Oracle® Communications

Cloud Native Core, Binding Support Function User Guide

Release 25.1.100
G19512-01
April 2025

Oracle Communications Cloud Native Core, Binding Support Function User Guide, Release 25.1.100

G19512-01

Contents

4 Configuring BSF Using CNC Console

5 BSF Alerts

My Oracle Support

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

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

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

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

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

What's New in This Guide

This section introduces the new and updated features for release 25.1.1xx.

Release 25.1.100 - G19512-01, April 2025

- **Feature Updates:**
  - **New Features:**
    - **Traffic Segregation**
      - Added the Traffic Segregation section to support Ingress and Egress Gateway traffic segregation in BSF.
  - **Stale Binding Detection Audit, Report and Recover**
    - Added Stale Binding Detection Audit, Report and Recover to describe revalidation of session binding records in BSF.
    - Added **Enable Binding Revalidation** to Management Service to configure revalidation of session binding records in BSF.
    - Added the following metrics to BSF Management Service to support revalidation of session binding records in BSF:
      - ocbsf_binding_revalidation_request_total
      - ocbsf_binding_revalidation_response_total
      - ocbsf_binding_revalidation_pcfBinding_missing_total
    - Added the following aletrts to List of Alerts to support revalidation of session binding records in BSF:
      - BINDING_REVALIDATION_PCF_BINDING_MISSING_MINOR
      - BINDING_REVALIDATION_PCF_BINDING_MISSING_MAJOR
      - BINDING_REVALIDATION_PCF_BINDING_MISSING_CRITICAL
- **Enhancements:**
  - **Support for cnDBTier APIs in CNC Console**
    - Added information about cnDBTier APIs support for Georeplication recovery in the Support for cnDBTier Functionalities in CNC Console section.
    - Added the Georeplication Recovery section to view the status of cnDBTier clusters and georeplication status on the CNC Console.
  - Added error code dictionary for Egress Gateway, Ingress Gateway, and NRF Client in Error Code Dictionary section.

Acronyms

This following table lists the acronyms and the terminologies used in this document.

Table Acronyms

Acronym	Description
AF	Application Function
BSF	Binding Support Function
DNN	Domain Network Name
FQDN	Fully Qualified Domain Names
GPSI	Generic Public Subscription Identifier
HTTP	Hypertext Transfer Protocol
MCC	Mobile Country Code
MNC	Mobile Network Code
NEF	Network Exposure Function
NF	Network Function
NID	Network Identifier
NRF	Oracle Communications Cloud Native Core, Network Repository Function
PCF	Oracle Communications Cloud Native Core, Policy Control Function
OCPM	Oracle Communications Policy Management
PDU	Protocol Data Unit
RDBMS	Relational Database Management System
S-NSSAI	Single Network Slice Selection Assistance Information. An S-NSSAI is comprised of: - A Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services; - A Slice Differentiator (SD), which is an optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.
SMF	Session Management Function
SNPN	Stand-alone Non-Public Network
SUPI	Subscription Permanent Identifier
UDSF	Unstructured Data Storage network function
UE	User Equipment

Preface

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

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

Conventions

The following text conventions are used in this document:

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

1 Introduction

This document provides information on how to configure the Oracle Communications Cloud Native Core Binding Support Function (BSF).

1.1 Overview

Binding Support Function (BSF) provides a Policy Control Function (PCF) session binding functionality and ensures an Application Function request for a certain PCF session that reaches the relevant Binding Support Function (BSF) holding the PCF Session information.

> **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.

BSF supports the following functions:

- Allows BSF users to register, discover, and remove the binding information
- Allows network function consumers to retrieve the binding information

CNC BSF Availability

Oracle Communications Cloud Native Core (CNC) BSF availability is dependent on many factors. BSF applications are designed to achieve 99.999% availability, according to the applicable Telecommunications Industry Association TL9000 standards, with the following deployment requirements:

- Deploy on a Cloud Native Environment with at least 99.999% Availability.
- Deploy with n + k application redundancy, where k is greater than or equal to one.
- Maintain production software within n-2 software releases, where n is the current general availability release.

