

# Oracle® Communications

## Cloud Native Core, Binding Support Function

### Troubleshooting Guide



Release 24.3.0  
G14591-01  
November 2024

ORACLE®

Copyright © 2021, 2024, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

# Contents

|       |                                              |    |
|-------|----------------------------------------------|----|
| 1     | Introduction                                 |    |
| 1.1   | Overview                                     | 1  |
| 1.2   | Audience                                     | 1  |
| 2     | Logs                                         |    |
| 2.1   | Log Levels                                   | 1  |
| 2.2   | Understanding Logs                           | 2  |
| 3     | Using Debug Tool                             |    |
| 3.1   | Configurable Parameters for Debug Tool       | 14 |
| 4     | Troubleshooting BSF                          |    |
| 4.1   | Deployment Issues                            | 1  |
| 4.1.1 | Helm Install Failure                         | 1  |
| 4.1.2 | Loss of Session Binding data                 | 2  |
| 4.2   | Startup Probes                               | 3  |
| 4.3   | Upgrade or Rollback Failure                  | 4  |
| 5     | BSF Alerts                                   |    |
| 5.1   | Configuring BSF Alerts                       | 1  |
| 5.2   | List of Alerts                               | 5  |
| 5.2.1 | AAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD | 5  |
| 5.2.2 | AAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD    | 5  |
| 5.2.3 | AAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD    | 6  |
| 5.2.4 | SCP_PEER_UNAVAILABLE                         | 6  |
| 5.2.5 | SCP_PEER_SET_UNAVAILABLE                     | 7  |
| 5.2.6 | STALE_CONFIGURATION                          | 7  |
| 5.2.7 | BSF_SERVICES_DOWN                            | 8  |
| 5.2.8 | BSFTrafficRateAboveThreshold                 | 8  |
| 5.2.9 | BSFTrafficRateAboveMajorThreshold            | 9  |

|        |                                                  |    |
|--------|--------------------------------------------------|----|
| 5.2.10 | BSFTrafficRateAboveCriticalThreshold             | 10 |
| 5.2.11 | BINDING_QUERY_RESPONSE_ERROR_MINOR               | 11 |
| 5.2.12 | BINDING_QUERY_RESPONSE_ERROR_MAJOR               | 11 |
| 5.2.13 | BINDING_QUERY_RESPONSE_ERROR_CRITICAL            | 12 |
| 5.2.14 | DIAM_RESPONSE_NETWORK_ERROR_MINOR                | 12 |
| 5.2.15 | DIAM_RESPONSE_NETWORK_ERROR_MAJOR                | 13 |
| 5.2.16 | DIAM_RESPONSE_NETWORK_ERROR_CRITICAL             | 13 |
| 5.2.17 | DUPLICATE_BINDING_REQUEST_ERROR_MINOR            | 14 |
| 5.2.18 | DUPLICATE_BINDING_REQUEST_ERROR_MAJOR            | 14 |
| 5.2.19 | DUPLICATE_BINDING_REQUEST_ERROR_CRITICAL         | 15 |
| 5.2.20 | IngressTotalErrorRateAboveMinorThreshold         | 15 |
| 5.2.21 | IngressTotalErrorRateAboveMajorThreshold         | 16 |
| 5.2.22 | IngressTotalErrorRateAboveCriticalThreshold      | 16 |
| 5.2.23 | PCFBindingErrorRateAboveMinorThreshold           | 17 |
| 5.2.24 | PCFBindingErrorRateAboveMajorThreshold           | 17 |
| 5.2.25 | PCFBindingErrorRateAboveCriticalThreshold        | 18 |
| 5.2.26 | IngressCreateErrorRateAboveMinorThreshold        | 18 |
| 5.2.27 | IngressCreateErrorRateAboveCriticalThreshold     | 19 |
| 5.2.28 | IngressCreateErrorRateAboveMajorThreshold        | 19 |
| 5.2.29 | IngressDeleteErrorRateAboveMinorThreshold        | 20 |
| 5.2.30 | IngressDeleteErrorRateAboveMajorThreshold        | 20 |
| 5.2.31 | IngressDeleteErrorRateAboveCriticalThreshold     | 21 |
| 5.2.32 | DBTierDownAlert                                  | 21 |
| 5.2.33 | CPUUsagePerServiceAboveMinorThreshold            | 22 |
| 5.2.34 | CPUUsagePerServiceAboveMajorThreshold            | 23 |
| 5.2.35 | CPUUsagePerServiceAboveCriticalThreshold         | 23 |
| 5.2.36 | MemoryUsagePerServiceAboveMinorThreshold         | 24 |
| 5.2.37 | MemoryUsagePerServiceAboveMajorThreshold         | 24 |
| 5.2.38 | MemoryUsagePerServiceAboveCriticalThreshold      | 25 |
| 5.2.39 | NRF_COMMUNICATION_FAILURE                        | 25 |
| 5.2.40 | NRF_SERVICE_REQUEST_FAILURE                      | 26 |
| 5.2.41 | PERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED | 26 |
| 5.2.42 | PodDoc                                           | 27 |
| 5.2.43 | PodCongested                                     | 27 |
| 5.2.44 | PodPendingRequestDoC                             | 28 |
| 5.2.45 | PodPendingRequestCongested                       | 28 |
| 5.2.46 | PodCPUDoC                                        | 29 |
| 5.2.47 | PodCPUCongested                                  | 29 |
| 5.2.48 | PodMemoryDoC                                     | 30 |
| 5.2.49 | PodMemoryCongested                               | 30 |
| 5.2.50 | ServiceOverloaded                                | 31 |
| 5.2.51 | ServiceResourceOverloaded                        | 32 |

|        |                                            |    |
|--------|--------------------------------------------|----|
| 5.2.52 | SYSTEM_IMPAIRMENT_MAJOR                    | 37 |
| 5.2.53 | SYSTEM_IMPAIRMENT_CRITICAL                 | 37 |
| 5.2.54 | SYSTEM_OPERATIONAL_STATE_NORMAL            | 38 |
| 5.2.55 | SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN  | 38 |
| 5.2.56 | SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN | 38 |
| 5.2.57 | DIAM_CONN_PEER_DOWN                        | 39 |
| 5.2.58 | DIAM_CONN_NETWORK_DOWN                     | 39 |

# My Oracle Support

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

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

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

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

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

# 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                                                                                                                                          |
| AF                   | Application Function                                                                                                                                                        |
| AMF                  | Access and Mobility Management Function                                                                                                                                     |
| ASM                  | Aspen Service Mesh                                                                                                                                                          |
| BSF                  | Oracle Communications Cloud Native Core, Binding Support Function                                                                                                           |
| CA                   | Certificate Authority                                                                                                                                                       |
| 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                                                                                                                           |
| GUAMI                | Globally Unique AMF Identifier                                                                                                                                              |
| IMAGE_TAG            | Image tag from release tar file. You can use any tag number.<br>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                                                                                                          |
| NPLI                 | Network Provided Location Information                                                                                                                                       |
| NRF                  | Oracle Communications Cloud Native Core, Network Repository Function                                                                                                        |
| PDB                  | Pod Disruption Budget                                                                                                                                                       |
| 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                                                                                                                                    |
| PDS                  | Policy Data Service                                                                                                                                                         |
| PRA                  | Presence Reporting Area                                                                                                                                                     |
| PRE                  | Policy Runtime Engine                                                                                                                                                       |
| PDU                  | Protocol Data Unit                                                                                                                                                          |
| Policy               | Oracle Communications Cloud Native Core, Converged Policy                                                                                                                   |

**Table (Cont.) Acronyms and Terminologies**

| Acronym | Definition                                                       |
|---------|------------------------------------------------------------------|
| QoS     | Quality of Service                                               |
| RAN     | Radio Access Network                                             |
| SAN     | Subject Alternate Name                                           |
| SMF     | Session Management Function                                      |
| UDR     | Oracle Communications Cloud Native Core, Unified Data Repository |
| SRA     | Successful Resource Allocation                                   |
| STR     | Session Termination Request (Rx)                                 |
| UE      | User Equipment                                                   |
| UPF     | User Plane Function                                              |
| UPSI    | UE Policy Section Identifier                                     |
| URSP    | UE Route Selection Policies                                      |

# What's New In This Guide

This section introduces the documentation updates for release 24.3.x.

