests. • **Increased Volume of Requests:** A spike in incoming requests can overwhelm the service, leading to request queues and increased wait times. **Recovery:** • Monitor system and service resource utilization. • Review recent changes to workload, configuration, or deployments. • Tune timeouts and thresholds appropriately based on observed service latency. • Analyze logs to pinpoint where delays are occurring in the request processing workflow. If the issue persists, please check with Support team.

5.1.2.46 UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Table 5-179 UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Field	Details
Description	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Summary	This alert is triggered when more than 10% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_late_arrival_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace)(rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.109
Metric Used	`ocpm_late_arrival_rejection_total`

Table 5-179 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Field	Details
Recommended Actions	Metric `ocpm_late_arrival_rejection_total` is pegged when a received requests is stale. **Cause:** Metric **ocpm_late_arrival_rejection_total** is pegged when a received requests is stale**.** • **Metric:** `ocpm_late_arrival_rejection_total` – Increments when the UE Service determines incoming requests are stale (arrived too late to process). – The staleness check is based on: * `3gpp-Sbi-Sender-Timestamp` (preferred) * `3gpp-Sbi-Origination-Timestamp` (fallback if sender timestamp is unavailable) * `3gpp-Sbi-Max-Rsp-Time` (maximum allowed response time, in ms) • **Request Example:** – `3gpp-Sbi-Sender-Timestamp='2025-11-03T09:48:01.000Z'` – `3gpp-Sbi-Max-Rsp-Time='3000'` (i.e., 3 seconds) • If request arrives after (Sender-Timestamp + Max-Rsp-Time), it is considered **stale** and counted in the metric. • **Alarm Condition:** – If **more than 10%** of ingress requests result in `504 GATEWAY_TIMEOUT` errors due to staleness, an alarm is raised. **Diagnostic Information:** 1. **Verify Time Synchronization** • Ensure all Network Functions (NFs) have synchronized system clocks (using NTP). • Time drift between sender and UE Service may falsely trigger staleness. 2. **Check Network Latency** • Investigate possible network delays or congestion between external NF and the UE Service. • High or unstable latency can lead to late arrival of requests. 3. **Analyze Sender Behavior** • Validate that the sending NF populates `3gpp-Sbi-Sender-Timestamp` (or Origination-Timestamp) correctly. • Misconfigured or delayed timestamping can corrupt staleness calculation. 4. **Assess Max Response Time Values** • Review if the `3gpp-Sbi-Max-Rsp-Time` value is appropriate for your network and application conditions. • Very short response times may not be feasible under current latency conditions. 5. **Review Application Load** • Monitor system/resource utilization (CPU, memory, queue lengths) on the UE Service. • Resource exhaustion may delay request processing, even if requests arrive on time. 6. **Correlation with Other Metrics** • Examine related metrics such as total request counts, processing times, error types, etc., to identify trends. • Check if certain sources or request types are consistently late. 7. **Check for Backlogs**

Table 5-179 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MINOR

Field	Details
	• Review UE Service logs for any signs of backlogs, bottlenecks, or spikes in the request handling pipeline. **Recovery:** 1. **Verify Time Synchronization** • Ensure all relevant Network Functions (NFs) have correct system time. Resynchronize clocks if any drift is detected. 2. **Check Network Latency and Connectivity** • Investigate any current network issues or bottlenecks between the external NF and the UE Service. Resolve any high latency or packet loss immediately if detected. 3. **Review UE Service Application & Resources** • Check the UE Service for high CPU/memory usage or any request processing backlogs. • Restart or scale up resources temporarily if the system is overloaded. 4. **Contact Upstream NF Owners** Notify owners of external NFs if they are sending delayed or incorrectly timestamped requests so they can take corrective action.

5.1.2.47 UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Table 5-180 UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Field	Details
Description	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Summary	This alert is triggered when more than 20% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_late_arrival_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace)(rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.109
Metric Used	`ocpm_late_arrival_rejection_total`

Table 5-180 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Field	Details
Recommended Actions	Metric `ocpm_late_arrival_rejection_total` is pegged when a received requests is stale. **Cause:** Metric **ocpm_late_arrival_rejection_total** is pegged when a received requests is stale**.** • **Metric:** `ocpm_late_arrival_rejection_total` – Increments when the UE Service determines incoming requests are stale (arrived too late to process). – The staleness check is based on: * `3gpp-Sbi-Sender-Timestamp` (preferred) * `3gpp-Sbi-Origination-Timestamp` (fallback if sender timestamp is unavailable) * `3gpp-Sbi-Max-Rsp-Time` (maximum allowed response time, in ms) • **Request Example:** – `3gpp-Sbi-Sender-Timestamp='2025-11-03T09:48:01.000Z'` – `3gpp-Sbi-Max-Rsp-Time='3000'` (i.e., 3 seconds) • If request arrives after (Sender-Timestamp + Max-Rsp-Time), it is considered **stale** and counted in the metric. • **Alarm Condition:** – If **more than 20%** of ingress requests result in `504 GATEWAY_TIMEOUT` errors due to staleness, an alarm is raised. **Diagnostic Information:** 1. **Verify Time Synchronization** • Ensure all Network Functions (NFs) have synchronized system clocks (using NTP). • Time drift between sender and UE Service may falsely trigger staleness. 2. **Check Network Latency** • Investigate possible network delays or congestion between external NF and the UE Service. • High or unstable latency can lead to late arrival of requests. 3. **Analyze Sender Behavior** • Validate that the sending NF populates `3gpp-Sbi-Sender-Timestamp` (or Origination-Timestamp) correctly. • Misconfigured or delayed timestamping can corrupt staleness calculation. 4. **Assess Max Response Time Values** • Review if the `3gpp-Sbi-Max-Rsp-Time` value is appropriate for your network and application conditions. • Very short response times may not be feasible under current latency conditions. 5. **Review Application Load** • Monitor system/resource utilization (CPU, memory, queue lengths) on the UE Service. • Resource exhaustion may delay request processing, even if requests arrive on time. 6. **Correlation with Other Metrics** • Examine related metrics such as total request counts, processing times, error types, etc., to identify trends. • Check if certain sources or request types are consistently late. 7. **Check for Backlogs**

Table 5-180 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_MAJOR

Field	Details
	• Review UE Service logs for any signs of backlogs, bottlenecks, or spikes in the request handling pipeline. **Recovery:** 1. **Verify Time Synchronization** • Ensure all relevant Network Functions (NFs) have correct system time. Resynchronize clocks if any drift is detected. 2. **Check Network Latency and Connectivity** • Investigate any current network issues or bottlenecks between the external NF and the UE Service. Resolve any high latency or packet loss immediately if detected. 3. **Review UE Service Application & Resources** • Check the UE Service for high CPU/memory usage or any request processing backlogs. • Restart or scale up resources temporarily if the system is overloaded. 4. **Contact Upstream NF Owners** Notify owners of external NFs if they are sending delayed or incorrectly timestamped requests so they can take corrective action.

5.1.2.48 UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Table 5-181 UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Field	Details
Description	This alert is triggered when more than 30% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Summary	This alert is triggered when more than 30% of the incoming requests towards UE Policy service are rejected due to requests being stale upon arrival to the service.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_late_arrival_rejection_total{microservice=~".*pcf_ueservice"}[5m])) / sum by (namespace)(rate(ocpm_ingress_request_total{microservice=~".*pcf_ueservice"}[5m]))) * 100 > 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.109
Metric Used	`ocpm_late_arrival_rejection_total`

Table 5-181 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Field	Details
Recommended Actions	Metric `ocpm_late_arrival_rejection_total` is pegged when a received requests is stale. **Cause:** Metric **ocpm_late_arrival_rejection_total** is pegged when a received requests is stale**.** • **Metric:** `ocpm_late_arrival_rejection_total` – Increments when the UE Service determines incoming requests are stale (arrived too late to process). – The staleness check is based on: * `3gpp-Sbi-Sender-Timestamp` (preferred) * `3gpp-Sbi-Origination-Timestamp` (fallback if sender timestamp is unavailable) * `3gpp-Sbi-Max-Rsp-Time` (maximum allowed response time, in ms) • **Request Example:** – `3gpp-Sbi-Sender-Timestamp='2025-11-03T09:48:01.000Z'` – `3gpp-Sbi-Max-Rsp-Time='3000'` (i.e., 3 seconds) • If request arrives after (Sender-Timestamp + Max-Rsp-Time), it is considered **stale** and counted in the metric. • **Alarm Condition:** – If **more than 30%** of ingress requests result in `504 GATEWAY_TIMEOUT` errors due to staleness, an alarm is raised. **Diagnostic Information:** 1. **Verify Time Synchronization** • Ensure all Network Functions (NFs) have synchronized system clocks (using NTP). • Time drift between sender and UE Service may falsely trigger staleness. 2. **Check Network Latency** • Investigate possible network delays or congestion between external NF and the UE Service. • High or unstable latency can lead to late arrival of requests. 3. **Analyze Sender Behavior** • Validate that the sending NF populates `3gpp-Sbi-Sender-Timestamp` (or Origination-Timestamp) correctly. • Misconfigured or delayed timestamping can corrupt staleness calculation. 4. **Assess Max Response Time Values** • Review if the `3gpp-Sbi-Max-Rsp-Time` value is appropriate for your network and application conditions. • Very short response times may not be feasible under current latency conditions. 5. **Review Application Load** • Monitor system/resource utilization (CPU, memory, queue lengths) on the UE Service. • Resource exhaustion may delay request processing, even if requests arrive on time. 6. **Correlation with Other Metrics** • Examine related metrics such as total request counts, processing times, error types, etc., to identify trends. • Check if certain sources or request types are consistently late. 7. **Check for Backlogs**

Table 5-181 (Cont.) UE_STALE_REQUEST_ARRIVAL_REJECT_CRITICAL

Field	Details
	• Review UE Service logs for any signs of backlogs, bottlenecks, or spikes in the request handling pipeline. **Recovery:** 1. **Verify Time Synchronization** • Ensure all relevant Network Functions (NFs) have correct system time. Resynchronize clocks if any drift is detected. 2. **Check Network Latency and Connectivity** • Investigate any current network issues or bottlenecks between the external NF and the UE Service. Resolve any high latency or packet loss immediately if detected. 3. **Review UE Service Application & Resources** • Check the UE Service for high CPU/memory usage or any request processing backlogs. • Restart or scale up resources temporarily if the system is overloaded. 4. **Contact Upstream NF Owners** Notify owners of external NFs if they are sending delayed or incorrectly timestamped requests so they can take corrective action.

5.1.2.49 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 5-182 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of N1N2 transfer failure notification reattempts failed.
Summary	More than 75% of N1N2 transfer failure notification reattempts failed.
Severity	Critical
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.106
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Table 5-182 (Cont.) UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case the alert notifies when there is a certain amount of reattempt failure for UE N1N2 transfer failure notification. If there is an increase of failure, operator can investigate on: • Why the flow triggering N1N2 transfer failure notification is failing, or • Check the health of the AMF to which the request are going to **Cause:** http_out_conn_response_total metric with indicated dimensions is pegged when PCF-UE receives a response for an outgoing reattempt transfer request triggered for N1N2TransferFailure notification. Dimensions: IsReattempt : true reattemptType : UE_N1N2TransferFailure OperationType : transfer ResponseCode : !2xx In this case more than 75% of outgoing transfer reattempts (due to **N1N2TransferFailure** as notified by AMF) receive a non-2xx (failure) response in the last 5 minutes (or selected sample frame) **Diagnostic Information :** 1. ***Check Recent Logs***: • Analyze logs for both PCF-UE and Egress Gateway in the relevant namespace for error details (timestamps matching the period of alert). • Focus on error responses: look for 4xx/5xx HTTP responses and their reasons. 2. ***Correlate with Traffic Patterns***: • Determine if failures are for specific to certain AMFs or random. • Check if there's a sudden surge in failures (indicating a broader issue). 3. ***Inspect Network Health and Configuration***: • Ensure connectivity and correct routing between PCF-UE and its downstream targets. • Validate configurations, especially recently changed ones. 4. ***Cross-check Incident/Event Timeline***: • Review recent maintenance, deployments, or network events that could correlate with the increase in failures. 5. ***Evaluate for Service Overload***: • Examine resource metrics (CPU, memory, rate of requests) of the affected service(PCF-UE, PCF-EGW) to determine if it's under duress. 6. ***Check with Peers***: • See if corresponding namespaces (other tenants/products) are seeing similar issues, could indicate a platform or shared service problem. **Recovery :** 1. **Resolve Underlying Service Issues**: • If the upstream service (e.g., AMF or other network function) is unhealthy, work with the respective team to restore normal operation. • Address any misconfiguration or errors causing repeated non-2xx responses.

Table 5-182 (Cont.) UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
	2. **Revert Recent Changes**: • If the issue correlates with recent deployments or configuration changes, consider rolling back to the previous stable state after assessing impact. 3. **Mitigate Service Overload**: • If resource constraints are detected (CPU, memory, connections), scale up resources or reduce load by throttling non-critical requests where possible. 4. **Network Remediation**: • Resolve any detected connectivity or routing issues between PCF-UE and the egress gateway or upstream endpoints. 5. **Monitor and Confirm Recovery**: • Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold. Ensure related services in affected namespaces also recover.

5.1.2.50 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 5-183 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of N1N2 transfer failure notification reattempts failed.
Summary	More than 50% of N1N2 transfer failure notification reattempts failed.
Severity	Major
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.106
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Table 5-183 (Cont.)
UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case the alert notifies when there is a certain amount of reattempt failure for UE N1N2 transfer failure notification. If there is an increase of failure, operator can investigate on: • Why the flow triggering N1N2 transfer failure notification is failing, or • Check the health of the AMF to which the request are going to **Cause:** http_out_conn_response_total metric with indicated dimensions is pegged when PCF-UE receives a response for an outgoing reattempt transfer request triggered for N1N2TransferFailure notification. Dimensions: IsReattempt : true reattemptType : UE_N1N2TransferFailure OperationType : transfer ResponseCode : !2xx In this case more than 50% of outgoing transfer reattempts (due to **N1N2TransferFailure** as notified by AMF) receive a non-2xx (failure) response in the last 5 minutes (or selected sample frame) **Diagnostic Information :** 1. ***Check Recent Logs***: • Analyze logs for both PCF-UE and Egress Gateway in the relevant namespace for error details (timestamps matching the period of alert). • Focus on error responses: look for 4xx/5xx HTTP responses and their reasons. 2. ***Correlate with Traffic Patterns***: • Determine if failures are for specific to certain AMFs or random. • Check if there's a sudden surge in failures (indicating a broader issue). 3. ***Inspect Network Health and Configuration***: • Ensure connectivity and correct routing between PCF-UE and its downstream targets. • Validate configurations, especially recently changed ones. 4. ***Cross-check Incident/Event Timeline***: • Review recent maintenance, deployments, or network events that could correlate with the increase in failures. 5. ***Evaluate for Service Overload***: • Examine resource metrics (CPU, memory, rate of requests) of the affected service(PCF-UE, PCF-EGW) to determine if it’s under duress. 6. ***Check with Peers***: • See if corresponding namespaces (other tenants/products) are seeing similar issues, could indicate a platform or shared service problem. **Recovery :** 1. **Resolve Underlying Service Issues**: • If the upstream service (e.g., AMF or other network function) is unhealthy, work with the respective team to restore normal operation. • Address any misconfiguration or errors causing repeated non-2xx responses. 2. **Revert Recent Changes**:

Table 5-183 (Cont.)
UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
	• If the issue correlates with recent deployments or configuration changes, consider rolling back to the previous stable state after assessing impact. 3. **Mitigate Service Overload**: • If resource constraints are detected (CPU, memory, connections), scale up resources or reduce load by throttling non-critical requests where possible. 4. **Network Remediation**: • Resolve any detected connectivity or routing issues between PCF-UE and the egress gateway or upstream endpoints. 5. **Monitor and Confirm Recovery**: • Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold. Ensure related services in affected namespaces also recover.