> **Note**
>
> BSF 25.1.100 supports upgrade from 24.3.x, 24.2.x, and 23.4.6.
>
> Also, 25.1.100 can be rolled back to 24.3.x, 24.2.x, 23.4.6.

- Apply bug fixes, critical patches, and configuration recommendations provided by Oracle promptly.
- Maintain disaster recovery procedures external to the applications for the reconstruction of lost or altered files, data, programs, or Cloud Native environment.
- Install, configure, operate, and maintain CNC BSF as per Oracle's applicable installation, operation, administration, and maintenance specifications.

- Maintain an active support contract and provide access to the deployed CNC BSF and your personnel to assist Oracle in addressing any outage.

CNC BSF availability is measured for each calendar year and is calculated as follows:

Table 1-1 Measuring CNC BSF Availability

Availability	Description
Planned Product Availability	(Product available time in each month) less (**Excluded Time** (defined below) in each month).
Actual Product Availability	(Planned Product Availability) less (any Unscheduled Outage)
Product Availability Level	(Actual Product Availability across all Production instances divided by Planned Product Availability across all Production instances) x 100

> **Note**
>
> **Excluded Time** means:
>
> - Scheduled maintenance time.
> - Lack of power or backhaul connectivity, except to the extent that such lack of backhaul connectivity was caused directly by the CNC NF.
> - Hardware failure.
> - Issues arising out of configuration errors or omissions.
> - Failures caused by third-party equipment or software not provided by Oracle.
> - Occurrence of any event under Force Majeure.
> - Any time associated with failure to maintain the recommended architecture and redundancy model requirements above.

1.2 References

Following are the reference documents:

- *Oracle Communications Cloud Native Binding Support Function Installation and Upgrade Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function Network Impact Report Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function Network Impact Report Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function Troubleshooting Guide*

2
BSF Architecture

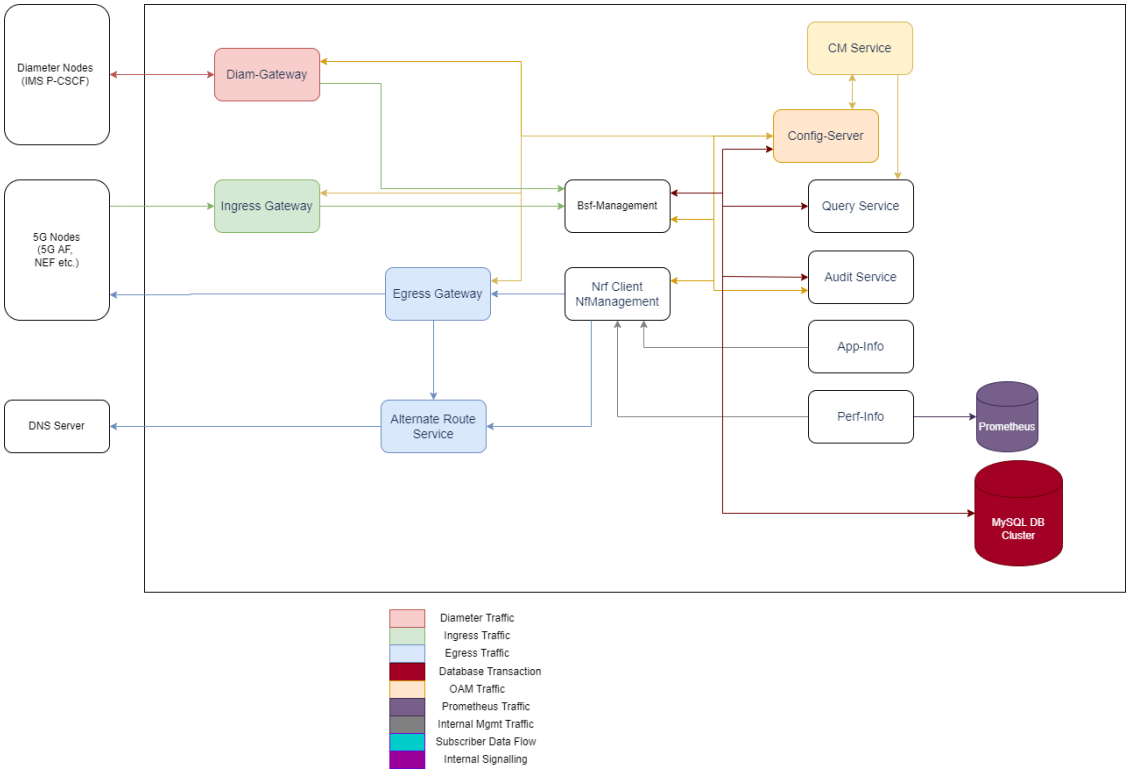
This section provides information about Oracle Communications Cloud Native Core Binding Support Function (BSF) Architecture.