## Release 24.3.0 - G14591-01, November 2024

- Added [Loss of Session Binding data](#) section with details of troubleshooting steps when there is loss of session binding data.
- Added details of the following alerts to support TLS in Diameter Gateway feature in [List of Alerts](#):
  - DGW\_TLS\_CONNECTION\_FAILURE
  - DIAM\_GATEWAY\_CERTIFICATE\_EXPIRY\_MINOR
  - DIAM\_GATEWAY\_CERTIFICATE\_EXPIRY\_MAJOR
  - DIAM\_GATEWAY\_CERTIFICATE\_EXPIRY\_CRITICAL
- Added details of the following alerts to support BSF Message Feed feature in [List of Alerts](#):
  - INGRESS\_GATEWAY\_DD\_UNREACHABLE\_MAJOR
  - EGRESS\_GATEWAY\_DD\_UNREACHABLE\_MAJOR

# 1

## Introduction

This document provides information about troubleshooting Oracle Communications Cloud Native Core, Binding Support Function (BSF) services and managed objects.

### 1.1 Overview

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

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

### 1.2 Audience

The BSF Troubleshooting Guide provides guidance to network administrators and professionals responsible for deployment and maintenance of BSF.

# 2

## 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>
```

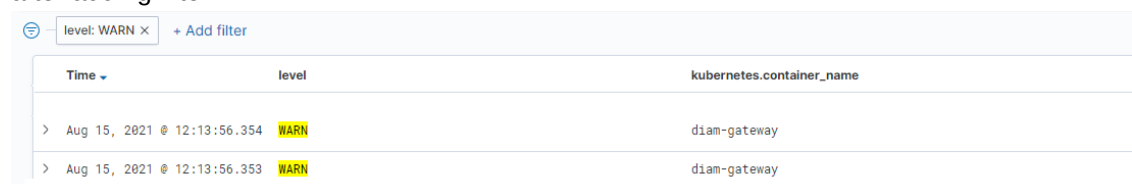
For more information on kubectl commands, see Kubernetes [website](#).

## 2.1 Log Levels

This section provides information on log levels supported by Oracle Communications Cloud Native Core, Binding Support Function (BSF).

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:



| level: WARN × + Add filter    |       |                           |
|-------------------------------|-------|---------------------------|
| Time                          | level | kubernetes.container_name |
| > Aug 15, 2021 @ 12:13:56.354 | WARN  | diam-gateway              |
| > Aug 15, 2021 @ 12:13:56.353 | WARN  | diam-gateway              |

### Supported Log Levels

For BSF, 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, Binding Support Function User Guide*.

## 2.2 Understanding Logs

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

### Understanding Logs

The following is a sample log for BSF services:

```
{
  "instant": {
    "epochSecond": 1627016656,
    "nanoOfSecond": 137175036
  },
  "thread": "Thread-2",
  "level": "INFO",
  "loggerName": "ocbsf.framework.domain.orchestration.AbstractProcess",
  "marker": {
    "name": "ALWAYS"
  },
  "message": "Received RECONFIGURE request",
  "endOfBatch": false,
  "loggerFqn": "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 BSF services.

The following table describes key attributes of a log message:

**Table 2-1 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.engineVersion | Engineering version of software                              |
| kubernetes.labels.mktgVersion   | Marketing version of software                                |
| kubernetes.labels.microservice  | Name of the microservice                                     |
| kubernetes.namespace_name       | Namespace of BSF deployment                                  |
| kubernetes.host                 | worker node name on which container is running               |
| kubernetes.pod_name             | Pod Name                                                     |
| kubernetes.container_name       | Container Name                                               |
| Docker.container_id             | Process ID internally assigned                               |
| kubernetes.labels.vendor        | Vendor of product                                            |

# 3

## 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 describes 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 BSF 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":["ocbsf"]} }]'
```

Sample output:

```
apiVersion: kyverno.io/v1
kind: ClusterPolicy
...
spec:
  rules:
    -exclude:
      resources:
        namespaces:
          -ocbsf
```

- 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": "ocbsf" }]'
```

Example:

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

Sample output:

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

- 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 BSF is installed on CNE version prior to 23.2.0  
PodSecurityPolicy (PSP) Creation

The following configurations must be performed in the Bastion Host.

- 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: bsf/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: ocbsf
rules:
  - apiGroups:
```

```
- policy
resources:
- podsecuritypolicies
verbs:
- use
resourceNames:
- debug-tool-psp
EOF
```

### *RoleBinding Creation*

Run the following command to attach the service account for your NF namespace with the role created for the tool PSP:

```
$ kubectl apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: debug-tool-rolebinding
  namespace: ocbsf
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 NF server.
- b. Open the custom\_values 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 "-" }}
```

It ensures that necessary values are added as prefix and suffix to the container name.

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

```
bsf-management-service:
  #extraContainers: DISABLED
  envMySQLDatabase: ocpm_bsf_1.7.0
  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 or 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.

**Execution of Debug Tool**

Following is the procedure to run Debug Tool.

Run the following command to enter Debug Tool Container:

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

```
$ kubectl get pods -n <k8s namespace>
```

Example:

```
$ kubectl get pods -n ocbsf
```

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

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

3. Run the debug tools:

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

Example:

```
bash -4.2$ tcpdump
```

4. Copy the output files from container to host:

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

### Tools Tested in Debug Container

Following is the list of debug tools that are tested.