5.1.2.51 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 5-184 UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of N1N2 transfer failure notification reattempts failed.
Summary	More than 25% of N1N2 transfer failure notification reattempts failed.
Severity	Minor
Expression	(sum by (namespace) (increase(http_out_conn_response_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(http_out_conn_request_total{isReattempt="true",reattemptType="UE_N1N2TransferFailure",operationType="transfer"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.106
Metric Used	http_out_conn_response_total, http_out_conn_request_total

Table 5-184 (Cont.)
UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The `http_out_conn_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case the alert notifies when there is a certain amount of reattempt failure for UE N1N2 transfer failure notification. If there is an increase of failure, operator can investigate on: • Why the flow triggering N1N2 transfer failure notification is failing, or • Check the health of the AMF to which the request are going to **Cause:** http_out_conn_response_total metric with indicated dimensions is pegged when PCF-UE receives a response for an outgoing reattempt transfer request triggered for N1N2TransferFailure notification. Dimensions: IsReattempt : true reattemptType : UE_N1N2TransferFailure OperationType : transfer ResponseCode : !2xx In this case more than 25% of outgoing transfer reattempts (due to **N1N2TransferFailure** as notified by AMF) receive a non-2xx (failure) response in the last 5 minutes (or selected sample frame) **Diagnostic Information :** 1. ***Check Recent Logs***: • Analyze logs for both PCF-UE and Egress Gateway in the relevant namespace for error details (timestamps matching the period of alert). • Focus on error responses: look for 4xx/5xx HTTP responses and their reasons. 2. ***Correlate with Traffic Patterns***: • Determine if failures are for specific to certain AMFs or random. • Check if there's a sudden surge in failures (indicating a broader issue). 3. ***Inspect Network Health and Configuration***: • Ensure connectivity and correct routing between PCF-UE and its downstream targets. • Validate configurations, especially recently changed ones. 4. ***Cross-check Incident/Event Timeline***: • Review recent maintenance, deployments, or network events that could correlate with the increase in failures. 5. ***Evaluate for Service Overload***: • Examine resource metrics (CPU, memory, rate of requests) of the affected service(PCF-UE, PCF-EGW) to determine if it’s under duress. 6. ***Check with Peers***: • See if corresponding namespaces (other tenants/products) are seeing similar issues, could indicate a platform or shared service problem. **Recovery :** 1. **Resolve Underlying Service Issues**: • If the upstream service (e.g., AMF or other network function) is unhealthy, work with the respective team to restore normal operation. • Address any misconfiguration or errors causing repeated non-2xx responses. 2. **Revert Recent Changes**:

Table 5-184 (Cont.)
UE_N1N2_TRANSFER_FAILURE_NOTIFICATION_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
	• If the issue correlates with recent deployments or configuration changes, consider rolling back to the previous stable state after assessing impact. 3. **Mitigate Service Overload**: • If resource constraints are detected (CPU, memory, connections), scale up resources or reduce load by throttling non-critical requests where possible. 4. **Network Remediation**: • Resolve any detected connectivity or routing issues between PCF-UE and the egress gateway or upstream endpoints. 5. **Monitor and Confirm Recovery**: • Continue monitoring the alert metric after remedial actions to confirm the failure rate falls below the alert threshold. Ensure related services in affected namespaces also recover.

5.1.2.52 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Table 5-185 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD
Description	More than 75% of amf discovery reattempts failed.
Summary	More than 75% of amf discovery reattempts failed.
Severity	Critical
Expression	(sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_response_total{operationType="timer_expiry_notification",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_request_total{operationType="timer_expiry_notification"}[5m]))) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.105
Metric Used	occnp_ue_nf_discovery_reattempt_response_total

Table 5-185 (Cont.) UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	The `occnp_ue_nf_discovery_reattempt_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case, the alert notifies when there is a certain number of reattempt failure while discovering AMF. If there is an increase of failure, operator can investigate on: • Why the AMF discovery flow is failing, or • Check the health of the AMF to which the request are going to. **Cause:** The main cause of the `occnp_ue_nf_discovery_reattempt_response_total` metric being pegged—indicating a notable number of reattempt failures during AMF discovery—is that the PCF-UE (Policy Control Function - User Equipment) is receiving non-success responses (failures) when retrying AMF (Access and Mobility Management Function) discovery requests. **Diagnostic Information:** • **AMF Unavailability or Health Issues:** The target AMF may be down, unresponsive, overloaded, or otherwise unhealthy, resulting in failed or rejected discovery attempts. • **Network Issues or Latency:** Communication issues such as network congestion, high latency, or dropped packets between the PCF-UE and the AMF (or intermediary NFs) can cause discovery attempts to fail. • **Incorrect Configuration:** Misconfigurations in the PCF-UE or AMF—such as wrong endpoint addresses, security settings, or authentication parameters—may prevent the successful completion of discovery requests. • **NRF (Network Repository Function) Problems:** If AMF discovery relies on the NRF and the NRF is unhealthy or misconfigured, the PCF-UE may be unable to retrieve up-to-date or correct AMF information. • **Resource Exhaustion:** If the system is under heavy load or resources (CPU, memory, threads) are depleted, discovery requests may not be handled on time. • **Timeouts and Slow Processing:** Slow responses from the AMF or network timeouts can contribute to repeated reattempts and failures. **Recovery:** • Review logs and error responses associated with AMF discovery attempts. • Check the health status and recent operational history of the target AMF and NRF. • Verify network health and connectivity between all relevant components. • Validate all associated configurations (PCF-UE, AMF, NRF). If the issue persists, please check with Support team.

5.1.2.53 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Table 5-186 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD
Description	More than 50% of amf discovery reattempts failed.
Summary	More than 50% of amf discovery reattempts failed.
Severity	Major

Table 5-186 (Cont.) UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MAJOR_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_response_total{operationType="timer_expiry_notification",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_request_total{operationType="timer_expiry_notification"}[5m]))) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.105
Metric Used	occnp_ue_nf_discovery_reattempt_response_total
Recommended Actions	The `occnp_ue_nf_discovery_reattempt_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then in this case, the alert notifies when there is a certain number of reattempt failure while discovering AMF. If there is an increase of failure, operator can investigate on: • Why the AMF discovery flow is failing, or • Check the health of the AMF to which the request are going to. **Cause:** The main cause of the `occnp_ue_nf_discovery_reattempt_response_total` metric being pegged—indicating a notable number of reattempt failures during AMF discovery—is that the PCF-UE (Policy Control Function - User Equipment) is receiving non-success responses (failures) when retrying AMF (Access and Mobility Management Function) discovery requests. **Diagnostic Information:** • **AMF Unavailability or Health Issues:** The target AMF may be down, unresponsive, overloaded, or otherwise unhealthy, resulting in failed or rejected discovery attempts. • **Network Issues or Latency:** Communication issues such as network congestion, high latency, or dropped packets between the PCF-UE and the AMF (or intermediary NFs) can cause discovery attempts to fail. • **Incorrect Configuration:** Misconfigurations in the PCF-UE or AMF—such as wrong endpoint addresses, security settings, or authentication parameters—may prevent the successful completion of discovery requests. • **NRF (Network Repository Function) Problems:** If AMF discovery relies on the NRF and the NRF is unhealthy or misconfigured, the PCF-UE may be unable to retrieve up-to-date or correct AMF information. • **Resource Exhaustion:** If the system is under heavy load or resources (CPU, memory, threads) are depleted, discovery requests may not be handled on time. • **Timeouts and Slow Processing:** Slow responses from the AMF or network timeouts can contribute to repeated reattempts and failures. **Recovery:** • Review logs and error responses associated with AMF discovery attempts. • Check the health status and recent operational history of the target AMF and NRF. • Verify network health and connectivity between all relevant components. • Validate all associated configurations (PCF-UE, AMF, NRF). If the issue persists, please check with Support team.

5.1.2.54 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Table 5-187 UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	UE_AMF_DISCOVERY_REATTEMPT_FAILURE_ABOVE_MINOR_THRESHOLD
Description	More than 25% of amf discovery reattempts failed.
Summary	More than 25% of amf discovery reattempts failed.
Severity	Minor
Expression	(sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_response_total{operationType="timer_expiry_notification",responseCode!~"2.*"}[5m])) / sum by (namespace) (increase(occnp_ue_nf_discovery_reattempt_request_total{operationType="timer_expiry_notification"}[5m]))) * 100 > 25
OID	1.3.6.1.4.1.323.5.3.52.1.2.105
Metric Used	occnp_ue_nf_discovery_reattempt_response_total
Recommended Actions	The `occnp_ue_nf_discovery_reattempt_response_total` metric is pegged when PCF-UE receives a response from a message that is going out of the NF. Then, in this case the alert notifies when there is a certain number of reattempt failure while discovering AMF. If there is an increase of failure, operator can investigate on: • Why the AMF discovery flow is failing, or • Check the health of the AMF to which the request are going to. **Cause:** The main cause of the `occnp_ue_nf_discovery_reattempt_response_total` metric being pegged—indicating a notable number of reattempt failures during AMF discovery—is that the PCF-UE (Policy Control Function - User Equipment) is receiving non-success responses (failures) when retrying AMF (Access and Mobility Management Function) discovery requests. **Diagnostic Information:** • **AMF Unavailability or Health Issues:** The target AMF may be down, unresponsive, overloaded, or otherwise unhealthy, resulting in failed or rejected discovery attempts. • **Network Issues or Latency:** Communication issues such as network congestion, high latency, or dropped packets between the PCF-UE and the AMF (or intermediary NFs) can cause discovery attempts to fail. • **Incorrect Configuration:** Misconfigurations in the PCF-UE or AMF—such as wrong endpoint addresses, security settings, or authentication parameters—may prevent the successful completion of discovery requests. • **NRF (Network Repository Function) Problems:** If AMF discovery relies on the NRF and the NRF is unhealthy or misconfigured, the PCF-UE may be unable to retrieve up-to-date or correct AMF information. • **Resource Exhaustion:** If the system is under heavy load or resources (CPU, memory, threads) are depleted, discovery requests may not be handled on time. • **Timeouts and Slow Processing:** Slow responses from the AMF or network timeouts can contribute to repeated reattempts and failures. **Recovery:** • Review logs and error responses associated with AMF discovery attempts. • Check the health status and recent operational history of the target AMF and NRF. • Verify network health and connectivity between all relevant components. • Validate all associated configurations (PCF-UE, AMF, NRF). If the issue persists, please check with Support team.

5.1.2.55 INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD

Table 5-188 INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD

Field	Details
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
Expression	(sum by(pod)(rate(ocpm_ingress_response_total{response_code!~"2.*"}[24h]) or (up * 0))/sum by(pod)(rate(ocpm_ingress_response_total[24h]))) * 100>= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.2
Metric Used	ocpm_ingress_response_total

Table 5-188 (Cont.) INGRESS_ERROR_RATE_ABOVE_10_PERCENT_PER_POD

Field	Details
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. **Cause** This alert fires when 10% or more of ingress (incoming) HTTP requests handled by any individual pod result in non-2xx (unsuccessful) responses, measured over a 1-day window. A high ingress error rate per pod suggests issues that could impact application availability, reliability, or user experience. Common causes include: • Application-level errors (returning 4xx or 5xx status codes) due to bugs, configuration issues, invalid client requests, or backend failures • Resource exhaustion (CPU, memory, open connections) or saturation within the affected pod • Dependency failures (database, cache, or external service outages), causing the pod to respond with errors • Recent deployments, rollouts, or configuration changes introducing regressions or incompatibilities • Network problems or timeouts impacting request processing • Unhandled exceptions or circuit breaker activations **Diagnostic Information** • Identify affected pods from alert labels • Review pod logs to categorize errors by type (4xx client errors, 5xx server errors, timeouts, etc.) • Correlate errors with spikes in traffic, resource usage, or specific endpoints • Examine resource utilization and health metrics (CPU, memory, connection pools, thread pools) • Check readiness/liveness probe status and pod restart history • Review changes in deployments, configurations, or dependencies preceding the alert • Investigate for signs of dependency issues, cascading failures, or external API problems **Recovery** • **Isolate and address root cause:** Use logs, error breakdowns, and metrics to determine if issues are within the pod, code, dependencies, or external factors • **Rollback if needed:** If problems started following a recent deployment or config change, consider reverting • **Increase resources or scale out:** Add capacity if the pod is resource-constrained • **Fix code or configuration:** Resolve bugs, correct misconfigurations, or address unhandled cases • **Remediate downstream/third-party issues:** Work with owners of failing dependencies if external **Alert resolution:** The alert will auto-resolve when the pod's ingress error rate falls below 10% for the measuring window For any additional guidance, contact My Oracle Support.

5.1.2.56 SM_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 5-189 SM_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
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
Expression	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.
OID	1.3.6.1.4.1.323.5.3.36.1.2.3
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. **Cause:** The metric `ocpm_ingress_request_total` is incremented for every inbound HTTP request reaching the SM component of the SM service with the dimension `serviceName3gpp="npcf-smpolicycontrol"`. If the 2-minute average exceeds 900 mps, this indicates that the system may be experiencing an overload or an abnormal spike in traffic. **Diagnostic Information:** **Examine Current Rate:** Query `ocpm_ingress_request_total` for `serviceName3gpp="npcf-smpolicycontrol"` to assess the current ingress traffic rate. **Review Upstream Sources:** Identify if request rates from any upstream SMF, AF, or TDF instances have increased. **Inspect Application Logs:** Check for `WARN` or `ERROR` messages in logs related to overload or congestion control rejections, which can help determine if the system is rejecting requests or experiencing resource pressure. **Recovery:** • **Throttle or Rate-Limit:** Apply or adjust overload/congestion control configurations to throttle or rate-limit requests from SMF as appropriate, to restore rate to expected levels. • **Scale Resources:** Add more replicas to the `sm-service` deployment if needed to reduce the average rate per instance. • **Threshold Adjustment:** Adjust the alert threshold if normal traffic patterns or business requirements change. **Alert Resolution:** When the sustained request rate stays below 900 mps, Prometheus will automatically clear the `SM_TRAFFIC_RATE_ABOVE_THRESHOLD` alert. For any additional guidance, contact My Oracle Support.

5.1.2.57 SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 5-190 SM_INGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
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
Expression	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. **Cause** This alert fires when more than 10% of all HTTP responses returned by the SM Service (`npcf-smpolicycontrol`)over the past day are non-2xx (i.e., not successful). This may be due to: • Upstream or downstream system failures • Application-level errors (5xx codes) • Client-side or bad requests (4xx codes) • Misconfiguration, rate limiting, or resource exhaustion **Diagnostic Information** • Break down error rates by response code to differentiate client, server, and other errors. • Search for error messages, stack traces, and signs of repeated failure or congestion. • Validate that dependencies(upstream services, DB) are functioning correctly. • Analyze recent deployments or config changes • Check for network latency **Recovery:** • **Identify and Address Root Cause:** Use error breakdown and logs to pinpoint and fix the underlying issue. • **Rollback Recent Changes:** If a recent deployment is responsible, consider rolling back temporarily. • **Scale or Resource Adjustment:** Add resources if you detect resource exhaustion. • **Rate Limiting or Throttling:** Apply throttling to minimize error propagation from upstream. **Alert Resolution:** Once the error rate remains below 10% for a sustained period (1 day), the alert will auto-resolve. For any additional guidance, contact My Oracle Support.

5.1.2.58 SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Table 5-191 SM_EGRESS_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
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
Expression	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	system_operational_state == 1
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. **Cause** This alert fires when more than 1% of all HTTP responses returned by the SM Service (`npcf-smpolicycontrol`)over the past day are non-2xx (i.e., not successful). This may be due to: • Upstream or downstream system failures • Application-level errors (5xx codes) • Client-side or bad requests (4xx codes) • Misconfiguration, rate limiting, or resource exhaustion **Diagnostic Information** • Break down error rates by response code to differentiate client, server, and other errors. • Search for error messages, stack traces, and signs of repeated failure or congestion. • Validate that dependencies(upstream services, DB) are functioning correctly. • Analyze recent deployments or config changes • Check for network latency **Recovery:** • **Identify and Address Root Cause:** Use error breakdown and logs to pinpoint and fix the underlying issue. • **Rollback Recent Changes:** If a recent deployment is responsible, consider rolling back temporarily. • **Scale or Resource Adjustment:** Add resources if you detect resource exhaustion. • **Rate Limiting or Throttling:** Apply throttling to minimize error propagation from upstream. **Alert Resolution:** Once the error rate remains below 10% for a sustained period (1 day), the alert will auto-resolve. For any additional guidance, contact My Oracle Support.

5.1.2.59 PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Table 5-192 PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD

Field	Details
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
Expression	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	**Cause:** The metric ocpm_userservice_inbound_count_total with dimension service_resource="chf-service" is incremented for every inbound HTTP request reaching the CHF connector service. If the 2-minute average exceeds 900 mps, this indicates that the system may be experiencing an overload or an abnormal spike in traffic. **Diagnostic Information:** **Examine Current Rate:** Query ocpm_userservice_inbound_count_total for service_resource="chf-service" to assess the current ingress traffic rate. **Review Upstream Sources:** Identify if request rates from any upstream CHF, SMF, AMF instances have increased. **Inspect Application Logs:** Check for `WARN` or `ERROR` messages in logs related to overload or congestion control rejections, which can help determine if the system is rejecting requests or experiencing resource pressure. **Recovery:** • **Throttle or Rate-Limit:** Apply or adjust congestion control configurations to throttle requests from downstream services as appropriate, to restore rate to expected levels. • **Scale Resources:** Add more replicas to the `Chf connector` deployment if needed to reduce the average rate per instance. • **Threshold Adjustment:** Adjust the alert threshold if normal traffic patterns or business requirements change. **Alert Resolution:** When the sustained request rate stays below 900 mps, Prometheus will automatically clear the PCF_CHF_INGRESS_TRAFFIC_RATE_ABOVE_THRESHOLD alert. For any additional guidance, contact My Oracle Support.