2.1 BSF Architecture

The BSF network function is a cloud native application that consists of multiple microservices running in cloud native environment.

The following figure describes the component level architecture of BSF:

Figure 2-1 Architecture of Binding Support Function



The microservices are logically categorized as following categories:

- **Connectivity**: It includes external entities that interact with BSF and vice-versa.
- **Adaptation & Mobility**: Components under this category provide an interface that ensures seamless interaction between external and internal entities. It contains the following components:
  - **Diameter Gateway**: Acts as a Gateway for all diameter traffic to BSF.
  - **Ingress Gateway**: Acts as a gateway for all incoming Ingress HTTP traffic.

  - **Egress Gateway**: Acts as a gateway for all outgoing Egress HTTP traffic.
  - **Alternate Route Service**: Provides alternate routing destinations for BSF (NRF-management) to re-route during failures. There are two options for alternate routing:
    1. DNS (SRV) based routing - A DNS server is required to resolve SRV records having alternate destinations with higher priority.
    2. Static routing - Static configuration for alternate destinations with weight or priority.
- **Business Logic**: Components under this category can be enabled based on deployment needs. It includes the following components:
  - **Bsf-Management**: It implements the nbsf interface as defined in 3GPP Specification 29.521.
  - **Nrf-Management**: It helps in the autonomous discovery of network functions.
- **Operations & Maintenance**: Components under this category perform specific tasks as follows:
  - **Config-Mgmt**: It provides GUI and REST OAM interfaces for service provisioning.
  - **Config Server**: It abstracts the database for storage and retrieval of configuration.
  - **Query**: It processes session viewer queries triggered from config management service.
  - **App-Info**: It monitors application (microservice) health and status.
  - **Perf-Info**: It monitors application (microservice) capacity and load status.
  - **Audit-service**: It runs the Audit engine to detect and process stale session records. Also, Audit-service counts the maximum number of active sessions for a particular service.
- **Data Management**: Components under this category are responsible for storing various types of persistent data.
- **Ingress and Egress Gateway Traffic Management**
  For more information on Ingress and Egress Gateway Traffic Management, see *Oracle Communications Cloud Native Environment User Guide.*

3
BSF Features

This section describes the key features of Oracle Communications Cloud Native Core, Binding Support Function (BSF).

3.1 Stale Binding Detection Audit, Report and Recover

Service disruption due to network storm, system overload, database latency, and other events can impact signaling between PCF and BSF. This service disruption can affect session binding between PCF and BSF.

BSF supports to revalidate the binding information of a PDU session and checks if there is any missing binding information in BSF due to service disruption between PCF and BSF.

When BSF receives a binding session revalidation request from PCF, BSF processes the request, determines if the session is available in BSF. Existence of the binding association for the PDU session in BSF confirms the binding association being valid in BSF. If the binding association is missing in BSF, it is restored by creating the association in BSF.

When the session binding revalidation is enabled in BSF

When BSF receives a PDU session binding revalidation request from PCF through Diameter Gateway:

- BSF checks if session binding revalidation is enabled in BSF and the revalidation request includes `x-oc-binding-revalidation` header.

  > **Note**
  >
  > Session binding revalidation can be enabled in BSF, either using **Enable Binding Revalidation** field in **Management Service** page on CNC Console or using `enableBindingRevalidation` parameter in BSF Management Service API. For more details, see Management Service.