*tcpdump*

**Table 3-1 tcpdump**

| Options Tested | Description                                                                                                       | Output                                                                                                                                                                                                                                                                                                | Capabilities          |
|----------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| -D             | Print the list of the network interfaces available on the system and on which <i>tcpdump</i> can capture packets. | <pre>tcpdump -D</pre> <ol style="list-style-type: none"> <li>1. eth02.</li> <li>2. nflog (Linux netfilter log (NFLOG) interface)</li> <li>3. nfqueue (Linux netfilter queue (NFQUEUE) interface)</li> <li>4. any (Pseudo-device that captures on all interfaces)</li> <li>5. lo [Loopback]</li> </ol> | NET_ADMIN,<br>NET_RAW |

Table 3-1 (Cont.) tcpdump

| Options Tested | Description                                                                  | Output                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Capabilities       |
|----------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| -i             | Listen on <i>interface</i> .                                                 | tcpdump -i eth0<br>tcpdump: verbose output suppressed, use -v or -vv for full protocol decode<br>listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes<br>12:10:37.381199 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 35<br>12:10:37.381952 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 out.     | tcpdump -w capture.pcap -i eth0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | NET_ADMIN, NET_RAW |
| -r             | Read packets from <i>file</i> (which was created with the <b>-w</b> option). | tcpdump -r capture.pcap<br>reading from file /tmp/capture.pcap, link-type EN10MB (Ethernet)<br>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 35<br>12:13:07.381194 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 31<br>12:13:07.381207 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 3-2 ip

| Options Tested | Description                 | Output                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Capabilities |
|----------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| addr show      | Look at protocol addresses. | ip addr show<br>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 forever<br>2: tunl0@NONE: <NOARP> mtu 1480 qdisc noop state DOWN group defaultlink/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00inet 0.0.0.0/0 scope host tunl0valid_lft forever preferred_lft forever<br>3: 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 | --           |

Table 3-2 (Cont.) ip

| Options Tested | Description         | Output                                                                                                                                                                                                                                                                                                     | Capabilities |
|----------------|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| route show     | List routes.        | ip route show<br>default via 169.254.1.1 dev eth0<br>169.254.1.1 dev eth0 scope link                                                                                                                                                                                                                       | --           |
| addrlabel list | List address labels | ip addrlabel list<br>prefix ::1/128 label 0<br>prefix ::/96 label 3<br>prefix ::ffff:0.0.0.0/96 label 4<br>prefix 2001::/32 label 6<br>prefix 2001:10::/28 label 7<br>prefix 3ffe::/16 label 12<br>prefix 2002::/16 label 2<br>prefix fec0::/10 label 11<br>prefix fc00::/7 label 5<br>prefix ::/0 label 1 | --           |

*netstat*

Table 3-3 netstat

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

Table 3-3 (Cont.) netstat

| Options Tested | Description                                | Output                                                                                                                                                                          | Capabilities |
|----------------|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| -i             | Display a table of all network interfaces. | netstat -i<br>Kernel Interface table<br>face MTU RX-OK RX-ERR RX-DRP<br>RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg<br>eth0 1440 4131 0 0 0 4355 0 0 0 BMRUlo 65536 0 0 0 0 0 0 0 LRU | --           |

*jq*

Table 3-4 jq

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

*curl*

Table 3-5 curl

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

*ping*

**Table 3-6 ping**

| Options Tested              | Description                                                                                                                  | Output                      | Capabilities          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------------------|
| <ip>                        | Run a ping test to see whether the target host is reachable or not.                                                          | ping 10.178.254.194         | NET_ADMIN,<br>NET_RAW |
| -c                          | Stop after sending 'c' number of ECHO_REQUEST packets.                                                                       | ping -c 5 10.178.254.194    | NET_ADMIN,<br>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,<br>NET_RAW |

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

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

Table 3-7 (Cont.) nmap

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

Table 3-7 (Cont.) nmap

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

*dig*

Table 3-8 dig

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

## 3.1 Configurable Parameters for Debug Tool

This section describes the configurable parameters that users can customize to configure debug tool.

**CNE Parameters****Table 3-9 CNE Parameters**

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

**Role Creation Parameters****Table 3-10 Role Creation**

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

**Table 3-11 Role Binding Creation**

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

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

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

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

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

# 4

## Troubleshooting BSF

This section provides information on how to troubleshoot the common errors that may occur during the installation and upgrade of Oracle Communications Cloud Native Core, Binding Support Function.

### 4.1 Deployment Issues

This section provides information on how to troubleshoot deployment issues for BSF.

#### 4.1.1 Helm Install Failure

##### If `helm install` command Fails

This section describes various scenarios and troubleshooting procedures if the `helm install` command fails.

##### Reasons for `helm install` failure:

- **Chart syntax issue**  
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 is stuck in a pending/error state and not able to execute, it will result in the timeout after 5 minutes as default timeout for `helm` command is "5 minutes". In this case, follow the below steps to troubleshoot.
- **`helm install` command failed in case of duplicated chart**

```
helm install /home/cloud-user/bsf_1.5.0/sprint3.1/ocbsf-1.5.0-  
sprint.3.1.tgz --name ocbsf2 --namespace ocbsf2 -f cust-ashish.yaml  
Error: release ocbsf2 failed: configmaps "perfinfo-config-ocbsf2" already  
exists
```

Here, configmap `perfinfo-config-ocbsf2` exists multiple times while creating the Kubernetes objects after the pre-upgrade hooks. This is a failure scenario. In this case, perform the following troubleshooting steps.

##### Troubleshooting steps:

1. Run the following command to cleanup the databases created by the `helm install` command :

```
DROP DATABASE IF EXISTS ocbsf_commonconfig;  
DROP DATABASE IF EXISTS ocbsf_config_server;  
DROP DATABASE IF EXISTS ocpm_bsf;  
DROP DATABASE IF EXISTS ocbsf_release;  
DROP DATABASE IF EXISTS ocbsf_audit_service;
```

2. Run the following 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 following command to delete all kubernetes objects:

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

4. Run the following command to list all the kubernetes objects:

```
helm ls --all
```

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

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

**Note**

If the execution of this command is taking more time, run the below command parallelly in another session to clear all the delete jobs.

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

Monitor the below command:

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

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

5. After the database cleanup, run the `helm install` command.

## 4.1.2 Loss of Session Binding data

### Symptom

When the NDB Cluster goes down (due to node group being down), it results in loss of session binding data from `pcf_binding` table in BSF.

### Problem

NOLOGGING is enabled for the `pcf_binding` table in the `ocpm_bsf` database which means there is non-persistent storage of session table in PV. Hence, when the NDB Cluster goes down there is loss of session binding data.

### Resolution Steps

To resolve this issue, perform the following steps:

1. Monitor the alerts and the KPI to determine the status of the BSF cnDBTier and the NF.
2. If there is an issue due to cnDBTier cluster down, perform a controlled shutdown of the BSF in the affected site.
3. Perform a GRR procedure in the cnDBTier to recover the database and replication.
4. Start the BSF again using the controlled shutdown procedure to reinitiate the BSF to accept traffic.