5.1.2.60 PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Table 5-193 PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
Name in Alert Yaml File	PcfChfEgressErrorRateAbove10Percent
Description	The number of failed transactions from CHF is more than 10 percent of the total transactions.
Summary	Transaction Error Rate detected above 10 Percent of Total Transactions
Severity	Critical
Expression	(sum(rate(ocpm_chf_tracking_response_total {servicename_3gpp="nchf-spendinglimitcontrol",response_code!~"2.*"} [24h]) or (up * 0)) / sum(rate(ocpm_chf_tracking_response_total {servicename_3gpp="nchf-spendinglimitcontrol"} [24h]))) 100 >= 10
OID	1.3.6.1.4.1.323.5.3.36.1.2.12
Metric Used	ocpm_chf_tracking_response_total

Table 5-193 (Cont.) PCF_CHF_EGRESS_ERROR_RATE_ABOVE_10_PERCENT

Field	Details
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_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. **Cause:** This alert fires when more than 10% of all HTTP responses for the PCF (CHF connector the PCF component that calls the external CHF via nchf-spendinglimitcontrol) over the past day are non-2xx (i.e., not successful). This may be due to: • External CHF partial outage or dependency failures. • Application-level errors (5xx) or timeouts on the CHF path. • Client/bad requests (4xx) from the CHF connector due to schema/version or auth issues. • Misconfiguration, rate limiting/throttling, TLS/mTLS or DNS problems, or resource exhaustion. **Diagnostic Information:** • Break down error rates by response class (4xx vs 5xx vs timeouts/TLS/connect resets). • Search CHF connector service logs and traces for recurring errors, stack traces, circuit-breaker events, or congestion. • Validate external CHF health and dependencies (service/DB), and check for throttling indicators. • Analyze recent deployments or configuration changes in PCF or CHF (endpoints, timeouts, retries, API versions). • Check for traffic spikes, connection pool saturation, CPU/memory pressure, or elevated latency. **Recovery:** • **Identify and address root cause:** Use error breakdown, logs, and traces to pinpoint whether the issue is in the PCF CHF client, network/TLS/auth, or the external CHF. • **Roll back recent changes:** Temporarily revert relevant PCF/CHF deployments or configs if correlated with the onset. • **Scale or resource adjustment:** Increase capacity or tune connection/thread pools; enable autoscaling if appropriate. • **Rate limiting or throttling:** Use bounded retries with backoff and apply throttling to reduce cascading failures. **Alert resolution:** Once the non-2xx rate remains below 10% for a sustained period (1 day), the alert will auto-resolve. For any additional guidance, contact My Oracle Support.

5.1.2.61 PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Table 5-194 PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	Ingress Timeout Error Rate detected above 10 Percent of Total towards CHF service (current value is: {{ $value }})
Summary	Timeout Error Rate detected above 10 Percent of Total Transactions
Severity	Major
Expression	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"}

Table 5-194 (Cont.) PCF_CHF_INGRESS_TIMEOUT_ERROR_ABOVE_MAJOR_THRESHOLD

Field	Details
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. **Cause:** This alert is triggered when more than 10% of all inbound requests from PCF (Policy Control Function) to the CHF (`nchf-spendinglimitcontrol`) time out over a 1-day window. This may impact charging, quota enforcement, or service delivery. Common causes include: • Network latency, intermittent packet loss, or connectivity issues between PCF and CHF • Overload, resource congestion, or unresponsiveness in the CHF or its dependencies • Resource exhaustion or scaling limits in the PCF, CHF, or intermediary components • Misconfiguration of timeout thresholds, retries, or circuit breaker settings • Downstream service or database issues affecting CHF's ability to respond in time • Recent changes or deployments that introduced performance bottlenecks or regressions **Diagnostic Information:** • Identify which part of the infrastructure is experiencing timeouts: is it consistent across all traffic or localized? • Review logs from PCF, CHF, and network/security appliances for repeated timeout, retry, or connection reset events • Check health dashboards for CHF (CPU, memory, response latency, DB availability, etc.) • Analyze request/response timings, queue lengths, and backlog at ingress points • Correlate with recent deployment, scaling, or network changes • Examine resource usage and pod health for PCF and CHF components **Recovery:** • **Isolate the root cause:** Use logs and health metrics to determine if the problem is with CHF availability, network path, or PCF. • **Scale or optimize:** Increase resources, scale instances, or optimize configuration for PCF and CHF services as needed. • **Rollback if needed:** If the alert correlates with new deployments or config changes, consider reverting. • **Network remediation:** Address any identified network latency, packet loss, or DNS resolution issues. • **Tune configuration:** Adjust timeout settings, connection pools, and retry logic based on observed conditions. • **Coordinate:** Engage CHF, PCF, and platform support teams as needed for collaborative troubleshooting. **Alert Resolution:** This alert will auto-resolve once the ingress timeout error rate drops below 10% of total requests to CHF over the evaluation window. For any additional guidance, contact My Oracle Support.

5.1.2.62 PCF_PENDING_BINDING_SITE_TAKEOVER

Table 5-195 PCF_PENDING_BINDING_SITE_TAKEOVER

Field	Details
Description	The site takeover configuration has been activated
Summary	The site takeover configuration has been activated
Severity	CRITICAL
Expression	sum by (application, container, namespace) (changes(occnp_pending_binding_site_takeover[2m])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.45
Metric Used	occnp_pending_binding_site_takeover
Recommended Actions	**Cause:** This alert fires when the site takeover functionality is engaged to handle geo-redundancy scenarios. Site takeover is typically activated when a site in a distributed PCF deployment is down or unreachable, empowering another site to process that site's pending binding operations for service continuity. **Diagnostic Information:** • Check configuration to confirm the alternate site profile is correctly set and the takeover flag is enabled. • Examine PendingOperation records to ensure the alternate site is processing entries from the down site's site ID. • Review service logs for site takeover-related events, handoff messages, and any associated errors during takeover or operation processing. **Recovery & Actions:** • **Verify** that site takeover activation was intentional and aligns with fail-over or DR (Disaster Recovery) procedures. • **Monitor** processing of pending operations for successful handoff and completion under the alternate site. • **Communicate** with relevant operations/support teams about the takeover to prevent conflicting operations. • **Disable site takeover** once the original site is restored to normal operation, so pending operations revert to their standard ownership and workflow. • **Audit** for any missed or failed operations during the site handover, and remediate as needed. **Alert Resolution:** The alert will auto-resolve once there are no new site takeover events, and the takeover configuration is deactivated or no longer required. For any additional guidance, contact My Oracle Support.

5.1.2.63 PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Table 5-196 PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Field	Details
Description	The Pending Operation table threshold has been reached.
Summary	The Pending Operation table threshold has been reached.
Severity	CRITICAL
Expression	sum by (application, container, namespace) (changes(occnp_threshold_limit_reached_total[2m])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.46

Table 5-196 (Cont.) PCF_PENDING_BINDING_THRESHOLD_LIMIT_REACHED

Field	Details
Metric Used	occnp_threshold_limit_reached_total
Recommended Actions	**Cause** This alert fires when the number of records in the Pending Operation table (to reattempt binding registration in BSF at a later time) reaches a predefined threshold. This means the system's retry or pending queue for binding operations is saturated and may be at risk of delaying, or failing new operations. Exceeding this threshold typically signals that retry or binding registrations are not clearing at an expected rate. Common causes include: • Persistent errors or failures from BSF in response to binding attempts, triggering retries • Widespread or systemic service degradation in BSF, Binding Service, or network paths • Application bugs resulting in stuck or orphaned PendingOperation records • Misconfigured thresholds, retry intervals, or logic in SM or Binding Service • Resource starvation (CPU, memory, DB connections) preventing timely processing of pending operations • Recent deployments, configuration updates, or load spikes overwhelming the binding flow **Diagnostic Information** • Check the volume, age, and growth trend of records in the Pending Operation table • Correlate with other alerts or incident tickets related to BSF, Binding Service, network, or DB health • Analyze logs from SM Service, Binding Service, and (if applicable) Audit Service for repeated errors, retry loops, or slow processing • Review recent deployments or configuration changes to PCF Service components • Inspect resource utilization for relevant pods, containers, and backend storage • Confirm correct configuration of the threshold limit, retry intervals, and error code handling **Recovery** • **Prioritize clearing pending records:** Investigate and remediate the root cause(s) of unprocessed binding operations (BSF issues, infra bottlenecks, logic bugs) • **Scale resources or prioritize processing:** Add capacity or redistribute load if resource constraints are found • **Tune configuration:** Adjust thresholds, error code mappings, and retry intervals as necessary • **Audit retry and cleanup logic:** Ensure orphaned or stale records are purged and retry logic is functioning as intended • **Rollback if needed:** If issue began with a recent deployment or config change, consider reverting • **Coordinate across teams:** Engage with BSF, Infrastructure, and DB owners as required **Alert resolution:** The alert will auto-resolve once the number of records in the Pending Operation table returns below the configured threshold and normal processing resumes. For any additional guidance, contact My Oracle Support.

5.1.2.64 PCF_PENDING_BINDING_RECORDS_COUNT

Table 5-197 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
Expression	sum by (application, container, namespace) (changes(occnp_pending_operation_records_count[10s])) > 0
OID	1.3.6.1.4.1.323.5.3.52.1.2.47
Metric Used	occnp_pending_operation_records_count
Recommended Actions	**Cause** This alert fires when a new pending binding operation is inserted into the system by the SM Service(to reattempt binding registration in BSF at a later time). This typically happens when the BSF reattempt settings are configured and the response from BSF to a binding registration indicates an error condition that requires a retry (as per pre-configured error codes). Common causes for entries in the PendingOperation table include:Common causes include: • BSF returns a transient or retry-eligible error code in response to binding requests. • Temporary unavailability or instability of BSF or related network paths. • Application bugs leading to improper handling of BSF responses or retry logic. • Recent configuration changes impacting retry or error handling logic. **Diagnostic Information** • Review SM Service and binding service logs to trace binding requests, BSF response codes, and the creation/updating of PendingOperations. • Verify resource utilization and health across relevant pods or containers. • Analyze timing and Volume of pending operation records—spikes may indicate regression or external service instability. **Recovery** • **Monitor pending operation clearance:** Confirm that retries triggered by Audit Service notifications are processed and successfully clear pending records. • **Investigate recurring or persistent errors:** If retries are frequently required or repeatedly fail, drill down to BSF responses, retry outcomes, and any correlated infrastructure issues. • **Coordinate with BSF/service owners:** If an underlying BSF or network problem persists, work with those teams to restore normal registration flow. • **Tune configuration:** Adjust error code mapping, retry intervals, or thresholds based on observed workload and service behavior. • **Rollback if needed:** Revert recent deployments or config updates if they correlate with spikes in pending operations. **Alert resolution:** The alert will auto-resolve when new pending binding operation records are no longer being routinely created, retries are succeeding, and the overall pending queue stabilizes or clears. For any additional guidance, contact My Oracle Support.

5.1.2.65 AUTONOMOUS_SUBSCRIPTION_FAILURE

Table 5-198 AUTONOMOUS_SUBSCRIPTION_FAILURE

Field	Details
Description	Autonomous subscription failed for a configured Slice Load Level
Summary	Autonomous subscription failed for a configured Slice Load Level
Severity	Critical
Expression	The number of failed Autonomous Subscription for a configured Slice Load Level in nwdaf-agent is greater than zero.
OID	1.3.6.1.4.1.323.5.3.52.1.2.49
Metric Used	subscription_failure{requestType="autonomous"}

Table 5-198 (Cont.) AUTONOMOUS_SUBSCRIPTION_FAILURE

Field	Details
Recommended Actions	The alert gets cleared when the failed Autonomous Subscription is corrected. To clear the alert, perform the following steps: 1. Delete the Slice Load Level configuration. 2. Re-provision the Slice Load Level configuration. **Cause:** This alert activates when there is at least one autonomous subscription (such as the NWDAF event subscription process) failure detected for a given S-NSSAI, indicating that the system was unable to successfully initiate or maintain a subscription for a specific network slice. Common causes may include: • Remote service (e.g., NWDAF) is unavailable, responds with a failure, or returns an error code. • Authentication/authorization failures (invalid tokens, credentials, certificates). • Incorrect, missing, or unsupported subscription parameters (S-NSSAI, event types, notification targets). • API version or schema mismatches between subscribing and serving systems. • Rate limiting, resource exhaustion, or capacity constraints in remote service. • Network or DNS/connectivity problems between components. • Recent deployment or configuration change introducing new issues. **Diagnostic Information:** • Check which S-NSSAI (network slice) is affected using the alert labels. • Review NWDAF gent service logs, and collect relevant error codes and messages from the failed subscription attempts. • Examine recent changes or deployments to the NWDAF Agent, remote NWDAF, or related interfaces/services. • Assess service health and connectivity between the agent and NWDAF (latency, errors, authentication status). • Validate the subscription request payload, endpoint URLs, and configuration for the target S-NSSAI. • Look for evidence of transient or repeated network/service issues. **Recovery:** • **Identify the failed subscription(s):** Use the alert labels and logs to pinpoint the slice(s) affected. • **Resolve remote or local service issues:** Work with relevant teams to restore NWDAF or agent functionality, address authentication or network problems, or resolve configuration mismatches. • **Retry or re-initiate subscriptions** as needed after addressing the root cause. • **Rollback changes** if the alert coincides with recent deployments, configuration modifications, or rollouts. **Alert Resolution:** This alert will automatically resolve once the system detects that there are no new autonomous subscription failures (i.e., no new increments in the failure counter) for the affected S-NSSAI(s) within the evaluation window. Successful re-establishment or correction will clear the alert. For any additional guidance, contact My Oracle Support.

5.1.2.66 AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Table 5-199 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
Expression	(sum(rate(http_out_conn_response_total{pod=~".*amservice.*",responseCode!~"2.*",servicename3gpp="npcf-am-policy-control"}[1d])) / sum(rate(http_out_conn_response_total{pod=~".*amservice.*",servicename3gpp="npcf-am-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.54
Metric Used	http_out_conn_response_total

Table 5-199 (Cont.) AM_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert triggers when 1% or more of notification requests sent from the AM service (part of PCF) to the AMF (`npcf-am-policy-control` endpoint) result in non-2xx (unsuccessful) responses over a 1-day window. These notifications inform AMF about access or mobility events. A significant portion of errors could be 404 responses, which occur when AMF does not have the corresponding session in its context. This may indicate attempts to notify AMF about sessions that have already ended or were never established. Other possible causes include: • Partial outage, degradation, or overload in the AMF • Application errors in the AM service or AMF (e.g., other 4xx or 5xx codes) • Schema or API mismatches due to recent deployments or configuration changes • Authentication, authorization, or TLS certificate issues • Network/connectivity problems • Resource exhaustion in the AMF **Diagnostic Information** • Break down non-2xx responses by HTTP status code, especially 404 versus other 4xx/5xx • Examine AM service and AMF logs for detailed error messages and patterns • Review session establishment, update, and termination flows in both AM service and AMF • Investigate recent deployments, configuration changes, or spikes in error rates • Assess resource usage and health of both AM service and AMF • Validate API contracts, payload formats, and endpoint configurations • Check for authentication/authorization or certificate issues **Recovery** • **Identify and resolve the root cause:** Use logs, traces, and error breakdowns to determine if high 404 rates are expected (due to session lifecycle), or if there is a systematic issue such as stale notifications • **Tune notification logic:** Adjust workflows to minimize duplicate or late notifications when sessions may already have ended • **Rollback or adjust recent changes:** If errors correlate with deployments or config updates, consider reverting them • **Scale or adjust resources:** Add capacity or tune connection/timeouts if resource exhaustion is present • **Remediate network or security problems:** Ensure stable communication and correct authentication/certificates between PCF and AMF **Alert resolution:** The alert will auto-resolve when the error rate drops below 1% over the measuring window For any additional guidance, contact My Oracle Support.