- If BSF identifies that the revalidation request is a colliding or a duplicate request, and the if the following parameters in the request matches with the stored binding object in BSF:
  - SUPI/GPSI
  - UE IP(IPV4/IPV6),
  - IPDomain(if IPV4 was present for UE IP)
  - dnn
  - snssai
  - diamHost/fqdn
  - pcfFqdn

  A binding revalidation request is considered as a duplicate request if the request is for the same subscriber (SUPI, DNN, SNSSAI, IPV4/IPv6 prefix, or IpDomain) from same PCF instances (ID/pcfDiamHost/pcfFqdn or pcfIpEndPoints). If the parameters in the request

matches with the stored binding object in BSF, BSF responds to PCF with the given `binding_id` and does not perform any database update.

- If the parameters do not match, or if it is not a duplicate request, BSF creates the binding record and responds to PCF with a 201 response to PCF including a location HTTP header field that contains the URI of the created binding information.
  Example:

  {apiRoot}/oc-bsf-configuration/v1/services/managementservice/{bindingId}

  where, {bindingId} is the new binding identifier for the session.

When the session binding revalidation is enabled in BSF

If the session binding revalidation is enabled in BSF, when BSF receives a PDU session revalidation request from PCF, BSF checks if the binding information exists in BSF. If the record created by the same PCF already exists, BSF deletes the existing record and creates a new record for the PDU session.

When BSF receives a PDU session revalidation request from PCF:

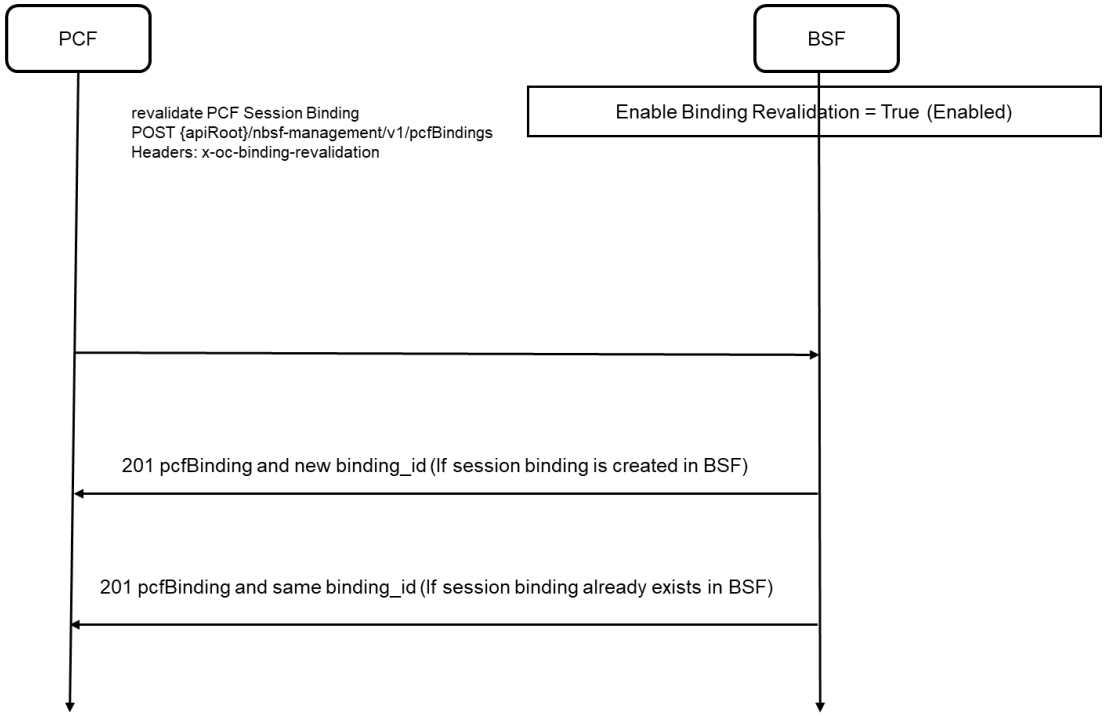
- BSF verifies if the parameters for late arrival handling is configured.
- If the request has not arrived late, BSF checks if **Enable Collision Detection** field is enabled.