## 4.2 Startup Probes

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

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

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

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

Example:

```
kubectl exec -it test-bsf-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-bsf-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-
bsf-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.

## 4.3 Upgrade or Rollback Failure

When Oracle Communications Cloud Native Core, Binding Support Function (BSF) 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 BSF 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](#).

# 5

## BSF Alerts

This section provides information on Oracle Communications Cloud Native Core, Binding Support Function (BSF) alerts and their configuration.

### Note

The performance and capacity of the BSF system may vary based on the call model, Feature/Interface configuration, and underlying CNE and hardware environment.

## 5.1 Configuring BSF Alerts

This section describes how to configure alerts for Oracle Communications Cloud Native Core, Binding Support Function. The Alert Manager uses the Prometheus measurements values as reported by microservices in conditions under alert rules to trigger alerts.

### Note

- The Alertmanager and Prometheus tools must run in CNE namespace, for example, `occne-infra`.
- Alert file is packaged with BSF Custom Templates. The **BSF Custom Templates.zip** file can be downloaded from MOS. Unzip the **BSF Custom Templates.zip** file to get **BSF\_Alertrules.yaml** file. This file must be readily available before the user configures alerts in Prometheus.

### Configuring Alerts for CNE versions prior to 1.5

To Configure BSF alerts in Prometheus:

1. Run the following command to find the configmap and configure alerts in the Prometheus server:

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

Where:

<Namespace> is the prometheus server namespace used in Helm install command.

For Example, assuming Prometheus server is under **occne-infra** namespace, run the following command to find the configmap:

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

Output: `occne-prometheus-server 4 46d`

2. Run the following command to take a backup of the current Prometheus server configmap:

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

where, <Name> is the Prometheus configmap name used in Helm install command.

3. Check if **alertsbsf** is present in the **t\_mapConfig.yaml** file by running the following command:

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

Depending on the outcome of the previous step, perform any of the following:

- If **alertsbsf** is present, delete the **alertsbsf** entry from the **t\_mapConfig.yaml** file, by running the following command:

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

**Note**

Run this command only once.

- If **alertsbsf** is not present, add the **alertsbsf** entry in the **t\_mapConfig.yaml** file by running the following command:

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

**Note**

Run this command only once.

4. Run the following command to reload the configmap with the modified file:

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

**Note**

It is not required for AlertRules.

5. Add **BSF\_Alertrules.yaml** file into Prometheus server configmap by running the following command :

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

where, <PATH> is the location of the **BSF\_Alertrules.yaml** file.

6. Restart prometheus-server pod.

7. Verify the alerts in Prometheus GUI.

The following image shows the BSF Alerts:

/etc/config/alerts/BSF\_Alertrules.yaml > BSF\_ALERTS

**BSF\_SERVICES\_DOWN** (2 active)

**IngressCreateErrorRateAbove1Percent** (2 active)

**IngressTotalErrorRateAbove10Percent** (1 active)

**PCFBindingErrorRateAbove1Percent** (3 active)

**BSFTrafficRateAboveThreshold** (0 active)

**IngressDeleteErrorRateAbove1Percent** (0 active)

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

To Configure BSF alerts in Prometheus:

1. Copy the **BSF\_Alertrules.yaml** file to the Bastion Host. Place this file in the /var/ocne/cluster/<cluster-name>/artifacts/alerts directory on the OCCNE Bastion Host.

```
$ pwd /var/ocne/cluster/stark/artifacts/alerts
$ ls
ocne_alerts.yaml
$ vi BSF_Alertrules.yaml
$ ls BSF_Alertrules.yaml ocne_alerts.yaml
```

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

```
$ chmod 644 BSF_Alertrules.yaml
```

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

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

4. To verify the alerts in the Prometheus GUI, select the Alerts tab and view alert details by selecting any individual rule from the list of configured rules.

### Configuring Alerts for CNE 1.9.0 and later versions

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

1. Copy the **BSF\_Alertrules.yaml** file to the Bastion Host.
2. To create or replace the PrometheusRule CRD, run the following command:

```
$ kubectl apply -f ocbsf-alerting-rules.yaml -n <namespace>
```

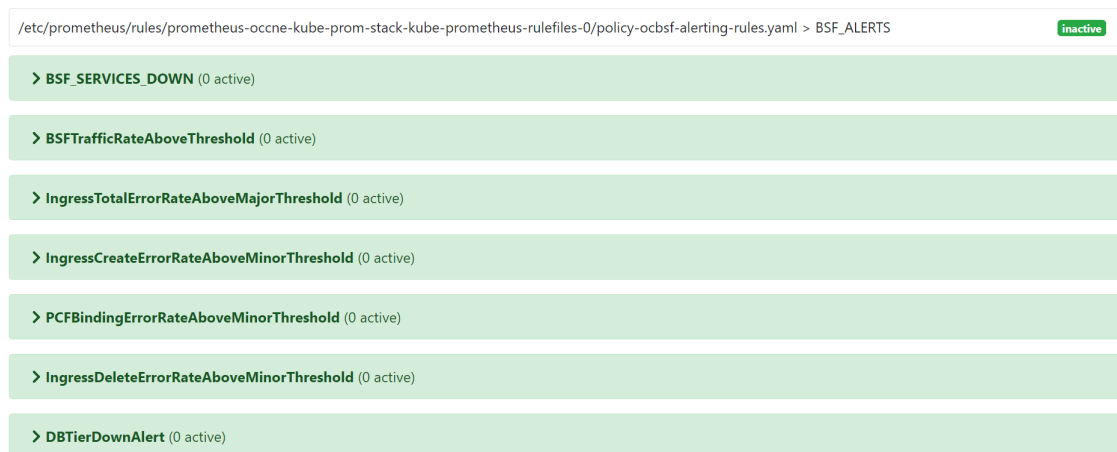
To verify if the CRD is created, run the following command:

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

3. To verify the alerts in the Prometheus GUI, select the Alerts tab and view alert details by selecting any individual rule from the list of configured alerts.

The following screen capture shows the Prometheus dashboard with BSF alerts configured for CNE 1.9.0:

**Figure 5-1 BSF alerts on Prometheus Dashboard**



#### Note

1. For upgrading to BSF 1.11.0 from a previous supported version on CNE 1.8.x, use the **BSF\_Alertrules\_cne1.5+.yaml** file. On the Prometheus dashboard, configure both old and new alert rules.
2. For installing BSF 1.11.0 on CNE 1.9.0 and later versions, use the **BSF\_Alertrules\_cne1.9+.yaml** file. On the Prometheus dashboard, configure only the new alert rules.

## 5.2 List of Alerts

This section lists the alerts available for Oracle Communications Cloud Native Core, Binding Support Function (BSF).

### 5.2.1 AAA\_RX\_FAIL\_COUNT\_EXCEEDS\_CRITICAL\_THRESHOLD

**Table 5-1 AAA\_RX\_FAIL\_COUNT\_EXCEEDS\_CRITICAL\_THRESHOLD**

| Field               | Details                                                                                                                                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description         | AAA Rx fail count exceeds the critical threshold limit.                                                                                                                                                               |
| Summary             | AAA Rx fail count exceeds the critical threshold limit.                                                                                                                                                               |
| Severity            | CRITICAL                                                                                                                                                                                                              |
| Condition           | sum by(namespace)<br>(rate(ocbsf_diam_response_network_total{msgType="AAA", appId="16777236", responseCode!~"2.*"}[5m]) /<br>rate(ocbsf_diam_response_network_total{msgType="AAA", appId="16777236"}[5m])) * 100 > 90 |
| OID                 | 1.3.6.1.4.1.323.5.3.37.1.2.40                                                                                                                                                                                         |
| Metric Used         | ocbsf_diam_response_network_total                                                                                                                                                                                     |
| Recommended Actions | For any additional guidance, contact My Oracle Support.                                                                                                                                                               |

### 5.2.2 AAA\_RX\_FAIL\_COUNT\_EXCEEDS\_MAJOR\_THRESHOLD

**Description**

AAA Rx fail count exceeds the major threshold limit

**Summary**

AAA Rx fail count exceeds the major threshold limit.

**Severity**

MAJOR

**Condition**

sum by(namespace)(rate(ocbsf\_diam\_response\_network\_total{msgType="AAA",  
appId="16777236", responseCode!~"2.\*"}[5m]) /  
rate(ocbsf\_diam\_response\_network\_total{msgType="AAA", appId="16777236"}[5m])) \* 100  
<=90 and sum by(namespace)(rate(ocbsf\_diam\_response\_network\_total{msgType="AAA",  
appId="16777236", responseCode!~"2.\*"}[5m]) /  
rate(ocbsf\_diam\_response\_network\_total{msgType="AAA", appId="16777236"}[5m])) \* 100 >  
80

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.40

**Metric Used**

ocbsf\_diam\_response\_network\_total

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.3 AAA\_RX\_FAIL\_COUNT\_EXCEEDS\_MINOR\_THRESHOLD

**Description**

AAA Rx fail count exceeds the minor threshold limit.

**Summary**

AAA Rx fail count exceeds the minor threshold limit.

**Severity**

MINOR

**Condition**