5.1.2.67 AM_AR_ERROR_RATE_ABOVE_1_PERCENT

Table 5-200 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
Expression	(sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*amservice.*",responseCode!~"2.*",servicename3gpp="npcf-am-policy-control"}[1d])) / sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*amservice.*",servicename3gpp="npcf-am-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.55
Metric Used	ocpm_ar_response_total

Table 5-200 (Cont.) AM_AR_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert fires when 1% or more of alternate routing (AR) requests initiated by the AM service (as part of PCF) to AMF (`npcf-am-policy-control`) result in non-2xx (unsuccessful) responses over a 1-day window, grouped by FQDN. Alternate routing is the process of retrying the original request to a different AMF instance when the initial attempt fails. A rising AR error rate suggests persistent issues with connectivity, service health, or configuration for primary or alternate AMF endpoints. Typical causes include: • Persistent unavailability, overload, or partial outages affecting some or all AMF instances • Application-level errors from AMF (many 4xx/5xx responses, including 404s for missing sessions) • Schema or API incompatibility after deployments or configuration changes • Authentication, authorization, or certificate-related failures during retries • Network or DNS problems affecting communication with one or more AMF instances • Resource exhaustion, scaling issues, or retry storm in the AM service • Misconfiguration of alternate endpoint lists or retry logic **Diagnostic Information** • Break down failed AR responses by HTTP status code (4xx, 5xx, timeouts) to pinpoint the failure type • Review AM service logs to identify why alternate routing was triggered and the response from each retry • Inspect AMF logs for errors and session context associated with AR requests • Assess health, status, and readiness of all AMF endpoints relevant to the alerting FQDN • Check authentication credentials, certificate validity, and endpoint configuration • Correlate AR error spikes with recent deployments, updates, scaling actions, or network incidents • Analyze retry logic to ensure backoff and failover policies are working as expected **Recovery** • **Isolate the root cause:** Use logs and metrics to determine if AR failures are due to persistent AMF unavailability, configuration problems, or retry logic bugs • **Remediate endpoint or network issues:** Restore AMF health, increase capacity, or fix network connectivity to all AMF endpoints • **Fix authentication or certificate problems:** Update or refresh security credentials as necessary • **Adjust or rollback changes as needed:** If increased errors align with a recent deployment or config update • **Tune retry/backoff policies:** Update AR configuration to minimize repeated failures or retry storms **Alert resolution:** The alert auto-resolves once the AR error rate drops below 1% over the measurement window For any additional guidance, contact My Oracle Support.

5.1.2.68 UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Table 5-201 UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Description	UE Notification Error Rate detected above 1 Percent of Total (current value is: {{ $value }})
Summary	UE Notification Error Rate detected above 1 Percent of Total (current value is: {{ $value }})
Severity	MINOR
Expression	(sum(rate(http_out_conn_response_total{pod=~".*ueservice.*",responseCode!~"2.*",servicename3gpp="npcf-ue-policy-control"}[1d])) / sum(rate(http_out_conn_response_total{pod=~".*ueservice.*",servicename3gpp="npcf-ue-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.56
Metric Used	http_out_conn_response_total

Table 5-201 (Cont.) UE_NOTIFICATION_ERROR_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert triggers when 1% or more of notification requests sent from the UE service (part of PCF) to the AMF (npcf-ue-policy-control endpoint) result in non-2xx (unsuccessful) responses over a 1-day window. These notifications inform AMF about UE policy events. A significant portion of errors could be 404 responses, which occur when AMF does not have the corresponding session in its context. This may indicate attempts to notify AMF about sessions that have already ended or were never established. Other possible causes include: • Partial outage, degradation, or overload in the AMF • Application errors in the AM service or AMF (e.g., other 4xx or 5xx codes) • Schema or API mismatches due to recent deployments or configuration changes • Authentication, authorization, or TLS certificate issues • Network/connectivity problems • Resource exhaustion in the AMF **Diagnostic Information** • Break down non-2xx responses by HTTP status code, especially 404 versus other 4xx/5xx • Examine AM service and AMF logs for detailed error messages and patterns • Review session establishment, update, and termination flows in both AM service and AMF • Investigate recent deployments, configuration changes, or spikes in error rates • Assess resource usage and health of both AM service and AMF • Validate API contracts, payload formats, and endpoint configurations • Check for authentication/authorization or certificate issues **Recovery** • **Identify and resolve the root cause:** Use logs, traces, and error breakdowns to determine if high 404 rates are expected (due to session lifecycle), or if there is a systematic issue such as stale notifications • **Tune notification logic:** Adjust workflows to minimize duplicate or late notifications when sessions may already have ended • **Rollback or adjust recent changes:** If errors correlate with deployments or config updates, consider reverting them • **Scale or adjust resources:** Add capacity or tune connection/timeouts if resource exhaustion is present • **Remediate network or security problems:** Ensure stable communication and correct authentication/certificates between PCF and AMF **Alert resolution:** The alert will auto-resolve when the error rate drops below 1% over the measuring window For any additional guidance, contact My Oracle Support.

5.1.2.69 UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Table 5-202 UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Field	Details
Description	Alternate Routing Error Rate detected above 1 Percent of Total on UE Service (current value is: {{ $value }})

Table 5-202 (Cont.) UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Field	Details
Summary	Transaction Error Rate detected above 1 Percent of Total Transactions on UE Alternate Routing
Severity	MINOR
Expression	(sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*ueservice.*",responseCode!~"2.*",servicename3gpp="npcf-ue-policy-control"}[1d])) / sum by (fqdn) (rate(ocpm_ar_response_total{pod=~".*ueservice.*",servicename3gpp="npcf-ue-policy-control"}[1d]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.57
Metric Used	ocpm_ar_response_total

Table 5-202 (Cont.) UE_AR_FAILURE_RATE_ABOVE_1_PERCENT

Field	Details
Recommended Actions	**Cause** This alert fires when 1% or more of alternate routing (AR) requests initiated by the AM service (as part of PCF) to AMF (npcf-ue-policy-control) result in non-2xx (unsuccessful) responses over a 1-day window, grouped by FQDN. Alternate routing is the process of retrying the original request to a different AMF instance when the initial attempt fails. A rising AR error rate suggests persistent issues with connectivity, service health, or configuration for primary or alternate AMF endpoints. Typical causes include: • Persistent unavailability, overload, or partial outages affecting some or all AMF instances • Application-level errors from AMF (many 4xx/5xx responses, including 404s for missing sessions) • Schema or API incompatibility after deployments or configuration changes • Authentication, authorization, or certificate-related failures during retries • Network or DNS problems affecting communication with one or more AMF instances • Resource exhaustion, scaling issues, or retry storm in the AM service • Misconfiguration of alternate endpoint lists or retry logic **Diagnostic Information** • Break down failed AR responses by HTTP status code (4xx, 5xx, timeouts) to pinpoint the failure type • Review AM service logs to identify why alternate routing was triggered and the response from each retry • Inspect AMF logs for errors and session context associated with AR requests • Assess health, status, and readiness of all AMF endpoints relevant to the alerting FQDN • Check authentication credentials, certificate validity, and endpoint configuration • Correlate AR error spikes with recent deployments, updates, scaling actions, or network incidents • Analyze retry logic to ensure backoff and failover policies are working as expected **Recovery** • **Isolate the root cause:** Use logs and metrics to determine if AR failures are due to persistent AMF unavailability, configuration problems, or retry logic bugs • **Remediate endpoint or network issues:** Restore AMF health, increase capacity, or fix network connectivity to all AMF endpoints • **Fix authentication or certificate problems:** Update or refresh security credentials as necessary • **Adjust or rollback changes as needed:** If increased errors align with a recent deployment or config update • **Tune retry/backoff policies:** Update AR configuration to minimize repeated failures or retry storms **Alert resolution:** The alert auto-resolves once the AR error rate drops below 1% over the measurement window For any additional guidance, contact My Oracle Support.

5.1.2.70 SMSC_CONNECTION_DOWN

Table 5-203 SMSC_CONNECTION_DOWN

Field	Details
Description	Connection to SMSC peer {{$labels.smscName}} is down in notifier service pod {{$labels.pod}}
Summary	Connection to SMSC peer {{$labels.smscName}} is down in notifier service pod {{$labels.pod}}
Severity	MAJOR
Expression	sum by(namespace, pod, smscName)(occnp_active_smsc_conn_count) == 0
OID	`1.3.6.1.4.1.323.5.3.52.1.2.63`
Metric Used	occnp_active_smsc_conn_count

Table 5-203 (Cont.) SMSC_CONNECTION_DOWN

Field	Details
Recommended Actions	**Cause** This alert fires when the connection count to a specific SMSC (Short Message Service Center) peer (`smscName`) drops to zero in a notifier service pod. This means that the notifier service in the indicated pod has lost connectivity with the SMSC peer, which may halt or delay SMS delivery for affected sessions. Common causes include: • Network connectivity issues between the notifier pod and the SMSC peer (latency, packet loss, firewall changes) • SMSC peer instance is offline, unresponsive, or undergoing maintenance • Unexpected restart or crash of the notifier service pod • TCP session timeout, reset, or socket exhaustion • TLS/certificate negotiation failures (if applicable) • Misconfiguration of SMSC endpoint, port, or authentication details • Recent pod or infrastructure changes affecting networking or endpoints **Diagnostic Information** • Identify which `namespace`, `pod`, and `smscName` are affected from alert labels • Check notifier pod logs for errors, timeouts, or repeated reconnection attempts to the SMSC • Confirm SMSC peer health and status via monitoring tools or coordination with peer's operations • Validate network connectivity (test with ping/telnet/traceroute), DNS resolution, and firewall or security rules • Review recent changes in deployment, SMSC endpoint configuration, or certificate rotation • Check for underlying resource issues (CPU, memory, open file/socket limits) on the notifier pod **Recovery** • **Restore connectivity:** Address any network or firewall problems between the notifier pod and SMSC peer • **Restart services:** If the notifier pod is in a bad state, restart it to reestablish the connection • **Engage SMSC operations:** If the peer is down, coordinate with the SMSC provider/team to restore service • **Correct configuration:** Verify endpoint settings, authentication, and port assignments in both notifier and SMSC • **Rollback recent changes:** If disconnection began after deployment or configuration change, consider reverting **Alert resolution:** The alert will auto-resolve once the connection count returns above zero for the affected pod and SMSC For any additional guidance, contact My Oracle Support.

5.1.2.71 LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Table 5-204 LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Field	Details
Name in Alert Yaml File	lockAcquisitionExceedsMinorThreshold
Description	The lock requests fails to acquire the lock count exceeds the minor threshold limit. The (current value is: {{ $value }})

Table 5-204 (Cont.) LOCK_ACQUISITION_EXCEEDS_MINOR_THRESHOLD

Field	Details
Summary	Keys used in Bulwark lock request which are already in locked state detected above 20 Percent of Total Transactions.
Severity	Minor
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >=20 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, between 20% and 50% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 20%. If the rate exceeds 50%, a higher severity alert will trigger.

5.1.2.72 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Table 5-205 LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Name in Alert Yaml File	lockAcquisitionExceedsMajorThreshold
Description	The lock requests fails to acquire the lock count exceeds the major threshold limit. The (current value is: {{ $value }})
Summary	Keys used in Bulwark lock request which are already in locked state detected above 50 Percent of Total Transactions.
Severity	Major
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >= 50 < 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total

Table 5-205 (Cont.) LOCK_ACQUISITION_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, between 50% and 75% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 50%. If the rate exceeds 75%, a higher severity alert will trigger.

5.1.2.73 LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Table 5-206 LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Name in Alert Yaml File	lockAcquisitionExceedsCriticalThreshold
Description	The lock requests fails to acquire the lock count exceeds the critical threshold limit. The (current value is: {{ $value }})
Summary	Keys used in Bulwark lock request which are already in locked state detected above 75 Percent of Total Transactions.
Severity	Critical

Table 5-206 (Cont.) LOCK_ACQUISITION_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Expression	(sum by (namespace) (increase(lock_response_total{requestType="acquireLock",responseType="failure"} [5m])) /sum by (namespace) (increase(lock_request_total{requestType="acquireLock"} [5m]))) * 100 >=75
OID	1.3.6.1.4.1.323.5.3.52.1.2.69
Metric Used	lock_request_total
Recommended Actions	**Cause** This alert fires when, within a 5-minute window, above 75% of lock acquisition requests (acquireLock) to the **Bulwark** service in any namespace fail. Elevated lock acquisition failure rates may indicate: • Lock contention, with multiple clients attempting to acquire the same lock/ resource concurrently (hot spots) • Stale or orphaned locks that are not being properly released • Performance degradation or partial outages in the Coherence distributed cache backend used by Bulwark • Misconfigured lock TTL (time to live), expiry, or retry/backoff policies • Recent deployment, scaling events, or increased load causing higher lock demand or contention • Bugs in the client logic resulting in frequent or incorrect lock requests **Diagnostic Information** • Identify affected namespaces and resources prone to high contention or failure • Examine Bulwark and application logs for specific lock acquisition errors or contention/wait messages • Review the health of the bulwark service(and coherence cluster), including resource utilization (CPU, memory) • Check lock TTL and cleanup mechanisms to ensure timely lock release by both typical and failure pathways • Analyze trends following deployments, configuration changes, or traffic spikes • Assess and validate the configuration for Bulwark (connection pools, timeouts, backoff settings) • Investigate for node clock skew, which can impact distributed locking **Recovery** • **Reduce Contention:** Identify and resolve any traffic pattern that causes lock contention • **Backend Remediation:** Scale or optimize Bulwark and address any backend health issues • **Configuration Tuning:** Adjust TTLs, retry intervals, and backoff strategies for optimal application behavior • **Rollback if Needed:** Revert recent changes to Bulwark deployments or configurations if correlated to failure spikes **Alert Resolution:** Alert will auto-resolve once lock acquisition failure rates in a namespace drop below 75%.

5.1.2.74 SM_UPDATE_NOTIFY_FAILED_ABOVE_50_PERCENT

Table 5-207 SM_UPDATE_NOTIFY_FAILED_ABOVE_50_PERCENT

Field	Details
Description	Update Notify Terminate sent to SMF failed >= 50 < 60

Table 5-207 (Cont.) SM_UPDATE_NOTIFY_FAILED_ABOVE_50_PERCENT

Field	Details
Summary	Update Notify Terminate sent to SMF failed >= 50 < 60
Severity	MINOR
Expression	(sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol",responseCode!~"2.*"})*100)/ sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol"}) >= 50 < 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.80
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause** This alert fires when, over the evaluation period, between 50% and 60% of `terminate_notify` HTTP outbound requests sent from PCF (SM Service pods) to SMF result in non-2xx (failed) HTTP responses. In this workflow, PCF notifies SMF to terminate a session. Notably, SMF will return a 404 error if the session does not exist in its current context. Elevated rates of 404 errors could indicate attempts to terminate already-removed sessions or stale references. Other common causes include: • SMF service partial outage or overload • Application-level errors (4xx other than 404, 5xx) • Network issues • Configuration mistakes • Recent deployments or system changes **Diagnostic Information** • Break down non-2xx responses by HTTP code (especially distinguishing 404s from 5xx or other 4xx) • Check PCF and SM Service logs for error details related to `terminate_notify` requests • Review SMF logs for the context and reasoning behind 404 responses • Analyze the timing and volume of session termination requests compared to active session counts • Correlate with recent maintenance, scaling events, or deployment changes • Evaluate resource utilization and connectivity between PCF and SMF **Recovery** • **Determine Root Cause:** Use error codes, logs, and traces to identify whether high 404s are expected (e.g., requests for sessions already removed) or whether there are issues with session tracking, race conditions, or stale data • **Rollback if Needed:** If recent changes coincide with failures, consider rolling back deployments or configurations. • **Scale/Resources:** Address resource exhaustion or performance bottlenecks as needed **Alert Resolution:** The alert will auto-resolve once failed response rates fall below 50% for the evaluation window. A higher-severity alert may trigger if failures exceed 60%. For any additional guidance, contact My Oracle Support.