  If the parameters in the request do not match with the stored binding information in BSF, BSF creates the binding record for the pcdId and responds to PCF with 201 response code with a new binding_id.

Call Flow

The following diagram depicts a sample call flow for revalidating the binding information for a PDU session in BSF when the binding revalidation is enabled in BSF and the revalidation request includes `x-oc-binding-revalidation` header:

Figure 3-1 Binding revalidation in BSF



1. BSF receives a binding revalidation request for a PDU session from PCF.
2. BSF checks if the session binding revalidation is enabled in BSF and the revalidation request includes `x-oc-binding-revalidation` header.
3. If the revalidation request is a duplicate or a colliding request and if the binding information for the PDU session already exists in BSF, BSF sends a 201 response code with the existing `binding_id`.
4. If the binding information stored in BSF differs from the details received in the request or if the binding information for the PDU session does not exist in BSF, BSF recreates the session biding record (re-registers) for the PDU session. BSF sends a 201 response code with the new `binding_id`.

Managing Stale Binding Detection Audit, Report and Recover

Enable

This feature can be eanbled using CNC Console for BSF as well as using REST API.

Enable using CNC Console

To enable this feature using CNC Console for BSF, configure **Enable Binding Revalidation** field on **Management Service** page under **Service Configurations** in CNC Console for BSF.

For more information, see Management Service.

Enable using REST API

To enable this feature using REST API, configure the `EnableBindingrevalidate` parameter under Management Service API for BSF: `{apiRoot}/oc-bsf-configuration/v1/services/managementservice`.

For more information, see *Management Service* section in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*.

Observability

Metrics

The following BSF Management service metrics are used to monitor this feature in BSF:

- ocbsf_binding_revalidation_request_total
- ocbsf_binding_revalidation_response_total
- ocbsf_binding_revalidation_pcfBinding_missing_total

For more information, see BSF Management Service.

Alerts

The following BSF alerts are used for this feature:

- BINDING_REVALIDATION_PCF_BINDING_MISSING_MINOR
- BINDING_REVALIDATION_PCF_BINDING_MISSING_MAJOR
- BINDING_REVALIDATION_PCF_BINDING_MISSING_CRITICAL

For more information, see List of Alerts.

Logging

The following logs with a specific marker "marker":{"name":"BINDING"}, "Binding Audit:<additional log text>" are generated for this feature:

- For Revalidation request, if the binding association is not present in BSF, BSF updates its logs with the failure for the revalidation request. The updated logs include:
  - SUPI
  - DNN
  - S-NSSAI
  - UE-IP (IPv6/IPV4)
  - IPDomain if available
  - PCF FQDN
  - error code and cause at “WARN” level
- For Revalidation request, if BSF can not reestablish or restore the BSF binding after all session retries, BSF updates its logs with the failure for the restoration request.
  - SUPI
  - DNN
  - S-NSSAI
  - UE-IP (IPv6/IPV4)
  - IPDomain if available
  - PCF FQDN
  - error code and cause at “WARN” level

3.2 Traffic Segregation

This feature provides end-to-end traffic segregation to BSF based on traffic types. Within a Kubernetes cluster, traffic segregation can divide applications or workloads into distinct sections such as OAM, SBI, Kubernetes control traffic, etc. The Multus CNI container network interface (CNI) plugin for Kubernetes enables attaching multiple network interfaces to pods to help segregate traffic from each BSF microservice.

This feature addresses the challenge of logically separating IP traffic of different profiles, which are typically handled through a single network (Kubernetes overlay). The new functionality ensures that critical networks are not cross-connected or sharing the same routes, thereby preventing network congestion.

With traffic segregation, operators can segregate traffic to external feeds and applications more effectively. Previously, all external traffic was routed through the same external network, but now, egress traffic from the BSF pods can be directed through non-default networks to third-party applications. This separation is achieved by leveraging cloud-native infrastructure and the load balancing algorithms in CNE.