```
sum by(namespace)(rate(ocbsf_diam_response_network_total{msgType="AAA",  
appld="16777236", responseCode!~"2.*"}[5m]) /  
rate(ocbsf_diam_response_network_total{msgType="AAA", appld="16777236"}[5m])) * 100  
<=80 and sum by(namespace)(rate(ocbsf_diam_response_network_total{msgType="AAA",  
appld="16777236", responseCode!~"2.*"}[5m]) /  
rate(ocbsf_diam_response_network_total{msgType="AAA", appld="16777236"}[5m])) * 100 >  
60
```

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.40

**Metric Used**

ocbsf\_diam\_response\_network\_total

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.4 SCP\_PEER\_UNAVAILABLE

**Description**

Configured SCP peer is unavailable.

**Summary**

ocbsf\_oc\_egressgateway\_peer\_health\_status != 0. SCP peer [ {{ \$labels.peer }} ] is unavailable.

**Severity**

Major

**Condition****OID**

1.3.6.1.4.1.323.5.3.37.1.2.38

**Metric Used**

ocbsf\_oc\_egressgateway\_peer\_health\_status

**Recommended Actions**

This alert gets cleared when unavailable SCPs become available.

For any additional guidance, contact My Oracle Support.

## 5.2.5 SCP\_PEER\_SET\_UNAVAILABLE

**Description**

None of the SCP peer available for configured peerset.

**Summary**

(ocbsf\_oc\_egressgateway\_peer\_count - ocbsf\_oc\_egressgateway\_peer\_available\_count) !=0 and (ocbsf\_oc\_egressgateway\_peer\_count) > 0. {{ \$value }} SCP peers under peer set {{\$labels.peerset}} are currently available.

**Severity**

Critical

**Condition**

One of the SCPs has been marked unhealthy.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.39

**Metric Used**

oc\_egressgateway\_peer\_count and oc\_egressgateway\_peer\_available\_count

**Recommended Actions**

NF clears the critical alarm when atleast one SCP peer in a peerset becomes available such that all other SCP peers in the given peerset are still unavailable.

For any additional guidance, contact My Oracle Support.

## 5.2.6 STALE\_CONFIGURATION

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

(sum by(namespace) (topic\_version{app\_kubernetes\_io\_name="config-server",topicName="config.level"})) / (count by(namespace) (topic\_version{app\_kubernetes\_io\_name="config-server",topicName="config.level"})) != (sum by(namespace) (topic\_version{app\_kubernetes\_io\_name!="config-server",topicName="config.level"})) / (count by(namespace) (topic\_version{app\_kubernetes\_io\_name!="config-server",topicName="config.level"}))

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.40

**Metric Used**

topic\_version

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.7 BSF\_SERVICES\_DOWN

**Description**

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

**Summary**

{{labels.service}} is not running!

**Severity**

Critical

**Condition**

None of the pods of the Binding Support Function (BSF) application is available.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.1

**Metric Used**

appinfo\_service\_running

**Recommended Actions**

Perform the following steps:

- Check for service specific alerts that may be causing the issues with service exposure.
- Verify if the POD is in a *Running* state by using the following command:

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

If the output shows any pod that is not running, copy the pod name and run the following command:

```
kubectl describe pod <podname> -n <namespace>
```

- Check the application logs on Kibana and look for database related failures such as connectivity, invalid secrets, and so on. The logs can be easily filtered for different services.
- Check for Helm status to ensure no errors are present by using the following command:

```
helm status <release-name> -n <namespace>
```

If it is not in STATUS: DEPLOYED, capture the logs and events again.

In case the issue persists, capture the outputs for the preceding steps and contact [My Oracle Support](#).

## 5.2.8 BSFTrafficRateAboveThreshold

**Description**

BSF service Ingress traffic Rate is above threshold of Max MPS(1000) (current value is: {{ \$value }})

**Summary**

Traffic Rate is above 90 Percent of Max requests per second(1000)

**Severity**

Major

**Condition**

The total Binding Management service Ingress traffic rate has crossed the configured threshold of 900 TPS.

The default value of this alert trigger point in the `BSF_Alertrules.yaml` file is when the Binding management service Ingress Rate crosses 90% of maximum ingress requests per second.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.2

**Metric Used**

ocpm\_ingress\_request\_total

**Recommended Actions**

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

 **Note**

Threshold levels can be configured using the `BSF_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 an increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any assistance, contact [My Oracle Support](#).

## 5.2.9 BSFTrafficRateAboveMajorThreshold

**Description**

BSF service Ingress traffic Rate is above threshold of Max MPS(1000) (current value is: {{ \$value }})

**Summary**

Traffic Rate is above 80 Percent of Max requests per second(1000)

**Severity**

Major

**Condition**

The total Binding Management service Ingress traffic rate has crossed the configured threshold of 800 TPS.

The default value of this alert trigger point in the `BSF_Alertrules.yaml` file is when the Binding management service Ingress Rate crosses 80% of maximum ingress requests per second.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.2

**Metric Used**

ocbsf\_ingress\_request\_total

**Recommended Actions**

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

**Note**

Threshold levels can be configured using the `BSF_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 an increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any assistance, contact [My Oracle Support](#).

## 5.2.10 BSFTrafficRateAboveCriticalThreshold

**Description**

BSF service Ingress traffic Rate is above threshold of Max MPS(1000) (current value is: {{ \$value }})

**Summary**

Traffic Rate is above 90 Percent of Max requests per second(1000)

**Severity**

Critical

**Condition**

The total Binding Management service Ingress traffic rate has crossed the configured threshold of 900 TPS.

The default value of this alert trigger point in the `BSF_Alertrules.yaml` file is when the Binding management service Ingress Rate crosses 90% of maximum ingress requests per second.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.2

**Metric Used**

ocbsf\_ingress\_request\_total

**Recommended Actions**

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

**Note**

Threshold levels can be configured using the `BSF_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 an increase in 4xx and 5xx error response codes.
2. Check **Ingress Gateway** logs on Kibana to determine the reason for the errors.

For any assistance, contact [My Oracle Support](#).

## 5.2.11 BINDING\_QUERY\_RESPONSE\_ERROR\_MINOR

**Description**

At least 20% of the Binding Query connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Summary**

At least 20% of the Binding Query connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Severity**

Minor

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_bindingQuery\_response\_total

**Condition**

BSF is able to raise threshold based alerts for duplicate Binding request received and handled at BSF.

If 30% of the requests fails for 10 mins, BSF is able to raise Minor Alert indicating duplicate Binding request are being detected at BSF.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.12 BINDING\_QUERY\_RESPONSE\_ERROR\_MAJOR

**Description**

At least 50% of the Binding Query connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Summary**

At least 50% of the Binding Query connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Severity**

Major

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_bindingQuery\_response\_total

**Condition**

BSF is able to raise threshold based alerts for duplicate Binding request received and handled at BSF.

If 50% of the requests fails for 10 mins, BSF is able to raise Major Alert indicating duplicate Binding request are being detected at BSF.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.13 BINDING\_QUERY\_RESPONSE\_ERROR\_CRITICAL

**Description**

At least 70% of the Binding Query connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Summary**

At least 70% of the Binding Query connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Severity**

Minor

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_bindingQuery\_response\_total

**Condition**

BSF is able to raise threshold based alerts for duplicate Binding request received and handled at BSF.

If 70% of the requests fails for 10 mins, BSF is able to raise Critical Alert indicating duplicate Binding request are being detected at BSF.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.14 DIAM\_RESPONSE\_NETWORK\_ERROR\_MINOR

**Description**

At least 20% of the Binding Registration requests failed were duplicate failures.

**Summary**

At least 20% of the Binding Registration requests failed were duplicate failures.

**Severity**

Minor

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_diam\_response\_network\_total

**Condition**

BSF is able to raise threshold based alerts for Message/Service Request Failure. When message failures like Binding Registration or deregistration request, Diameter Requests Failure with error "DIAMETER\_UNABLE\_TO\_DELIVER" are observed, BSF is able to raise alerts.

If 20% of the requests fails for 10 mins, BSF is able to raise Minor Alert indicating the procedure or service which is failing.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.15 DIAM\_RESPONSE\_NETWORK\_ERROR\_MAJOR

**Description**

At least 50% of the Diam Response connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Summary**

At least 50% of the Diam Response connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Severity**

Major

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_diam\_response\_network\_total

**Condition**

BSF is able to raise threshold based alerts for Message/Service Request Failure. When message failures like Binding Registration or deregistration request, Diameter Requests Failure with error "DIAMETER\_UNABLE\_TO\_DELIVER" are observed, BSF is able to raise alerts.

If 50% of the requests fails for 10 mins, BSF is able to raise Major Alert indicating the procedure or service which is failing.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.16 DIAM\_RESPONSE\_NETWORK\_ERROR\_CRITICAL

**Description**

At least 70% of the Diam Response connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Summary**

At least 70% of the Diam Response connection requests failed with error 'DIAMETER\_UNABLE\_TO\_DELIVER'.

**Severity**

Critical

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_diam\_response\_network\_total

**Condition**

BSF is able to raise threshold based alerts for Message/Service Request Failure. When message failures like Binding Registration or deregistration request, Diameter Requests Failure with error "DIAMETER\_UNABLE\_TO\_DELIVER" are observed, BSF is able to raise alerts.

If 75% of the requests fails for 10 mins, BSF is able to raise Critical Alert indicating the procedure or service which is failing.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.17 DUPLICATE\_BINDING\_REQUEST\_ERROR\_MINOR

**Description**

At least 20% of the Binding Registration requests failed were duplicate failures.

**Summary**

At least 20% of the Binding Registration requests failed were duplicate failures.

**Severity**

Minor

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_ingress\_request\_total

**Condition**

If 30% of the requests fails for 10 mins, BSF is able to raise Minor Alert indicating duplicate Binding request are being detected at BSF.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.18 DUPLICATE\_BINDING\_REQUEST\_ERROR\_MAJOR

**Description**

At least 50% of the Binding Registration requests failed were duplicate failures.

**Summary**

At least 50% of the Binding Registration requests failed were duplicate failures.

**Severity**

Major

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_ingress\_request\_total

**Condition**

If 50% of the requests fails for 10 mins, BSF is able to raise Major Alert indicating duplicate Binding request are being detected at BSF.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.19 DUPLICATE\_BINDING\_REQUEST\_ERROR\_CRITICAL

**Description**

At least 70% of the Binding Registration requests failed were duplicate failures.

**Summary**

At least 70% of the Binding Registration requests failed were duplicate failures.

**Severity**

Critical

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.24

**Metric Used**

ocbsf\_ingress\_request\_total

**Condition**

If 70% of the requests fails for 10 mins, BSF is able to raise Critical Alert indicating duplicate Binding request are being detected at BSF.

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.20 IngressTotalErrorRateAboveMinorThreshold

**Description**

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

**Summary**

Transaction Error Rate detected above 1 Percent of Total Transactions

**Severity**

Minor

**Condition**

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

**OID**

oid: "1.3.6.1.4.1.323.5.3.37.1.2.3"

**Metric Used**

ocbsf\_ingress\_response\_total

**Recommended Actions**

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

For any assistance, contact [My Oracle Support](#).

## 5.2.21 IngressTotalErrorRateAboveMajorThreshold

**Description**

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

**Summary**

Transaction Error Rate detected above 10 Percent of Total Transactions

**Severity**

Critical

**Condition**

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

**OID**

oid: "1.3.6.1.4.1.323.5.3.37.1.2.3"

**Metric Used**

ocpm\_ingress\_response\_total

**Recommended Actions**

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

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

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

For any assistance, contact [My Oracle Support](#).

## 5.2.22 IngressTotalErrorRateAboveCriticalThreshold

**Description**

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

**Summary**

Transaction Error Rate detected above 10 Percent of Total Transactions

**Severity**

Critical

**Condition**

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