5.1.2.75 SM_UPDATE_NOTIFY_FAILED_ABOVE_60_PERCENT

Table 5-208 SM_UPDATE_NOTIFY_FAILED_ABOVE_60_PERCENT

Field	Details
Description	Update Notify Terminate sent to SMF failed >= 60 < 70
Summary	Update Notify Terminate sent to SMF failed >= 60 < 70
Severity	MAJOR
Expression	(sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol",responseCode!~"2.*"})*100)/ sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol"}) >= 60 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.80
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause** This alert fires when, over the evaluation period, between 60% and 70% of `terminate_notify` HTTP outbound requests sent from PCF (SM Service pods) to SMF result in non-2xx (failed) HTTP responses. In this workflow, PCF notifies SMF to terminate a session. Notably, SMF will return a 404 error if the session does not exist in its current context. Elevated rates of 404 errors could indicate attempts to terminate already-removed sessions or stale references. Other common causes include: • SMF service partial outage or overload • Application-level errors (4xx other than 404, 5xx) • Network issues • Configuration mistakes • Recent deployments or system changes **Diagnostic Information** • Break down non-2xx responses by HTTP code (especially distinguishing 404s from 5xx or other 4xx) • Check PCF and SM Service logs for error details related to `terminate_notify` requests • Review SMF logs for the context and reasoning behind 404 responses • Analyze the timing and volume of session termination requests compared to active session counts • Correlate with recent maintenance, scaling events, or deployment changes • Evaluate resource utilization and connectivity between PCF and SMF **Recovery** • **Determine Root Cause:** Use error codes, logs, and traces to identify whether high 404s are expected (e.g., requests for sessions already removed) or whether there are issues with session tracking, race conditions, or stale data • **Rollback if Needed:** If recent changes coincide with failures, consider rolling back deployments or configurations. • **Scale/Resources:** Address resource exhaustion or performance bottlenecks as needed **Alert Resolution:** The alert will auto-resolve once failed response rates fall below 60% for the evaluation window. A higher-severity alert may trigger if failures exceed 70%. For any additional guidance, contact My Oracle Support.

5.1.2.76 SM_UPDATE_NOTIFY_FAILED_ABOVE_70_PERCENT

Table 5-209 SM_UPDATE_NOTIFY_FAILED_ABOVE_70_PERCENT

Field	Details
Description	Update Notify Terminate sent to SMF failed >= 70
Summary	Update Notify Terminate sent to SMF failed >= 70
Severity	CRITICAL
Expression	(sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol",responseCode!~"2.*"})*100)/ sum(occnp_http_out_conn_response_total{operationType="terminate_notify",pod=~".*smservice.*",servicename3gpp="npcf-smpolicycontrol"}) >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.80
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	**Cause** This alert fires when, over the evaluation period, above 70% of `terminate_notify` HTTP outbound requests sent from PCF (SM Service pods) to SMF result in non-2xx (failed) HTTP responses. In this workflow, PCF notifies SMF to terminate a session. Notably, SMF will return a 404 error if the session does not exist in its current context. Elevated rates of 404 errors could indicate attempts to terminate already-removed sessions or stale references. Other common causes include: • SMF service partial outage or overload • Application-level errors (4xx other than 404, 5xx) • Network issues • Configuration mistakes • Recent deployments or system changes **Diagnostic Information** • Break down non-2xx responses by HTTP code (especially distinguishing 404s from 5xx or other 4xx) • Check PCF and SM Service logs for error details related to `terminate_notify` requests • Review SMF logs for the context and reasoning behind 404 responses • Analyze the timing and volume of session termination requests compared to active session counts • Correlate with recent maintenance, scaling events, or deployment changes • Evaluate resource utilization and connectivity between PCF and SMF **Recovery** • **Determine Root Cause:** Use error codes, logs, and traces to identify whether high 404s are expected (e.g., requests for sessions already removed) or whether there are issues with session tracking, race conditions, or stale data • **Rollback if Needed:** If recent changes coincide with failures, consider rolling back deployments or configurations. • **Scale/Resources:** Address resource exhaustion or performance bottlenecks as needed **Alert Resolution:** The alert will auto-resolve once failed response rates fall below 70%. For any additional guidance, contact My Oracle Support.

5.1.2.77 UPDATE_NOTIFY_FAILURE_ABOVE_30_PERCENT

Table 5-210 UPDATE_NOTIFY_FAILURE_ABOVE_30_PERCENT

Field	Details
Description	{{ $value }} % of update notify sent to SMF that failed.
Summary	More than 30% of update notify sent to SMF failed
Severity	minor
Expression	sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.94
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	`occnp_http_out_conn_response_total` metric is pegged when PCF receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of update-notify failure coming from SMF. If there is an increase of update-notify failure operator can revise if all the flows that trigger update-notify are failing or analyze which flow is failing the most or if the SMF that request are going to is unhealthy. For any additional guidance, contact My Oracle Support.

5.1.2.78 UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT

Table 5-211 UPDATE_NOTIFY_FAILURE_ABOVE_50_PERCENT

Field	Details
Description	Number of Update notify that failed is equal or above 50% but less than 70% in a given time period
Summary	Number of Update notify that failed is equal or above 50% but less than 70% in a given time period
Severity	MAJOR
Expression	(sum by (namespace) (rate(**occnp_http_out_conn_response_total**{operationType="update_notify",microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(**occnp_http_out_conn_response_total**{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.94
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	`occnp_http_out_conn_response_total` metric is pegged when PCF receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of update-notify failure coming from SMF. If there is an increase of update-notify failure operator can revise if all the flows that trigger update-notify are failing or analyze which flow is failing the most or if the SMF that request are going to is unhealthy. For any additional guidance, contact My Oracle Support.

5.1.2.79 UPDATE_NOTIFY_FAILURE_ABOVE_70_PERCENT

Table 5-212 UPDATE_NOTIFY_FAILURE_ABOVE_70_PERCENT

Field	Details
Description	{{ $value }} % of update notify sent to SMF that failed
Summary	More than 70% of update notify sent to SMF failed
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm",responseCode!~"2.*"}[5m])) / sum by (namespace) (rate(occnp_http_out_conn_response_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.94
Metric Used	occnp_http_out_conn_response_total
Recommended Actions	`occnp_http_out_conn_response_total` metric is pegged when PCF receives a response from a message that is going out of the NF. In this case the alert is notifying when there is a certain amount of update-notify failure coming from SMF. If there is an increase of update-notify failure operator can revise if all the flows that trigger update-notify are failing or analyze which flow is failing the most or if the SMF that request are going to is unhealthy. For any additional guidance, contact My Oracle Support.

5.1.2.80 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST

Table 5-213 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST

Field	Details
Description	Ingress Gateway traffic gets rejected more than 1% because of ratelimiting.
Summary	Ingress Gateway traffic gets rejected more than 1% because of ratelimiting.
Severity	Major
Expression	(sum by (namespace,pod) (rate(oc_ingressgateway_http_request_ratelimit_values_total {Allowed="false",app_kubernetes_io_name="occnp-ingress-gateway"}[2m])))/ (sum by (namespace,pod) (rate(oc_ingressgateway_http_request_ratelimit_values_total {app_kubernetes_io_name="occnp-ingress-gateway"}[2m]))) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.103
Metric Used	oc_ingressgateway_http_request_ratelimit_values_total

Table 5-213 (Cont.) POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST

Field	Details
Recommended Actions	**Cause:** Alert is triggered when percentage of denied requests is above 1% of total tps.. **Diagnostic Information:** • Metric involved: oc_ingressgateway_http_request_ratelimit_values_total • Error observed: 429 Too Many Requests, NF_CONGESTION_RISK • Cause value: Allowed="false" • Condition: podProtectionByRateLimiting.enabled = true and podProtectionByRateLimiting.fillRate settings • Verification steps: – podProtectionByRateLimiting.fillRate to a lower value and podProtectionByRateLimiting.deniedRequestActions.action=REJECT for lower congestion level – Run 4500 TPS or above for SM traffic; – Confirm some request dropped with Error 429. – Verify that the alert get triggered. • Monitoring recommendations: – Monitor 4xx error; and counter increase for oc_ingressgateway_http_request_ratelimit_values_total{Allowed="false"} – Watch for spikes following client deployments. **Recovery:** • Check Network traffic burst and storm • Investigate traffic load balancer issues and network issues. • Review SM Service Resources • Restart or scale up resources temporarily if the system is congested • Reconfig setting for podProtectionByRateLimiting.fillRate to a higher value and assign podProtectionByRateLimiting.deniedRequestActions.action=REJECT to higher congestion level • Disable feature if this flow is the only one affected we can disable this feature as a last resource For any additional guidance, contact My Oracle Support.

5.1.2.81 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD

Table 5-214 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	UE N1N2 Notification Rate containing request of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 20 Percent of Total n1n2 notify Request.
Summary	UE N1N2 Notification Rate containing request of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 20 Percent of Total n1n2 notify Request.
Severity	Minor
Expression	sum by (namespace) (rate(ue_n1_transfer_ue_notification_total{commandType="MANAGE_UE_POLICY_COMMAND_REJECT"}[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.91
Metric Used	ue_n1_transfer_ue_notification_total

Table 5-214 (Cont.) UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	The ue_n1_transfer_ue_notification_total metric is pegged when a fragment delivered by the PCF (pcf-ue service) is rejected by the UE (User Equipment). So, the operator needs to check on the AMF/UE side why these UPSI/URSP rules were rejected. For any additional guidance, contact My Oracle Support.

5.1.2.82 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD

Table 5-215 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	UE N1N2 Notification Rate containing request of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 50 Percent of Total n1n2 notify Request.
Summary	UE N1N2 Notification Rate containing request of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 50 Percent of Total n1n2 notify Request.
Severity	Major
Expression	sum by (namespace) (rate(ue_n1_transfer_ue_notification_total{commandType="MANAGE_UE_POLICY_COMMAND_REJECT"}[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.91
Metric Used	ue_n1_transfer_ue_notification_total
Recommended Actions	ue_n1_transfer_ue_notification_total metric is pegged when fragment delivered by PCF (pcf-ue service) is rejected by UE (User Equipment). So operator needs to check on AMF/UE side why these UPSI/URSP rules were rejected. For any additional guidance, contact My Oracle Support.

5.1.2.83 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD

Table 5-216 UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	UE N1N2 Notification Rate containing request of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 75 Percent of Total n1n2 notify Request.
Summary	UE N1N2 Notification Rate containing request of MANAGE_UE_POLICY_COMMAND_REJECT from AMF is detected to be above 75 Percent of Total n1n2 notify Request.
Severity	CRITICAL
Expression	sum by (namespace) (rate(ue_n1_transfer_ue_notification_total{commandType="MANAGE_UE_POLICY_COMMAND_REJECT"}[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.91
Metric Used	ue_n1_transfer_ue_notification_total

Table 5-216 (Cont.) UE_N1N2_NOTIFY_REJECTION_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	ue_n1_transfer_ue_notification_total metric is pegged when fragment delivered by PCF (pcf-ue service) is rejected by UE (User Equipment). So operator needs to check on AMF/UE side why these UPSI/URSP rules were rejected. For any additional guidance, contact My Oracle Support.

5.1.2.84 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD

Table 5-217 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	Over 20% percent of total N1N2 transfer requests from AMF are of N1N2 transfer failure notification requests from AMF.
Summary	Above 20 percent of total N1N2 transfer requests from AMF are of N1N2 transfer failure notification requests from AMF.
Severity	Minor
Expression	sum by (namespace) (rate(ue_n1_transfer_failure_notification_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.92
Metric Used	ue_n1_transfer_failure_notification_total
Recommended Actions	ue_n1_transfer_failure_notification_total metric is pegged when PCF receives transfer failure notification from AMF In this case operator needs to check for connectivity issues on AMF and UE - why fragment transfer to UE failed. Also operator might have to check if AMF has proper retransmission and reattempt configurations in place For any additional guidance, contact My Oracle Support.

5.1.2.85 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Table 5-218 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	Over 50% percent of total N1N2 transfer requests from AMF are of N1N2 transfer failure notification requests from AMF.
Summary	Over 50% percent of total N1N2 transfer requests from AMF are of N1N2 transfer failure notification requests from AMF.
Severity	Major
Expression	sum by (namespace) (rate(ue_n1_transfer_failure_notification_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.92
Metric Used	ue_n1_transfer_failure_notification_total

Table 5-218 (Cont.) UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	ue_n1_transfer_failure_notification_total metric is pegged when PCF receives transfer failure notification from AMF In this case operator needs to check for connectivity issues on AMF and UE - why fragment transfer to UE failed. Also operator might have to check if AMF has proper retransmission and reattempt configurations in place. For any additional guidance, contact My Oracle Support.

5.1.2.86 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD

Table 5-219 UE_N1N2_TRANSFER_FAILURE_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	Over 75% percent of total N1N2 transfer requests from AMF are of N1N2 transfer failure notification requests from AMF.
Summary	Over 75% percent of total N1N2 transfer requests from AMF are of N1N2 transfer failure notification requests from AMF.
Severity	Critical
Expression	sum by (namespace) (rate(ue_n1_transfer_failure_notification_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.92
Metric Used	ue_n1_transfer_failure_notification_total
Recommended Actions	ue_n1_transfer_failure_notification_total metric is pegged when PCF receives transfer failure notification from AMF In this case operator needs to check for connectivity issues on AMF and UE - why fragment transfer to UE failed. Also operator might have to check if AMF has proper retransmission and reattempt configurations in place. For any additional guidance, contact My Oracle Support.

5.1.2.87 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD

Table 5-220 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	Over 20% of UE N1N2 transfers have T3501 timer expiry before the N1N2 notify is received from AMF for the respective transfer.
Summary	Over 20% of UE N1N2 transfers have T3501 timer expiry before the N1N2 notify is received from AMF for the respective transfer.
Severity	Minor

Table 5-220 (Cont.) UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MINOR_THRESHOLD

Field	Details
Expression	sum by (namespace) (rate(ue_n1_transfer_t3501_expiry_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.93
Metric Used	ue_n1_transfer_t3501_expiry_total
Recommended Actions	ue_n1_transfer_t3501_expiry_total metric is pegged when PCF was not able to get any N1N2 notification message from AMF before T3501 timer expires In this case operator needs to check on AMF side why N1N2 message was delayed, also connectivity between PCF and AMF needs to be checked If connection between PCF and AMF is not an issue then as workaround operator can increase T3501 timer time by navigating to PCF GUI Service Configuration -> PCF UE Timer Setting section and increasing T3501 Timer Duration field to a bigger value. For any additional guidance, contact My Oracle Support.

5.1.2.88 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD

Table 5-221 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	Over 50% of UE N1N2 transfers have T3501 timer expiry before the N1N2 notify is received from AMF for the respective transfer.
Summary	Over 50% of UE N1N2 transfers have T3501 timer expiry before the N1N2 notify is received from AMF for the respective transfer.
Severity	Major
Expression	sum by (namespace) (rate(ue_n1_transfer_t3501_expiry_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.93
Metric Used	ue_n1_transfer_t3501_expiry_total
Recommended Actions	ue_n1_transfer_t3501_expiry_total metric is pegged when PCF was not able to get any N1N2 notification message from AMF before T3501 timer expires. In this case operator needs to check on AMF side why N1N2 message was delayed, also connectivity between PCF and AMF needs to be checked. If connection between PCF and AMF is not an issue then as workaround operator can increase T3501 timer time by navigating to PCF GUI. Service Configuration -> PCF UE Timer Setting section and increasing T3501 Timer Duration field to a bigger value. For any additional guidance, contact My Oracle Support.

5.1.2.89 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD

Table 5-222 UE_N1N2_TRANSFER_T3501_TIMER_EXPIRY_RATE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	Over 75% of UE N1N2 transfers have T3501 timer expiry before the N1N2 notify is received from AMF for the respective transfer.
Summary	Over 75% of UE N1N2 transfers have T3501 timer expiry before the N1N2 notify is received from AMF for the respective transfer.
Severity	Critical
Expression	sum by (namespace) (rate(ue_n1_transfer_t3501_expiry_total[5m])) / sum by (namespace) (rate(ue_n1_transfer_response_total[5m])) * 100 > 75
OID	1.3.6.1.4.1.323.5.3.52.1.2.93
Metric Used	ue_n1_transfer_t3501_expiry_total
Recommended Actions	ue_n1_transfer_t3501_expiry_total metric is pegged when PCF was not able to get any N1N2 notification message from AMF before T3501 timer expires In this case operator needs to check on AMF side why N1N2 message was delayed, also connectivity between PCF and AMF needs to be checked If connection between PCF and AMF is not an issue then as workaround operator can increase T3501 timer time by navigating to PCF GUI Service Configuration -> PCF UE Timer Setting section and increasing T3501 Timer Duration field to a bigger value For any additional guidance, contact My Oracle Support.