The feature supports the configuration of separate networks, Network Attachment Definitions (NADs), and the Cloud Native Load Balancer (CNLB). These configurations are crucial for enabling cloud native load balancing, facilitating ingress-egress traffic separation, and optimizing load distribution within BSF.

Prerequisites

The CNLB feature is only available in BSF if CNE is installed with CNLB and Multus.

Cloud Native Load Balancer (CNLB)

CNE provides Cloud Native Load Balancer (CNLB) for managing the ingress and egress network as an alternate to the existing LBVM, lb-controller, and egress-controller solutions. You can enable or disable this feature only during a fresh CNE installation. When this feature is enabled, CNE automatically uses CNLB to control ingress traffic. To manage the egress traffic, you must preconfigure the egress network details in the `cnlb.ini` file before installing CNE.

> **Note**
>
> CNLB is supported only for IPv4 stack.

For more information about enabling and configuring CNLB, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*, and *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

Network Attachment Definitions for CNLB

A Network Attachment Definition (NAD) is a resource used to set up a network attachment, in this case, a secondary network interface to a pod. BSF supports two types of CNLB NADs:

1. **Ingress Network Attachment Definitions**
   Ingress NADs are used to handle inbound traffic only. This traffic enters the CNLB application through an external interface service IP address and is routed internally using interfaces within CNLB networks.
   - **Naming Convention:**`nf-<service_network_name>-int`

2. **Egress Only Network Attachment Definitions**
   Egress Only NADs enable outbound traffic only. An NF pod can initiate traffic and route it through a CNLB application, translating the source IP address to an external egress IP address. An egress NAD contains network information to create interfaces for NF pods and routes to external subnets.
   - **Requirements:** Destination (egress) subnet addresses are known beforehand and defined under the `cnlb.ini` file's `egress_dest` variable to generate NADs.
   - **Naming Convention:**`nf-<service_network_name>-egr`
3. **Ingress/Egress Network Attachment Definitions**
   Ingress/Egress Network Attachment Definitions enable inbound/outbound traffic. An NF pod can initiate traffic and route it through a CNLB app, translating source IP address to an external egress IP address (defined under **cnlb.ini** file **egress_addr** variable). An Ingress/Egress Network Attachment Definition contains network information to create interfaces for NF pods and routes to external subnets. Even though an Ingress/Egress Network Attachment Definition enables outbound traffic, it also handles inbound traffic, so if inbound/outbound traffic is needed an Ingress/Egress Network Attachment Definition should be used.
   - **Requirements:** Source (ingress) and destination (egress) subnet addresses are known beforehand and defined under **cnlb.ini** file **egress_dest** variable to generate Network Attachment Definitions.
   - **Naming Convention:**`nf-<service_network_name>-ie`

Managing Ingress and Egress Traffic Segregation

Enable:

This feature is disabled by default. To enable this feature, you must configure the network attachment annotations in the custom values file.

Configuration

For more information about Traffic Segregation configuration, see " Configuring Traffic Segregation" section in *Oracle Communications Cloud Native Core, Converged Binding Support Function Installation, Upgrade, and Fault Recovery Guide.*.

Observe

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

Maintain

To resolve any alerts at the system or application level, see BSF Alerts section. If the alerts persist, perform the following:

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

3.3 Logging Support for Error Response

Error handling framework was introduced in earlier release of BSF as a general purpose error handling tool. This feature used the error handling framework to add more details to the error using 3GPP error response format.

BSF sends error responses to consumer NFs due to some exceptions, such as signaling, validations, and internal errors. These error responses have payloads containing the problem title, status, details, and cause of the error that are used to investigate the error. BSF has been enhanced to support logs for the error responses.