**OID**

oid: "1.3.6.1.4.1.323.5.3.37.1.2.3"

**Metric Used**

ocbsf\_ingress\_response\_total

**Recommended Actions**

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

For any assistance, contact [My Oracle Support](#).

## 5.2.23 PCFBindingErrorRateAboveMinorThreshold

**Description**

PCF Binding Error Rate above 1 Percent in {{\$labels.kubernetes\_name}} in {{\$labels.kubernetes\_namespace}}

**Summary**

PCF Binding Error Rate in {{\$labels.kubernetes\_node}} (current value is: {{ \$value }})

**Severity**

Critical

**Condition**

The total number of failed transactions for retrieving PCF Bindings is above 1 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.5

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

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

To assess the reason for failed transactions, check the service specific metrics for the GET method.

For any assistance, contact [My Oracle Support](#).

## 5.2.24 PCFBindingErrorRateAboveMajorThreshold

**Description**

PCF Binding Error Rate above 5 Percent in {{\$labels.microservice}} in {{\$labels.namespace}}

**Summary**

PCF Binding Error Rate in {{\$labels.kubernetes\_node}} (current value is: {{ \$value }})

**Severity**

Major

**Condition**

The total number of failed transactions for retrieving PCF Bindings is above 5 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.5

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

The alert gets cleared when the number of failed transactions is below 5% of the total transactions.

To assess the reason for failed transactions, check the service specific metrics for the GET method.

For any assistance, contact [My Oracle Support](#).

## 5.2.25 PCFBindingErrorRateAboveCriticalThreshold

**Description**

PCF Binding Error Rate above 10 Percent in {{\$labels.microservice}} in {{\$labels.namespace}}

**Summary**

PCF Binding Error Rate in {{\$labels.kubernetes\_node}} (current value is: {{ \$value }})

**Severity**

Critical

**Condition**

The total number of failed transactions for retrieving PCF Bindings is above 10 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.5

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

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

To assess the reason for failed transactions, check the service specific metrics for the GET method.

For any assistance, contact [My Oracle Support](#).

## 5.2.26 IngressCreateErrorRateAboveMinorThreshold

**Description**

BSF Ingress Create Error Rate above 1 Percent in {{\$labels.kubernetes\_name}} in {{\$labels.kubernetes\_namespace}}

**Summary**

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

**Severity**

Minor

**Condition**

The total number of failed transactions for creating requests (POST method of operation) for BSF service is above 1 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.4

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

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

To assess the reason for failed transactions, check the service specific metrics for the POST method.

For any assistance, contact [My Oracle Support](#).

## 5.2.27 IngressCreateErrorRateAboveCriticalThreshold

**Description**

BSF Ingress Create Error Rate above 10 Percent in {{ \$labels.microservice }} in {{ \$labels.namespace }}

**Summary**

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

**Severity**

Critical

**Condition**

The total number of failed transactions for creating requests (POST method of operation) for BSF service is above 10 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.4

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

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

To assess the reason for failed transactions, check the service specific metrics for the POST method.

For any assistance, contact [My Oracle Support](#).

## 5.2.28 IngressCreateErrorRateAboveMajorThreshold

**Description**

BSF Ingress Create Error Rate above 5 Percent in {{ \$labels.microservice }} in {{ \$labels.namespace }}

**Summary**

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

**Severity**

Major

**Condition**

The total number of failed transactions for creating requests (POST method of operation) for BSF service is above 5 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.4

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

The alert gets cleared when the number of failed transactions is below 5% of the total transactions.

To assess the reason for failed transactions, check the service specific metrics for the POST method.

For any assistance, contact [My Oracle Support](#).

## 5.2.29 IngressDeleteErrorRateAboveMinorThreshold

**Description**

Ingress Delete Error Rate above 1 Percent in {{ \$labels.kubernetes\_name }} in {{ \$labels.kubernetes\_namespace }}

**Summary**

Ingress Delete Error Rate in {{ \$labels.kubernetes\_node }} (current value is: {{ \$value }})

**Severity**

Critical

**Condition**

The total number of failed transactions for delete requests (DELETE method of operation) for BSF service is above 1 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.6

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

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

To assess the reason for failed transactions, check the service specific metrics for the DELETE method.

For any assistance, contact [My Oracle Support](#).

## 5.2.30 IngressDeleteErrorRateAboveMajorThreshold

**Description**

Ingress Delete Error Rate above 5 Percent in {{ \$labels.microservice }} in {{ \$labels.namespace }}

**Summary**

Ingress Delete Error Rate in {{ \$labels.kubernetes\_node }} (current value is: {{ \$value }})

**Severity**

Major

**Condition**

The total number of failed transactions for delete requests (DELETE method of operation) for BSF service is above 5 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.6

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

The alert gets cleared when the number of failed transactions is below 5% of the total transactions.

To assess the reason for failed transactions, check the service specific metrics for the DELETE method.

For any assistance, contact [My Oracle Support](#).

## 5.2.31 IngressDeleteErrorRateAboveCriticalThreshold

**Description**

Ingress Delete Error Rate above 10 Percent in {{ \$labels.microservice }} in {{ \$labels.namespace }}

**Summary**

Ingress Delete Error Rate in {{ \$labels.kubernetes\_node }} (current value is: {{ \$value }})

**Severity**

Critical

**Condition**

The total number of failed transactions for delete requests (DELETE method of operation) for BSF service is above 10 percent of the total transactions.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.6

**Metric Used**

http\_server\_requests\_seconds\_count

**Recommended Actions**

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

To assess the reason for failed transactions, check the service specific metrics for the DELETE method.

For any assistance, contact [My Oracle Support](#).

## 5.2.32 DBTierDownAlert

**Description**

DB cannot be reachable!

**Summary**

DB cannot be reachable!

**Severity**

Critical

**Condition**

The database is not available.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.7

**Metric Used**

appinfo\_category\_running

**Recommended Actions**

Check whether the database service is up.

Check the status or age of the MySQL pod by using the following command:

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

where <namespace> is the namespace used to deploy MySQL pod.

This alert is cleared automatically when the DB service is up and running.

## 5.2.33 CPUUsagePerServiceAboveMinorThreshold

**Description**

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

**Summary**

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

**Severity**

Minor

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.8

**Metric Used**

cgroup\_cpu\_usage

**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 `BSF_Alertrules.yaml` file.

For any assistance, contact [My Oracle Support](#).

## 5.2.34 CPUUsagePerServiceAboveMajorThreshold

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.9

**Metric Used**

cgroup\_cpu\_usage

**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 `BSF_Alertrules.yaml` file.

For any assistance, contact [My Oracle Support](#).

## 5.2.35 CPUUsagePerServiceAboveCriticalThreshold

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.10

**Metric Used**

cgroup\_cpu\_usage

**Recommended Actions**

The alert gets cleared when the CPU utilization falls below the critical threshold.

**Note**

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

For any assistance, contact [My Oracle Support](#).

## 5.2.36 MemoryUsagePerServiceAboveMinorThreshold

**Description**

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

**Summary**

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

**Severity**

Minor

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.11

**Metric Used**

`cgroup_memory_usage`

**Recommended Actions**

The alert gets cleared when the memory utilization falls below the minor threshold or crosses the major threshold, in which case `MemoryUsagePerServiceAboveMajorThreshold` alert shall be raised.

**Note**

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

For any assistance, contact [My Oracle Support](#).

## 5.2.37 MemoryUsagePerServiceAboveMajorThreshold

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.12

**Metric Used**

cgroup\_memory\_usage

**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 `BSF_Alertrules.yaml` file.

For any additional guidance, contact [My Oracle Support](#).

## 5.2.38 MemoryUsagePerServiceAboveCriticalThreshold

**Summary**

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

**Description**

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

**Severity**

Critical

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.13

**Metric Used**

cgroup\_memory\_usage

**Recommended Actions**

The alert gets cleared when the memory utilization falls below the critical threshold.

**Note**

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

For any assistance, contact [My Oracle Support](#).

## 5.2.39 NRF\_COMMUNICATION\_FAILURE

**Summary**

There has been a external failure communication error with NRF.

**Description**

There has been a external failure communication error with NRF.

**Severity**

Info

**Condition**

BSF is able to raise and clear alarms for the failure of external communication, that is in case of the unavailability of producer NRF.

- Raise alert if: `ocbsf_nrfclient_nrf_operative_status == 0`
- Clear alert if: `ocbsf_nrfclient_nrf_operative_status == 1`

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.18