5.1.2.90 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL_THRESHOLD

Table 5-223 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_error_response_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.111
Metric Used	ocpm_handle_update_notify_error_response_as_pending_confirmation_total

Table 5-223 (Cont.) RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_CRITICAL_THRESHOLD

Field	Details
Recommended Actions	Cause: Metric ocpm_handle_update_notify_error_response_as_pending_confirmation_total is pegged when the operation Update Notify towards SMF ends up with an Error • Metrics: ocpm_handle_update_notify_error_response_as_pending_confirmation_total – This will be incremented when configuration flag SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED is enabled and specific error error is added in SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPOMNSE_CODE and timeout happens during update notify triggered by AAR-I and AAR-U. • Alarm Condition: – If more than or equal to 70% of update_notify total requests fails with configured errorCode, an alarm is raised Diagnostic Information: • Check Network Latency – Investigate possible delays in network which is resulting in timeouts • Verify sender information – Verify if the notifUri where we are sending the information is correct • Verify receiver NF – Verify that the SMF that is receiving the traffic is in a healthy state • Review application – Verify if Sm is not congested – If signs like constant error logs are showing – Monitor System/resource utilization (CPU, Memory, queues) Recover: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF and the SM Service. Resolve any high latency or packet loss immediately if detected. • Review SM Service Application and Resources – Restart or scale up resources temporarily if the system is overloaded • Disable feature – if this flow is the only one affected we can disable this feature as a last resource For any additional guidance, contact My Oracle Support.

5.1.2.91 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_THRESHOLD

Table 5-224 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 50% in a given time period.

Table 5-224 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MAJOR_THRESHOLD

Field	Details
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 50% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_error_response_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.111
Metric Used	ocpm_handle_update_notify_error_response_as_pending_confirmation_total
Recommended Actions	Cause: Metric ocpm_handle_update_notify_error_response_as_pending_confirmation_total is pegged when the operation Update Notify towards SMF ends up with an Error • Metrics: ocpm_handle_update_notify_error_response_as_pending_confirmation_total – This will be incremented when configuration flag SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED is enabled and specific error error is added in SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPOMNSE_CODE and timeout happens during update notify triggered by AAR-I and AAR-U. • Alarm Condition: – If more than or equal to 50% but less than 70% of update_notify total requests fails with configured errorCode, an alarm is raised Diagnostic Information: • Check Network Latency – Investigate possible delays in network which is resulting in timeouts • Verify sender information – Verify if the notifUri where we are sending the information is correct • Verify receiver NF – Verify that the SMF that is receiving the traffic is in a healthy state • Review application – Verify if Sm is not congested – If signs like constant error logs are showing – Monitor System/resource utilization (CPU, Memory, queues) Recover: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF and the SM Service. Resolve any high latency or packet loss immediately if detected. • Review SM Service Application and Resources – Restart or scale up resources temporarily if the system is overloaded • Disable feature – if this flow is the only one affected we can disable this feature as a last resource For any additional guidance, contact My Oracle Support.

5.1.2.92 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_THRESHOLD

Table 5-225 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_error_response_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm", responseCode=~"5xx/4xx"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.111
Metric Used	ocpm_handle_update_notify_error_response_as_pending_confirmation_total

Table 5-225 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_ERROR_RESPONSE_ABOVE_MINOR_THRESHOLD

Field	Details
Recommended Actions	Cause: Metric **ocpm_handle_update_notify_error_response_as_pending_confirmation_total** is pegged when the operation **Update Notify** towards SMF ends up with an error. **Metrics:** • **ocpm_handle_update_notify_error_response_as_pending_confirmation_total** – This will be incremented when: * Configuration flag `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED` is enabled, and * A specific error is added in `SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.RESPONSE_CODE`, and * A timeout happens during Update Notify triggered by AAR-I and AAR-U. **Alarm Condition:** • If **≥50% and < 70%** of update_notify total requests fail with the configured error code, an alarm is raised. **Diagnostic Information:** • **Check Network Latency** – Investigate possible delays in the network that are resulting in timeouts. • **Verify Sender Information** – Verify if the `notifUri` where we are sending the information is correct. • **Verify Receiver NF** – Verify that the SMF receiving the traffic is in a healthy state. • **Review Application** – Verify that SM is not congested. – Check for constant error logs. – Monitor system/resource utilization (CPU, memory, queues). **Recover:** • **Check Network Latency and Connectivity** – Investigate any current network issues or bottlenecks between the external NF and the SM service. – Resolve any high latency or packet loss immediately if detected. • **Review SM Service Application and Resources** – Restart or scale up resources temporarily if the system is overloaded. • **Disable Feature** – If this flow is the only one affected, disable this feature as a last resort.

5.1.2.93 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHOLD

Table 5-226 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Summary	This alert is triggered when the number of update notify failed because a timeout is equal or above 70% in a given time period.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_timeout_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.112
Metric Used	ocpm_handle_update_notify_timeout_as_pending_confirmation_total

Table 5-226 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_CRITICAL_THRESHOLD

Field	Details

Recommended Actions	**Cause:**
	Metric **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** is pegged when the **Update Notify** operation towards SMF ends up with a timeout.
	Metrics:
	• **ocpm_handle_update_notify_timeout_as_pending_confirmation_total**
	– This will be incremented when:
	* Configuration flag
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED`
	is enabled, and
	* A specific error is added in
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS`
	, and
	* A timeout happens during Update Notify triggered by AAR-I and AAR-U.
	Alarm Condition:
	• If ⩾**70%** of update_notify total requests fail with a timeout, an alarm is raised.
	Diagnostic Information:
	• **Check Network Latency**
	– Investigate possible delays in the network that are resulting in timeouts.
	• **Verify Sender Information**
	– Verify if the
	`notifUri`
	where we are sending the information is correct.
	• **Verify Receiver NF**
	– Verify that the SMF receiving the traffic is in a healthy state.
	• **Review Application**
	– Verify that SM is not congested.
	– Check for constant error logs.
	– Monitor system/resource utilization (CPU, memory, queues).
	Recover:
	• **Check Network Latency and Connectivity**
	– Investigate any current network issues or bottlenecks between the external NF and the SM service.
	– Resolve any high latency or packet loss immediately if detected.
	• **Review SM Service Application and Resources**
	– Restart or scale up resources temporarily if the system is overloaded.
	• **Disable Feature**
	– If this flow is the only one affected, disable this feature as a last resort.
	For any additional guidance, contact My Oracle Support.

5.1.2.94 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD

Table 5-227 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify that failed because a timeout is equal or above 50% but less than 70% in a given time period.
Summary	This alert is triggered when the number of update notify that failed because a timeout is equal or above 50% but less than 70% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_timeout_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.112
Metric Used	ocpm_handle_update_notify_timeout_as_pending_confirmation_total

Table 5-227 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MAJOR_THRESHOLD

Field	Details
Recommended Actions	Cause: Metric **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** is pegged when the operation Update Notify towards SMF ends up with a timeout. • Metrics: **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** – This will be incremented when the configuration flag SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED is enabled and a specific error is added in SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS, and a timeout happens during update notify triggered by AAR-I and AAR-U. • Alarm Condition: – If more than or equal to 50% but less than 70% of update_notify total requests fail with a timeout, an alarm is raised. Diagnostic Information: • Check Network Latency – Investigate possible delays in the network which are resulting in timeouts. • Verify sender information – Verify if the notifUri where we are sending the information is correct. • Verify receiver NF – Verify that the SMF that is receiving the traffic is in a healthy state. • Review application – Verify if SM is not congested. – Look for signs such as constant error logs. – Monitor system/resource utilization (CPU, memory, queues). Recover: • Check Network Latency and Connectivity – Investigate any current network issues or bottlenecks between the external NF and the SM Service. Resolve any high latency or packet loss immediately if detected. • Review SM Service Application and Resources – Restart or scale up resources temporarily if the system is overloaded. • Disable feature – If this flow is the only one affected, you can disable this feature as a last resort. For any additional guidance, contact My Oracle Support.

5.1.2.95 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Table 5-228 RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Field	Details
Description	This alert is triggered when the number of update notify that failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.

Table 5-228 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Field	Details
Summary	This alert is triggered when the number of update notify that failed because a timeout is equal or above 30% but less than 50% of total Rx sessions.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_handle_update_notify_timeout_as_pending_confirmation_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m])) / sum by (namespace) (rate(ocpm_rx_update_notify_request_total{operationType="update_notify",microservice=~".*pcf_sm"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.112
Metric Used	ocpm_handle_update_notify_timeout_as_pending_confirmation_total

Table 5-228 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

Field	Details

Recommended Actions	**Cause:**
	Metric **ocpm_handle_update_notify_timeout_as_pending_confirmation_total** is pegged when the **Update Notify** operation towards SMF ends up with a timeout.
	Metrics:
	• **ocpm_handle_update_notify_timeout_as_pending_confirmation_total**
	– This will be incremented when:
	* Configuration flag
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.ENABLED`
	is enabled, and
	* A specific error is added in
	`SYSTEM.RX.UPDATE_NOTIFY.RULES.PENDING_CONFIRMATION.EXCEPTIONS`
	, and
	* A timeout happens during Update Notify triggered by AAR-I and AAR-U.
	Alarm Condition:
	• If **≥30% and < 50%** of update_notify total requests fail with a timeout, an alarm is raised.
	Diagnostic Information:
	• **Check Network Latency**
	– Investigate possible delays in the network that are resulting in timeouts.
	• **Verify Sender Information**
	– Verify if the
	`notifUri`
	where we are sending the information is correct.
	• **Verify Receiver NF**
	– Verify that the SMF receiving the traffic is in a healthy state.
	• **Review Application**
	– Verify that SM is not congested.
	– Check for constant error logs.
	– Monitor system/resource utilization (CPU, memory, queues).
	Recover:
	• **Check Network Latency and Connectivity**
	– Investigate any current network issues or bottlenecks between the external NF and the SM service.
	– Resolve any high latency or packet loss immediately if detected.
	• **Review SM Service Application and Resources**
	– Restart or scale up resources temporarily if the system is overloaded.
	• **Disable Feature**
	– If this flow is the only one affected, disable this feature as a last resort.

Table 5-228 (Cont.)
RX_PENDING_CONFIRMATION_UPDATE_NOTIFY_TIMEOUT_ABOVE_MINOR_THRESHOLD

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

5.1.2.96 PCF_STATE_NON_FUNCTIONAL_CRITICAL

Table 5-229 PCF_STATE_NON_FUNCTIONAL_CRITICAL

Field	Details
Description	Policy is in non functional state due to DB cluster state down.
Summary	Policy is in non functional state due to DB cluster state down.
Severity	Critical
Expression	appinfo_nfDbFunctionalState_current{nfDbFunctionalState="Not_Running"} == 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.102
Metric Used	appinfo_nfDbFunctionalState_current
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.2.97 UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Table 5-230 UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code!~"2.*",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.108
Metric Used	ocpm_udr_tracking_response_total

Table 5-230 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR is received in UDR connector. This alert is notifying when the number of responses received from UDR for operation resubscribe that failed is above the threshold mentioned. **Cause:** The **ocpm_udr_tracking_response_total** metric is pegged whenever a response is received from the UDR in the UDR Connector. In this case, alerts are triggered when the number of failed responses received from UDR for the **resubscribe** operation exceeds the configured threshold. This alert is triggered when **more than 50% but less than 70%** of GET calls for UDR revalidation (`operation_type=resubscribe`, `service_resource=subscription-revalidation`) sent by the **PCF-UserService** fail (i.e., receive non-2xx HTTP response codes). **Diagnostic Information:** 1. **Check Recent Logs** • Review logs from the **PCF UDR Connector** and **Egress Gateway** for the relevant time intervals. • Review errors at **SCP routing**. • Identify the failure responses—look for non-2xx HTTP status codes and any error payloads. 2. **Analyze Failure Patterns** • Determine if failures are tied to specific UDRs, subscriber groups, or are distributed across all revalidations. • Assess whether there is a spike in failed revalidations or if failures are intermittent. 3. **Inspect UDR Health and Reachability** • Verify the health and responsiveness of the UDR service. • Check network connectivity from the PCF to UDR; look for timeouts, DNS errors, or other connectivity issues in intermediary services (EGW, SCP). 4. **Review PCF–UDR Connector Configuration** • Ensure proper configuration of endpoints, service credentials, and connection settings between PCF and UDR. • Review any recent configuration or deployment changes that might correspond to the start of failures. 5. **Check for Resource or Rate Limiting** • Evaluate whether there are signs of resource exhaustion (CPU, memory, network) on either service. • Investigate if the UDR is rate-limiting incoming requests or experiencing overload. 6. **Correlate with Related Alerts or Incidents** • Cross-check whether other alerts in the same namespace indicate broader issues (e.g., infrastructure, dependency outages, authentication errors). **Recovery:** 1. **Restore UDR Service Health** • Address any service outages, restarts, or degraded performance on the UDR side.

Table 5-230 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
	• If resource constraints are detected, consider scaling UDR or optimizing load. 2. **Fix Connectivity or Configuration Issues** • Resolve network issues (latency, DNS, firewall). • Correct any erroneous endpoint URLs or authentication parameters in PCF User or UDR Connector configurations. For any additional guidance, contact My Oracle Support.

5.1.2.98 UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Table 5-231 UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code!~"2.*",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.108
Metric Used	ocpm_udr_tracking_response_total

Table 5-231 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR is received in UDR connector. This alert is notifying when the number of responses received from UDR for operation resubscribe that failed is above the threshold mentioned. **Cause:** The **ocpm_udr_tracking_response_total** metric is pegged whenever a response is received from the UDR in the UDR Connector. In this case, alerts are triggered when the number of failed responses received from UDR for the **resubscribe** operation exceeds the configured threshold. This alert is triggered when **more than 70%** of GET calls for UDR revalidation (`operation_type=resubscribe`, `service_resource=subscription-revalidation`) sent by the **PCF-UserService** fail (i.e., receive non-2xx HTTP response codes). **Diagnostic Information:** 1. **Check Recent Logs** • Review logs from **PCF UDR Connector** and **Egress Gateway** for the relevant time intervals. • Review errors at **SCP routing**. • Identify the failure responses — look for non-2xx HTTP status codes and any error payloads. 2. **Analyze Failure Patterns** • Determine if failures are tied to specific UDRs, subscriber groups, or are distributed across all revalidations. • Assess whether there is a spike in failed revalidations or if failures are intermittent. 3. **Inspect UDR Health and Reachability** • Verify the health and responsiveness of the UDR service. • Check network connectivity from the PCF to UDR; look for timeouts, DNS errors, or other connectivity issues in intermediary services (EGW, SCP). 4. **Review PCF–UDR Connector Configuration** • Ensure proper configuration of endpoints, service credentials, and connection settings between PCF and UDR. • Review any recent configuration or deployment changes that might correspond to the start of failures. 5. **Check for Resource or Rate Limiting** • Evaluate whether there are signs of resource exhaustion (CPU, memory, network) on either service. • Investigate if the UDR is rate-limiting incoming requests or experiencing overload. 6. **Correlate with Related Alerts or Incidents** • Cross-check whether other alerts in the same namespace indicate broader issues (e.g., infrastructure, dependency outages, authentication errors). **Recovery:** 1. **Restore UDR Service Health** • Address any service outages, restarts, or degraded performance on the UDR side. • If resource constraints are detected, consider scaling UDR or optimizing load.

Table 5-231 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
	2. **Fix Connectivity or Configuration Issues** • Resolve network issues (latency, DNS, firewall). • Correct any erroneous endpoint URLs or authentication parameters in PCF User or UDR Connector configurations. For any additional guidance, contact My Oracle Support.

5.1.2.99 UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Table 5-232 UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Severity	Minor
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code!~"2.*",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.108
Metric Used	ocpm_udr_tracking_response_total

Table 5-232 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Field	Details

Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR is received in UDR connector. This alert is notifying when the number of responses received from UDR for operation resubscribe that failed is above the threshold mentioned.
	Cause:
	The **ocpm_udr_tracking_response_total** metric is pegged whenever we receive a response from the UDR in the UDR Connector.
	In this case, alerts are triggered when the number of failed responses received from UDR for the **resubscribe** operation is above the configured threshold.
	This alert is triggered when **more than 30% but less than 50%** of GET calls for UDR revalidation
	(
	`operation_type=resubscribe`
	,
	`service_resource=subscription-revalidation`
	) sent by the **PCF-UserService** fail (i.e., receive non-2xx HTTP response codes).
	Diagnostic Information:
	1. **Check Recent Logs**
	• Review logs from the **PCF UDR Connector** and **Egress Gateway** for the relevant time intervals.
	• Review errors at **SCP routing**.
	• Identify the failure responses — look for non-2xx HTTP status codes and any error payloads.
	2. **Analyze Failure Patterns**
	• Determine if failures are tied to specific UDRs, subscriber groups, or are distributed across all revalidations.
	• Assess if there is a spike in failed revalidations or if failures are intermittent.
	3. **Inspect UDR Health and Reachability**
	• Verify the health and responsiveness of the UDR service.
	• Check network connectivity from the PCF to UDR; look for timeouts, DNS errors, or other connectivity issues in intermediary services (EGW, SCP).
	4. **Review PCF–UDR Connector Configuration**
	• Ensure proper configuration of endpoints, service credentials, and connection settings between PCF and UDR.
	• Review any recent configuration or deployment changes that might correspond to the start of failures.
	5. **Check for Resource or Rate Limiting**
	• Evaluate if there are signs of resource exhaustion (CPU, memory, network) on either service.
	• Investigate if the UDR is rate-limiting incoming requests or experiencing overload.
	6. **Correlate with Related Alerts or Incidents**

Table 5-232 (Cont.) UDR_GET_REVALIDATION_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
	• Cross-check if other alerts in the same namespace indicate broader issues (e.g., infrastructure, dependency outages, authentication errors). **Recovery:** 1. **Restore UDR Service Health** • Address any service outages, restarts, or degraded performance on the UDR side. • If resource constraints are detected, consider scaling UDR or optimizing load. 2. **Fix Connectivity or Configuration Issues** • Resolve network issues (latency, DNS, firewall). • Correct any erroneous endpoint URLs or authentication parameters in PCF User or UDR Connector configurations. For any additional guidance, contact My Oracle Support.