When sending any error response triggered by an HTTP Request, this error response format will be mapped into the following *general log format*:

```
{
  “errorStatus”: “Value”, (ProblemDetails status field)
  “errorTitle”: “Value”, (ProblemDetails title field)
  “errorDetails”: “Value”, (ProblemDetails detail field)
  “errorCause”: “Value”  (ProblemDetails cause field)
  “sender”: “Value”, (nfType-nfInstanceId)
  “subscriberId”: “Value” (UE ID associated with event if present)
}
```

Table 3-1 General Log Format

Parameter	Description	Example
errorStatus	Specifies the status code of the error.	404, 500, etc.
errorTitle	Specifies the title of the error.	Required parameter in binding data is missing
errorDetails	Specifies the error detail produced by error handling framework in case of BSF as producer. **Note:** For errorDetails field to be populated in the required format, error handling framework should be enabled in CNC Console for the required service.	`ocbsf1-2-api-gateway.bsf1-2.svc.atlantic.morrisville.us.lab.oracle.com:BSF_MGMT:Mandatory parameter is missing in request :EC-OBSF-BSF_MGMT-REQVLD-EI-05-02-400-00010-01-02`
errorCause	Specifies the cause of the error.	MANDATORY_IE_MISSING
sender	Specifies the sender which is composed by the nfType plus the instanceId. **Note:** In case of BSF as producer of error, the sender field will be BSF plus the instanceId of the BSF.	BSF-fe7d992b-0541-4c7d-ab84-c6d70b1b0666
subscriberId	Specifies the subscriberId which can be SUPI or GPSI associated with the event.	`imsi-65008100001061`

In the case of subscriberID, if UE identifier is present and shows UE identifier flag as *enabled*, the logging happens in the following hierarchy:

1. If SUPI and GPSI both are present, use SUPI.
2. If SUPI is not present, and GPSI is present, use GPSI.

> **Note**
>
> Sender-contains the *nfType-instanceId*from the sender of the HTTP Request. Where *nfType* is a value which contains the type of Network Function set as *BSF* by default, and *nfInstanceId*is a unique identifier for a specific instance of a Network Function. This value is set in the application configuration for BSF

Managing Enhancements to Logging Support for Error Response

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

Enable

By default, this feature is disabled. The operator can enable this feature through the CNC Console configurations.

> **Note**
>
> Oracle does not recommend enabling this feature. When this feature is enabled, sensitive information in the form of UE identifier gets published. Users can secure the logs in their environment using appropriate configuration.

Configure

You can configure logging support for error response using the **Enable Enhanced Logging** and **Enable UE Identifier Information** toggle buttons. These toggle buttons are availabe in **General Settings** under **General Configurations** on CNC Console for BSF. For information about how to configure for BSF Management Service in CNC Console, see General Settings.

Observe

There are no new metrics in BSF Management Service for this feature.

3.4 Support for TLS

BSF uses Hypertext Transfer Protocol Secure (HTTPS) and Diameter Gateway to establish secured connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS).

TLS comprises the following components:

- **Handshake Protocol:** Exchanges the security parameters of a connection.
- **Record Protocol:** Receives the messages to be transmitted, fragments the data into multiple blocks, secures the records, and then transmits the result. Received data is delivered to higher-level peers.

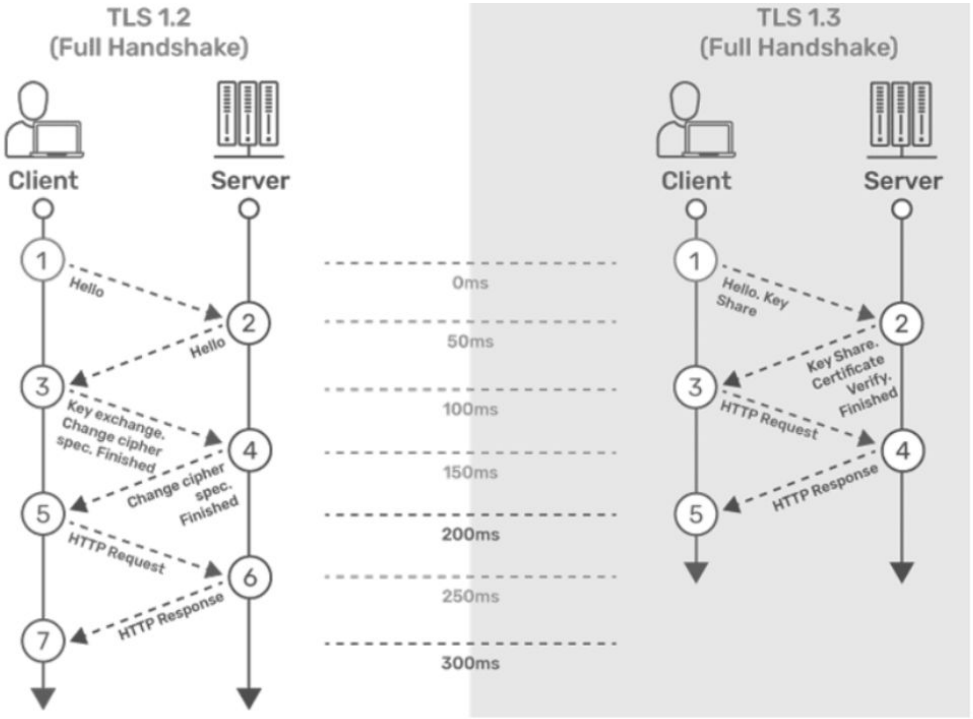
This feature enables the support for TLS 1.3 to all consumer NFs, producer NFs, the Data Director, SBI Interfaces, and any interfaces previously supporting TLS 1.2. Support for TLS 1.2 will remain available.