**Metric Used**`ocbsf_nrfclient_nrf_operative_status`**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.40 NRF\_SERVICE\_REQUEST\_FAILURE

**Summary**

There has been a Service Request Failure with NRF, either due to Registration failure or Profile update failure.

**Description**

There has been a Service Request Failure with NRF, either a Registration failure, Heartbeat failure, or Profile Update Failure.

**Severity**

Info

**Condition**

BSF is able to raise and clear alarms in case of Service Request Failures with NRF like the Registration failure, Heartbeat failure, Profile Update Failure.

- raise alert if: `ocbsf_nrfclient_nfUpdate_status == 0`
- clear alert if: `ocbsf_nrfclient_nfUpdate_status == 1`

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.19

**Metric Used**`ocbsf_nrfclient_nfUpdate_status`**Recommended Actions**

For any assistance, contact [My Oracle Support](#).

## 5.2.41 PERF\_INFO\_ACTIVE\_OVERLOAD\_THRESHOLD\_FETCH\_FAILED

**Summary**

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

**Description**

The application raises PERF\_INFO\_ACTIVE\_OVERLOAD\_THRESHOLD\_FETCH\_FAILED alert when it fails to fetch the current active overload level threshold data and `active_overload_threshold_fetch_failed == 1`.

**Severity**

Major

**Condition**

`active_overload_threshold_fetch_failed == 1`

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.20

**Metric Used**

`active_overload_threshold_fetch_failed`

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support.

## 5.2.42 PodDoc

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

The pod congestion status is set to Danger of Congestion.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.25

**Metric Used**

`ocbsf_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 (<https://support.oracle.com>).

## 5.2.43 PodCongested

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

The pod congestion status is set to congested.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.26

**Metric Used**

ocbsf\_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 (<https://support.oracle.com>).

## 5.2.44 PodPendingRequestDoC

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.27

**Metric Used**

ocbsf\_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 (<https://support.oracle.com>).

## 5.2.45 PodPendingRequestCongested

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

The pod congestion status is set to congested for PendingRequest.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.28

**Metric Used**

ocbsf\_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 (<https://support.oracle.com>).

## 5.2.46 PodCPUDoC

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

The pod congestion status is set to DoC for CPU.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.29

**Metric Used**

ocbsf\_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 (<https://support.oracle.com>).

## 5.2.47 PodCPUCongested

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

The pod congestion status is set to congested for CPU.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.30

**Metric Used**

ocbsf\_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 (<https://support.oracle.com>).

## 5.2.48 PodMemoryDoC

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

The pod congestion status is set to DoC for memory.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.31

**Metric Used**

ocbsf\_pod\_resource\_congestion\_state{type="memory"}

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support (<https://support.oracle.com>).

## 5.2.49 PodMemoryCongested

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

The pod congestion status is set to congested for memory.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.32

**Metric Used**

ocbsf\_pod\_resource\_congestion\_state{type="memory"}

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support (<https://support.oracle.com>).

## 5.2.50 ServiceOverloaded

**Description**

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

**Summary**

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

**Severity**

Minor

**Condition**

The overload level of the service is L1.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.14

**Metric Used**

load\_level

**Recommended Actions**

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

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

The overload level of the service is L2.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.14

**Metric Used**

load\_level

**Recommended Actions**

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

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

The overload level of the service is L3.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.14

**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.

## 5.2.51 ServiceResourceOverloaded

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

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

**Summary**

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

**Severity**

Minor

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="memory"}

**Recommended Actions**

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

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="memory"}

**Recommended Actions**

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

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="memory"}

**Recommended Actions**

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

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

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

**Summary**

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

**Severity**

Minor

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="cpu"}

**Recommended Actions**

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

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="cpu"}

**Recommended Actions**

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

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="cpu"}

**Recommended Actions**

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

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

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

**Summary**

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

**Severity**

Minor

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="svc\_pending\_count"}

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support.

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="svc\_pending\_count"}

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support.

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="svc\_pending\_count"}

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support.

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

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

**Summary**

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

**Severity**

Minor

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="svc\_failure\_count"}

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support.

**Description**

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

**Summary**

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

**Severity**

Major

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**Metric Used**

service\_resource\_overload\_level{type="svc\_failure\_count"}

**Recommended Actions**

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

For any additional guidance, contact My Oracle Support.

**Description**

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

**Summary**

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

**Severity**

Critical

**Condition**

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

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.15

**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.

## 5.2.52 SYSTEM\_IMPAIRMENT\_MAJOR

**Description**

Major Impairment alert raised for REPLICATION\_FAILED or REPLICATION\_CHANNEL\_DOWN or BINLOG\_STORAGE usage

**Summary**

Major Impairment alert raised for REPLICATION\_FAILED or REPLICATION\_CHANNEL\_DOWN or BINLOG\_STORAGE usage

**Severity**

Major

**Condition**

Major Impairment alert

**OID**

1.3.6.1.4.1.323.5.3.36.1.2.43

**Metric Used**

db\_tier\_replication\_status

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.53 SYSTEM\_IMPAIRMENT\_CRITICAL

**Description**

Critical Impairment alert raised for REPLICATION\_FAILED or REPLICATION\_CHANNEL\_DOWN or BINLOG\_STORAGE usage

**Summary**

Critical Impairment alert raised for REPLICATION\_FAILED or REPLICATION\_CHANNEL\_DOWN or BINLOG\_STORAGE usage

**Severity**

Critical

**Condition**

Critical Impairment alert

**OID**

1.3.6.1.4.1.323.5.3.36.1.2.43

**Metric Used**

db\_tier\_replication\_status

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.54 SYSTEM\_OPERATIONAL\_STATE\_NORMAL

**Description**

System Operational State is now in normal state

**Summary**

System Operational State is now in normal state

**Severity**

Info

**Condition**

System Operational State is now in normal state

**OID**

1.3.6.1.4.1.323.5.3.36.1.2.44

**Metric Used**

system\_operational\_state == 1

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.55 SYSTEM\_OPERATIONAL\_STATE\_PARTIAL\_SHUTDOWN

**Description**

System Operational State is now in partial shutdown state

**Summary**

System Operational State is now in partial shutdown state

**Severity**

Info

**Condition**

System Operational State is now in partial shutdown state

**OID**

1.3.6.1.4.1.323.5.3.36.1.2.44

**Metric Used**

system\_operational\_state == 2

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.56 SYSTEM\_OPERATIONAL\_STATE\_COMPLETE\_SHUTDOWN

**Description**

System Operational State is now in complete shutdown state

**Summary**

System Operational State is now in complete shutdown state

**Severity**

Info

**Condition**

System Operational State is now in complete shutdown state

**OID**

1.3.6.1.4.1.323.5.3.36.1.2.44

**Metric Used**

system\_operational\_state == 3

**Recommended Actions**

For any additional guidance, contact My Oracle Support.

## 5.2.57 DIAM\_CONN\_PEER\_DOWN

**Description**

Diameter connection to peer {{ \$labels.origHost }} is down.

**Summary**

Diameter connection to peer down.

**Severity**

Major

**Condition**

Diameter connection to peer origHost in given namespace is down.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.18

**Metric Used**

ocbsf\_diam\_conn\_network

**Recommended Actions**For any assistance, contact [My Oracle Support](#).

## 5.2.58 DIAM\_CONN\_NETWORK\_DOWN

**Description**

All diameter network connections are down.

**Summary**

All diameter network connections are down.

**Severity**

Critical

**Condition**

All diameter networks in a kubernetes namespace are down.

**OID**

1.3.6.1.4.1.323.5.3.37.1.2.19

**Metric Used**

ocbsf\_diam\_conn\_network

**Recommended Actions**

For any assistance, contact [My Oracle Support](#).