5.1.2.100 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT

Table 5-233 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed with status code 404 NOT FOUND.
Summary	This alert is triggered when more than 70% of the UDR revalidation using method GET call failed with status code 404 NOT FOUND.
Severity	Critical
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code="404",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.52.1.2.110
Metric Used	ocpm_udr_tracking_response_total

Table 5-233 (Cont.) UDR_GET_REVALIDATION_404_FAILURE_ABOVE_CRITICAL_PERCENT

Field	Details
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR in UDR connector is received. This alert notifies when the number of responses received from UDR for operation resubscribe that failed with a 404 Not Found is above the threshold mentioned. Cause: This alert is triggered when more than 70% of UDR revalidation GET operations managed by PCF fail with an HTTP 404 (Not Found) response code within the specified window. A 404 response indicates that the requested subscription for revalidation was not found in UDR. Diagnostic Information: 1. Check UDR logs: Look for 404 errors and the accompanying trigger request details (trigger of UDR revalidation request) for the affected time period. 2. Verify subscription states: Ensure that the subscriptions expected to be present actually exist and are not being deleted, expired, or unavailable. 3. Investigate Missing Subscriptions: • Determine why the revalidation call is being made for a non-existent subscription ID. If the subscription has gone stale, verify why an audit was not triggered for it. • Check if there is a data synchronization issue between the originator and UDR. 4. Look for patterns: Determine whether the 404s are concentrated in a particular user group. Recovery: 1. Audit Subscription Lifecycle: Ensure proper creation, update, and deletion workflows so stale subscription IDs are not reused or referenced. 2. Review Recent Deployments or Changes: Check whether recent code or configuration changes in **pcf_user** or UDR might have led to increased 404s. For any additional guidance, contact My Oracle Support.

5.1.2.101 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT

Table 5-234 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 50% but less that 70% of the UDR revalidation using method GET call failed.
Severity	Major
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code="404",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 50 < 70

Table 5-234 (Cont.) UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MAJOR_PERCENT

Field	Details
OID	1.3.6.1.4.1.323.5.3.52.1.2.110
Metric Used	ocpm_udr_tracking_response_total
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR in UDR connector is received. This alert notifies when the number of responses received from UDR for operation resubscribe that failed with a 404 Not Found is above the threshold mentioned. Cause: This alert is triggered when more than 50% (but less than 70%) of UDR revalidation GET operations managed by PCF fail with an HTTP 404 (Not Found) response code within the specified window. A 404 response indicates that the requested subscription for revalidation was not found in UDR. Diagnostic Information: 1. Check UDR logs: Look for 404 errors and the accompanying trigger request details (trigger of UDR revalidation request) for the affected time period. 2. Verify subscription states: Ensure that the subscriptions expected to be present actually exist and are not being deleted, expired, or unavailable. 3. Investigate missing subscriptions: • Determine why the revalidation call is being made for a non-existent subscription ID. If the subscription has gone stale, verify why an audit was not triggered for the same. • Check if there is a data synchronization issue between the originator and UDR. 4. Look for patterns: Determine whether the 404s are concentrated in a particular user group. Recovery: 1. Audit subscription lifecycle: Ensure proper creation, update, and deletion workflows so stale subscription IDs are not reused or referenced. 2. Review recent deployments or changes: Check whether recent code or configuration changes in pcf_user or UDR might have led to increased 404s. For any additional guidance, contact My Oracle Support.

5.1.2.102 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT

Table 5-235 UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
Description	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Summary	This alert is triggered when more than or equal to 30% but less that 50% of the UDR revalidation using method GET call failed.
Severity	Minor

Table 5-235 (Cont.) UDR_GET_REVALIDATION_404_FAILURE_ABOVE_MINOR_PERCENT

Field	Details
Expression	(sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",response_code="404",service_resource="subscription-revalidation"}[5m])) / sum by (namespace) (rate(ocpm_udr_tracking_response_total{operation_type="resubscribe",microservice=~".*pcf_user",service_resource="subscription-revalidation"}[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.52.1.2.110
Metric Used	ocpm_udr_tracking_response_total
Recommended Actions	The `ocpm_udr_tracking_response_total` metric is pegged whenever a response from UDR in UDR connector is received. This alert notifies when the number of responses received from UDR for operation resubscribe that failed with a 404 Not Found is above the threshold mentioned. Cause: This alert is triggered when more than 30% (but less than 50%) of UDR revalidation GET operations managed by PCF fail with an HTTP 404 (Not Found) response code within the specified window. A 404 response indicates that the requested subscription for revalidation was not found in UDR. Diagnostic Information: 1. Check UDR logs: Look for 404 errors and the accompanying trigger request details (trigger of UDR revalidation request) for the affected time period. 2. Verify subscription states: Ensure that the subscriptions expected to be present actually exist and are not being deleted, expired, or unavailable. 3. Investigate missing subscriptions: • Determine why the revalidation call is being made for a non-existent subscription ID. If the subscription has gone stale, verify why an audit was not triggered for the same. • Check if there is a data synchronization issue between the originator and UDR. 4. Look for patterns: Determine whether the 404s are concentrated in a particular user group. Recovery: 1. Audit subscription lifecycle: Ensure proper creation, update, and deletion workflows so stale subscription IDs are not reused or referenced. 2. Review recent deployments or changes: Check whether recent code or configuration changes in **pcf_user** or UDR might have led to increased 404s. For any additional guidance, contact My Oracle Support.

5.1.2.103 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Table 5-236 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting

Table 5-236 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",imm_reports_present="false"}[5m])) / sum(rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.116
Metric Used	occnp_immrep_response_total

Table 5-236 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing AM user data check is based on: * `service_subresource = "am-data"` (indicates the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `imm_reports_present = "false"` (indicates no AM user data was returned from UDR as part of the Immediate Reporting capability) – If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response without AM user data as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (e.g., `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.104 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Table 5-237 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.116
Metric Used	occnp_immrep_response_total

Table 5-237 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing AM user data check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no AM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response **without** user data for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and still no AM user data is retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.105 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Table 5-238 UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting.
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for AM as part of immediate reporting.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.116
Metric Used	occnp_immrep_response_total

Table 5-238 (Cont.) UDR_AM_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The missing AM user data check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no AM user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response **without** user data for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in the request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.106 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Table 5-239 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.117
Metric Used	occnp_immrep_response_total

Table 5-239 (Cont.) UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR in the POST REST API request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.107 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Table 5-240 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.117
Metric Used	occnp_immrep_response_total

Table 5-240 (Cont.) UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Recommended Actions	Cause: The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. – The failed feature negotiation check is based on: * `service_subresource = "am-data"` (to indicate the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in the request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved, inform the UDR operators whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.108 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Table 5-241 UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for AM as part of immediate reporting
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="am-data",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.117
Metric Used	occnp_immrep_response_total

Table 5-241 (Cont.) UDR_AM_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "am-data"` (indicates the UDR POST was to get AM user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `immediate_report_pcc = "false"` (indicates that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response with **failed feature negotiation** for AM as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and AM user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.109 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR

Table 5-242 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.118
Metric Used	occnp_immrep_response_total

Table 5-242 (Cont.) UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MINOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The missing UE user data check is based on: * `service_subresource = "ue-policy-set"` (indicates the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (indicates this is a POST call) * `imm_reports_present = "false"` (indicates no UE user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **10% but less than 20%** of the traffic: UDR returned a POST Subscribe response **without UE user data** as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and UE user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.110 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Table 5-243 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.118
Metric Used	occnp_immrep_response_total

Table 5-243 (Cont.) UDR_UE_IMMREP_RESPONSE_MISSING_DATA_MAJOR

Field	Details
Recommended Actions	**Cause:** The metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a **POST Subscription with Immediate Reporting**. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The missing UE user data check is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no UE user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, the alarm will trigger. **Alarm Condition:** • More than or equal to **20% but less than 30%** of the traffic: UDR returned a POST Subscribe response **without UE user data** as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the **30th byte set to 1** when converted to hex (for example, `40000000`). • This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to **true** in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the **ImmReportPcc** feature enabled. 4. **Last Resort – Inform UDR Operator** • If the above points are validated and UE user data is still not retrieved: – Inform the UDR operators. – Ask them to verify whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the **30th byte allotted for ImmReportPcc**. 2. Verify `immRep` is being sent as **true**. 3. Verify the UDR profile chosen to perform the UDR POST has **ImmReportPcc enabled** after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.111 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Table 5-244 UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but without user data for UE as part of immediate reporting
Severity	CRITICAL
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",imm_reports_present="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.118
Metric Used	occnp_immrep_response_total

Table 5-244 (Cont.) UDR_UE_IMMREP_RESPONSE_MISSING_DATA_CRITICAL

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for a POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The missing UE user data check is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `imm_reports_present = "false"` (to indicate no UE user data was returned from UDR as part of the Immediate Reporting capability) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response without UE user data as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.112 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Table 5-245 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Description	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Summary	More than or equal to 10% but less that 20% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 10 < 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.119
Metric Used	occnp_immrep_response_total

Table 5-245 (Cont.) UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MINOR

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **10%** but less than **20%** of the traffic: UDR returned a POST Subscribe response with failed feature negotiation for UE as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.113 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Table 5-246 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Description	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Summary	More than or equal to 20% but less that 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Severity	Major
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 20 < 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.119
Metric Used	occnp_immrep_response_total

Table 5-246 (Cont.) UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_MAJOR

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **20%** but less than **30%** of the traffic: UDR returned a POST Subscribe response with failed feature negotiation for UE as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the UDR POST request payload. 3. **Verify UDR Profile** • Ensure User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.114 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Table 5-247 UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Description	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Summary	More than or equal to 30% of the traffic, UDR returned with POST subscribe response but with failed feature negotiation for UE as part of immediate reporting
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post",immediate_report_pcc="false"}[5m]))) / (sum by (namespace) (rate(occnp_immrep_response_total{service_subresource="ue-policy-set",operation_type="post"}[5m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.119
Metric Used	occnp_immrep_response_total

Table 5-247 (Cont.) UDR_UE_IMMREP_FEATURE_NEGOTIATION_FAILED_CRITICAL

Field	Details
Recommended Actions	**Cause:** Metric **occnp_immrep_response_total** is pegged when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. **Metric:** • **occnp_immrep_response_total** – Increments when UDR-C receives a user data response from UDR for POST Subscription with Immediate Reporting. – The failed feature negotiation is based on: * `service_subresource = "ue-policy-set"` (to indicate the UDR POST was to get UE user data from UDR) * `operation_type = "POST"` (to determine this is a POST call) * `immediate_report_pcc = "false"` (to indicate that no feature negotiation happened with UDR on the ImmReportPcc feature) • If these metric dimensions are satisfied, then the alarm will trigger. **Alarm Condition:** • More than or equal to **30%** of the traffic: UDR returned a POST Subscribe response with failed feature negotiation for UE as part of Immediate Reporting. **Diagnostic Information:** 1. **Verify ImmReportPcc** • Ensure the `suppFeat` attribute sent towards UDR for the POST REST API call in its request payload has the 30th byte allocated as 1 when converted to hex (for example, `"40000000"`). This is crucial for feature negotiation with UDR. 2. **Verify immRep** • Ensure the `immRep` attribute is set to `true` in the request payload for the UDR POST. 3. **Verify UDR Profile** • Ensure that User Data is requested only for those UDR profiles that PCF obtained from NRF with the ImmReportPcc feature enabled. 4. **Last Resort – Intimate UDR Operator** • If the above points are validated and still no UE user data is retrieved, then intimate the same to UDR operators to check whether the Immediate Reporting feature is working and negotiated from their end. **Recovery:** 1. Verify the `suppFeat` attribute is sent with the 30th byte allotted for ImmReportPcc. 2. Verify `immRep` is being sent as `true`. 3. Verify the UDR profile being chosen to perform the UDR POST has ImmReportPcc enabled after on-demand/autonomous UDR discovery. For any additional guidance, contact My Oracle Support.

5.1.2.115 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST_EGW

Table 5-248 POD_PROTECTION_BY_RATELIMIT_REJECTED_REQUEST_EGW

Field	Details
Description	Egress Gateway traffic is getting rejected more than 1% because of ratelimiting.
Summary	Egress Gateway traffic is getting rejected more than 1% because of ratelimiting.
Severity	Major
Expression	(sum(rate(oc_egressgateway_http_request_ratelimit_values_total {allowed="false",app_kubernetes_io_name="egress-gateway",,namespace="$NAMESPACE"}[2m]) or (up * 0)))/ sum(rate(oc_egressgateway_http_request_ratelimit_values_total {app_kubernetes_io_name="egress-gateway",,namespace="$NAMESPACE"}[2m])) * 100 >= 1
OID	1.3.6.1.4.1.323.5.3.52.1.2.114
Metric Used	oc_egressgateway_http_request_ratelimit_values_total
Recommended Actions	The alert is cleared when the failure rate goes below 1% of total tps. For any additional guidance, contact My Oracle Support.

5.1.2.116 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERCENT

Table 5-249 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 60% in a given time period.
Severity	Critical
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="403"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.120
Metric Used	occnp_pa_sponsored_sessions_total

Table 5-249 (Cont.) SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). **Cause:** Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **403 Requested Service Not Authorized** response. This occurs when the client sends a Sponsored request with `umcDataIncluded="false"` but the requested service is not authorized. As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. **Diagnostic Information:** • **Metric involved:**`occnp_pa_sponsored_sessions_total` • **Error observed:** 403 Requested Service Not Authorized • **Condition:** Unauthorized Sponsored Connectivity requests **Verification steps:** 1. Send a Sponsored Connectivity request with valid authorization and supported features. 2. Confirm the request succeeds. 3. Verify that the 403 / Requested Service Not Authorized ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Track the 4xx error ratio by caller/tenant and by sponsor/ASP. • Pay special attention to spikes after client deployments or policy/configuration changes. **Recovery:** 1. Identify the failing caller. 2. Review the request payload, entitlement, and policy configuration. 3. Confirm that the sponsor/ASP is authorized for the requested service. 4. Correct any misconfigurations in policy rules or subscription data. 5. Ensure that Sponsored Connectivity is supported in both the PCF SM Service and the PA Service. 6. Escalate if the issue persists after authorization or policy fixes, or if it impacts multiple tenants or partners.

5.1.2.117 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCENT

Table 5-250 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.

Table 5-250 (Cont.)
SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 40% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="403"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 40 < 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.120
Metric Used	occnp_pa_sponsored_sessions_total
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). **Cause:** Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **403 Requested Service Not Authorized** response. This occurs when the client sends a Sponsored request with `umcDataIncluded="false"` but the requested service is not authorized. As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. **Diagnostic Information:** • **Metric involved:**`occnp_pa_sponsored_sessions_total` • **Error observed:** 403 Requested Service Not Authorized • **Condition:** Unauthorized Sponsored Connectivity requests **Verification steps:** 1. Send a Sponsored Connectivity request with valid authorization and supported features. 2. Confirm the request succeeds. 3. Verify that the 403 / Requested Service Not Authorized ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Track the 4xx error ratio by caller/tenant and by sponsor/ASP. • Pay special attention to spikes after client deployments or policy/configuration changes. **Recovery:** 1. Identify the failing caller. 2. Review the request payload, entitlement, and policy configuration. 3. Confirm that the sponsor/ASP is authorized for the requested service. 4. Correct any misconfigurations in policy rules or subscription data. 5. Ensure that Sponsored Connectivity is supported in both the PCF SM Service and the PA Service. 6. Escalate if the issue persists after authorization or policy fixes, or if it impacts multiple tenants or partners.

5.1.2.118 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCENT

Table 5-251 SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 20% in a given time period.
Severity	Minor
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="403"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 20 < 40
OID	1.3.6.1.4.1.323.5.3.52.1.2.120
Metric Used	occnp_pa_sponsored_sessions_total

Table 5-251 (Cont.)
SMF_REQUESTED_SERVICE_NOT_AUTHORIZED_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **403 Requested Service Not Authorized** response. This occurs when the client sends a Sponsored request with `umcDataIncluded="false"`, but the requested service is not authorized. As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 403 Requested Service Not Authorized • **Condition:** Unauthorized Sponsored Connectivity requests **Verification steps:** 1. Send a Sponsored Connectivity request with valid authorization and supported features. 2. Confirm the request succeeds. 3. Verify that the 403 / Requested Service Not Authorized ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Track the 4xx error ratio by caller/tenant and by sponsor/ASP. • Pay special attention to spikes after client deployments or policy/configuration changes. Recovery: 1. Identify the failing caller. 2. Review the request payload, entitlement, and policy configuration. 3. Confirm that the sponsor/ASP is authorized for the requested service. 4. Correct any misconfigurations in policy rules or subscription data. 5. Ensure that Sponsored Connectivity is supported in both the PCF SM Service and the PA Service. 6. Escalate if the issue persists after authorization or policy fixes, or if it impacts multiple tenants or partners.

5.1.2.119 AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT

Table 5-252 AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 60% in a given time period.
Severity	Critical

Table 5-252 (Cont.) AF_MANDATORY_IE_MISSING_SC_ABOVE_CRITICAL_THRESHOLD_PERCENT

Field	Details
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="400",cause="MANDATORY_IE_MISSING"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.122
Metric Used	occnp_pa_sponsored_sessions_total
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **400 Bad Request** due to `cause="MANDATORY_IE_MISSING"`. This happens when the client sends a Sponsored Connectivity request missing one or more mandatory Information Elements (IEs). As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 400 Bad Request • **Cause value:** MANDATORY_IE_MISSING • **Condition:** Sponsored Connectivity requests missing mandatory IE fields • **Common missing IEs:** sponId, aspId, afAppId **Verification steps:** 1. Send a valid Sponsored Connectivity request including all mandatory IEs. 2. Ensure sponId and aspId are present and that Sponsored Connectivity is negotiated. 3. Confirm the request succeeds. 4. Verify that the 400 / MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Monitor the 4xx error ratio by caller/tenant and by sponsor/ASP. • Watch for spikes following client deployments or gateway transformation changes. Recovery: 1. Identify the failing caller. 2. Compare the request payload against the API contract. 3. Restore all mandatory IE fields (sponId, aspId, afAppId, etc.). 4. Review and fix any gateway or payload transformation issues. 5. Redeploy the corrected configuration or client. 6. Escalate if the issue persists after fixes or impacts multiple tenants.

5.1.2.120 AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT

Table 5-253 AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 40% in a given time period.
Severity	Major
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="400",cause="MANDATORY_IE_MISSING"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 40 < 60
OID	1.3.6.1.4.1.323.5.3.52.1.2.122
Metric Used	occnp_pa_sponsored_sessions_total

Table 5-253 (Cont.) AF_MANDATORY_IE_MISSING_SC_ABOVE_MAJOR_THRESHOLD_PERCENT

Field	Details
Recommended Actions	If this alert gets triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **400 Bad Request** due to `cause="MANDATORY_IE_MISSING"`. This happens when the client sends a Sponsored Connectivity request missing one or more mandatory Information Elements (IEs). As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 400 Bad Request • **Cause value:** MANDATORY_IE_MISSING • **Condition:** Sponsored Connectivity requests missing mandatory IE fields • **Common missing IEs:** sponId, aspId, afAppId **Verification steps:** 1. Send a valid Sponsored Connectivity request including all mandatory IEs. 2. Ensure sponId and aspId are present and that Sponsored Connectivity is negotiated. 3. Confirm the request succeeds. 4. Verify that the 400 / MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Monitor the 4xx error ratio by caller/tenant and by sponsor/ASP. • Watch for spikes following client deployments or gateway transformation changes. Recovery: 1. Identify the failing caller. 2. Compare the request payload against the API contract. 3. Restore all mandatory IE fields (sponId, aspId, afAppId, etc.). 4. Review and fix any gateway or payload transformation issues. 5. Redeploy the corrected configuration or client. 6. Escalate if the issue persists after fixes or impacts multiple tenants.

5.1.2.121 AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT

Table 5-254 AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Description	{{ $value }} % of patch requests failed in {{$labels.namespace}}.
Summary	This alert is triggered when the number of PATCH request that failed is equal to or above 20% in a given time period.
Severity	Minor

Table 5-254 (Cont.) AF_MANDATORY_IE_MISSING_SC_ABOVE_MINOR_THRESHOLD_PERCENT

Field	Details
Expression	(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total{responseCode="400",cause="MANDATORY_IE_MISSING"}[5m])))/(sum by (namespace) (rate(occnp_pa_sponsored_sessions_total[5m]))) * 100 >= 20 < 40
OID	1.3.6.1.4.1.323.5.3.52.1.2.122
Metric Used	occnp_pa_sponsored_sessions_total
Recommended Actions	If this alert is triggered, Prometheus metrics or other tools can be used to check what error codes are being thrown and identify if the error comes from the NF being reached (in this case SM). Cause: Alerts are triggered when Sponsored Connectivity requests processed by PA-Service fail with a **400 Bad Request** due to `cause="MANDATORY_IE_MISSING"`. This happens when the client sends a Sponsored Connectivity request missing one or more mandatory Information Elements (IEs). As a result, PA rejects the request and increments the **occnp_pa_sponsored_sessions_total** metric. Diagnostic Information: • **Metric involved:** occnp_pa_sponsored_sessions_total • **Error observed:** 400 Bad Request • **Cause value:** MANDATORY_IE_MISSING • **Condition:** Sponsored Connectivity requests missing mandatory IE fields • **Common missing IEs:** sponId, aspId, afAppId **Verification steps:** 1. Send a valid Sponsored Connectivity request including all mandatory IEs. 2. Ensure sponId and aspId are present and that Sponsored Connectivity is negotiated. 3. Confirm the request succeeds. 4. Verify that the 400 / MANDATORY_IE_MISSING ratio drops below the alert threshold within one evaluation window. **Monitoring recommendations:** • Monitor the 4xx error ratio by caller/tenant and by sponsor/ASP. • Watch for spikes following client deployments or gateway transformation changes. Recovery: 1. Identify the failing caller. 2. Compare the request payload against the API contract. 3. Restore all mandatory IE fields (sponId, aspId, afAppId, etc.). 4. Review and fix any gateway or payload transformation issues. 5. Redeploy the corrected configuration or client. 6. Escalate if the issue persists after fixes or impacts multiple tenants.

5.1.3 PCRF Alerts

This section provides information about PCRF alerts.

5.1.3.1 PRE_UNREACHABLE_EXCEEDS_CRITICAL_THRESHOLD

Table 5-255 PRE_UNREACHABLE_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	PRE fail count exceeds the critical threshold limit.
Summary	Alert PRE unreachable NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	Critical
Expression	PRE fail count exceeds the critical threshold limit.
OID	1.3.6.1.4.1.323.5.3.44.1.2.9
Metric Used	http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.2 PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD

Table 5-256 PRE_UNREACHABLE_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	PRE fail count exceeds the major threshold limit.
Summary	Alert PRE unreachable NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	Major
Expression	PRE fail count exceeds the major threshold limit.
OID	1.3.6.1.4.1.323.5.3.44.1.2.9
Metric Used	http_out_conn_response_total{container="pcrf-core", responseCode!~"2.*", serviceResource="PRE"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.3 PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD

Table 5-257 PRE_UNREACHABLE_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	PRE fail count exceeds the minor threshold limit.
Summary	Alert PRE unreachable NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	minor
Expression	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.

5.1.3.4 PCRF_DOWN

Table 5-258 PCRF_DOWN

Field	Details
Description	PCRF Service is down
Summary	Alert PCRF_DOWN NS:{{ $labels.kubernetes_namespace }}, PODNAME: {{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL: {{ $labels.release }}
Severity	Critical
Expression	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.

5.1.3.5 CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-259 CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	CCA fail count exceeds the critical threshold limit
Summary	Alert CCA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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.

5.1.3.6 CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-260 CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	CCA fail count exceeds the major threshold limit
Summary	Alert CCA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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.

5.1.3.7 CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-261 CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	CCA fail count exceeds the minor threshold limit
Summary	Alert CCA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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.

5.1.3.8 AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-262 AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	AAA fail count exceeds the critical threshold limit
Summary	Alert AAA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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	occnp_diam_response_local_total{msgType=~"AAA.*", responseCode!~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.9 AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-263 AAA Fail Count Exceeds Major Threshold

Field	Details
Description	AAA fail count exceeds the major threshold limit
Summary	Alert AAA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	The failure rate of AAA messages has exceeded the major 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.

5.1.3.10 AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-264 AAA Fail Count Exceeds Minor Threshold

Field	Details
Description	AAA fail count exceeds the minor threshold limit
Summary	Alert AAA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	The failure rate of AAA messages has exceeded the 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.

5.1.3.11 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-265 RAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the critical threshold limit
Summary	Alert RAA_Rx_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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.

5.1.3.12 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-266 RAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the major threshold limit
Summary	Alert RAA_Rx_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode!~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.13 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-267 RAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Rx fail count exceeds the minor threshold limit
Summary	Alert RAA_Rx_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode! ~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.14 RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-268 RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Gx fail count exceeds the critical threshold limit
Summary	Alert RAA_GX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode! ~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.15 RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-269 RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Gx fail count exceeds the major threshold limit
Summary	Alert RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode! ~"2.*"}

Table 5-269 (Cont.) RAA_GX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

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

5.1.3.16 RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-270 RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Gx fail count exceeds the minor threshold limit
Summary	Alert RAA_GX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode!~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.17 ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-271 ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA fail count exceeds the critical threshold limit
Summary	Alert ASA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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	occnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.18 ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-272 ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA fail count exceeds the major threshold limit

Table 5-272 (Cont.) ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Summary	Alert ASA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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	occnp_diam_response_local_total{msgType=~"ASA.*", responseCode!~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.19 ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-273 ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA fail count exceeds the minor threshold limit
Summary	Alert ASA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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.

5.1.3.20 STA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-274 STA_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	STA fail count exceeds the critical threshold limit.
Summary	sum(rate(occnp_diam_response_local_total{msgType="STA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA"}[5m])) * 100 > 90
Severity	Critical
Expression	The failure rate of STA messages has exceeded the configured critical threshold limit.
OID	1.3.6.1.4.1.323.5.3.44.1.2.19
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.21 STA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-275 STA_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	STA fail count exceeds the major threshold limit.
Summary	sum(rate(occnp_diam_response_local_total{msgType="STA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA"}[5m])) * 100 > 80
Severity	Major
Expression	The failure rate of STA messages has exceeded the configured major threshold limit.
OID	1.3.6.1.4.1.323.5.3.44.1.2.19
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.22 STA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-276 STA_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	STA fail count exceeds the minor threshold limit.
Summary	sum(rate(occnp_diam_response_local_total{msgType="STA", responseCode!~"2.*"}[5m])) / sum(rate(occnp_diam_response_local_total{msgType="STA"}[5m])) * 100 > 60
Severity	Minor
Expression	The failure rate of STA messages has exceeded the configured minor threshold limit.
OID	1.3.6.1.4.1.323.5.3.44.1.2.19
Metric Used	occnp_diam_response_local_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.23 ASATimeoutlCountExceedsThreshold

Table 5-277 ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	ASA timeout count exceeds the critical threshold limit
Summary	Alert ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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.

5.1.3.24 ASA_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-278 ASA_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	ASA timeout count exceeds the major threshold limit
Summary	Alert ASA_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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.

5.1.3.25 ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-279 ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	ASA timeout count exceeds the minor threshold limit
Summary	Alert ASA_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
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.

5.1.3.26 RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-280 RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Field	Details
Description	RAA Gx timeout count exceeds the critical threshold limit
Summary	Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
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.

5.1.3.27 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-281 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Gx timeout count exceeds the major threshold limit
Summary	Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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.

5.1.3.28 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-282 RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Gx timeout count exceeds the minor threshold limit
Summary	Alert RAA_GX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Gx", responseCode! ~"timeout"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.29 RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD

Table 5-283 RAA Rx Timeout Count Exceeds Critical Threshold

Field	Details
Description	RAA Rx timeout count exceeds the critical threshold limit
Summary	Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_CRITICAL_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Expression	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"}

Table 5-283 (Cont.) RAA Rx Timeout Count Exceeds Critical Threshold

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

5.1.3.30 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Table 5-284 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
Description	RAA Rx timeout count exceeds the major threshold limit
Summary	Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_MAJOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode! ~"timeout"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.31 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Table 5-285 RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
Description	RAA Rx timeout count exceeds the minor threshold limit
Summary	Alert RAA_RX_TIMEOUT_COUNT_EXCEEDS_MINOR_THRESHOLD NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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	occnp_diam_response_local_total{msgType="RAA", appType="Rx", responseCode! ~"timeout"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.32 RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Table 5-286 RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	CCA, AAA, RAA, ASA and STA error rate combined is above 10 percent

Table 5-286 (Cont.) RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Summary	Alert RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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	occnp_diam_response_local_total{ responseCode!~"2.*"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.33 RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Table 5-287 RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Description	CCA, AAA, RAA, ASA and STA error rate combined is above 5 percent
Summary	Alert RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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.

5.1.3.34 RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Table 5-288 RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Description	CCA, AAA, RAA, ASA and STA error rate combined is above 1 percent
Summary	Alert RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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.

5.1.3.35 Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Table 5-289 Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	Rx error rate combined is above 10 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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.

5.1.3.36 Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Table 5-290 Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Description	Rx error rate combined is above 5 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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.

5.1.3.37 Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Table 5-291 Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Description	Rx error rate combined is above 1 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Rx"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.38 Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Table 5-292 Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT

Field	Details
Description	Gx error rate combined is above 10 percent
Summary	Alert Gx_RESPONSE_ERROR_RATE_ABOVE_CRITICAL_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Critical
Expression	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	occnp_diam_response_local_total{ responseCode!~"2.*", appType="Gx"}
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.39 Gx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Table 5-293 Gx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT

Field	Details
Description	Gx error rate combined is above 5 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MAJOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Major
Expression	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.

5.1.3.40 Gx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Table 5-294 Gx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT

Field	Details
Description	Gx error rate combined is above 1 percent
Summary	Alert Rx_RESPONSE_ERROR_RATE_ABOVE_MINOR_PERCENT NS: {{ $labels.kubernetes_namespace }}, PODNAME:{{ $labels.kubernetes_pod_name }}, INST:{{ $labels.instance }} REL:{{ $labels.release }}
Severity	Minor
Expression	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.

5.1.3.41 STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL

Table 5-295 STALE_DIAMETER_REQUEST_CLEANUP_CRITICAL

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 30%
Summary	The Diameter requests are being discarded due to timeout processing occurring above 30%
Severity	Critical
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total[24h])) / sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER"}[24h]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.52.1.2.82
Metric Used	occnp_stale_diam_request_cleanup_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.42 STALE_DIAMETER_REQUEST_CLEANUP_MAJOR

Table 5-296 STALE_DIAMETER_REQUEST_CLEANUP_MAJOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 20%
Summary	The Diameter requests are being discarded due to timeout processing occurring above 20%
Severity	Major
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total[24h])) / sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER"}[24h]))) * 100 >= 20
OID	1.3.6.1.4.1.323.5.3.52.1.2.82
Metric Used	occnp_stale_diam_request_cleanup_total
Recommended Actions	For any additional guidance, contact My Oracle Support.

5.1.3.43 STALE_DIAMETER_REQUEST_CLEANUP_MINOR

Table 5-297 STALE_DIAMETER_REQUEST_CLEANUP_MINOR

Field	Details
Description	The Diameter requests are being discarded due to timeout processing occurring above 10%
Summary	The Diameter requests are being discarded due to timeout processing occurring above 10%
Severity	Minor

Table 5-297 (Cont.) STALE_DIAMETER_REQUEST_CLEANUP_MINOR

Field	Details
Expression	(sum by (namespace, microservice, pod) (increase(occnp_stale_diam_request_cleanup_total[24h])) / sum by (namespace, microservice, pod) (increase(occnp_diam_request_local_total{msgType!~"DWR|CER"}[24h]))) * 100 >= 10
OID	1.3.6.1.4.1.323.5.3.52.1.2.82
Metric Used	occnp_stale_diam_request_cleanup_total
Recommended Actions	For any additional guidance, contact My Oracle Support.