> **Note**
>
> If both TLS 1.2 and TLS 1.3 are supported, TLS 1.3 is given priority.

TLS 1.2 and TLS 1.3 Handshake

This section describes the differences between TLS 1.3 and TLS 1.2, as well as the advantages of TLS 1.3 over TLS 1.2 and earlier versions.

Figure 3-2 TLS 1.2 and TLS 1.3 Handshake



TLS 1.2

Step 1: The connection or handshake starts when the client sends a "client hello" message to the server. This message consists of cryptographic information such as supported protocols and cipher suites. It also contains a random value or random byte string.

Step 2: To respond to the "client hello" message, the server sends a 'server hello' message. This message contains the CipherSuite that the server has selected from the options provided by the client. The server also sends its certificate, along with the session ID and another random value.

Step 3: The client verifies the certificate sent by the server. When the verification is complete, it sends a byte string encrypted using the public key of the server's certificate.

Step 4: When the server receives the secret, both the client and server generate a master key along with session keys (ephemeral keys). These session keys are used for symmetrically encrypting the data.

Step 5: The client sends an "HTTP Request" message to the server to enable the server to transition to symmetric encryption using the session keys.

Step 6: To respond to the client's "HTTP Request" message, the server does the same and switches its security state to symmetric encryption. The server concludes the handshake by sending an HTTP response.

Step 7: The client-server handshake is completed in two round trips.

TLS 1.3
Step 1: The connection or handshake begins when the client sends a "client hello" message to the server, which includes the list of supported cipher suites and the client's key share for the specific key agreement protocol.

Step 2: To respond to the "client hello" message, the server sends the key agreement protocol that it has chosen. The "Server Hello" message includes the server key share, server certificate, and the "Server Finished" message.

Step 3: The client verifies the server certificate, generates keys since it has the server's key share, and then sends the "Client Finished" message along with an HTTP request.

Step 4: The server completes the handshake by sending an HTTP response.

> **Note**
>
> ASM and TLS are not supported together.

The following table provides comparison of TLS 1.2 with TLS 1.3:

Table 3-2 Comparison of TLS 1.2 with TLS 1.3

Feature	TLS 1.2	TLS 1.3
TLS Handshake	This is less efficient as it requires more round-trips to complete the handshake process.	This is more efficient as it requires less round-trips to complete the handshake process.
Cipher Suites	This has less secured Cipher Suites.	This has more secured Cipher Suites. They support the following ciphers: • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_AES_128_CCM_8_SHA256: This Cipher is not supported by Java library. • TLS_AES_128_CCM_SHA256: This Cipher is not supported by Java library.
Round-Trip Time (RTT)	This has higher RTT during TLS handshake.	This has low RTT.
Performance	This has higher latency during TLS handshake.	This has low latency during TLS handshake.

Note

- BSF does not prioritize cipher suites on the basis of priorities. To select cipher on the basis of priorities, you must write the cipher suites in the decreasing order of priority.
- BSF does not prioritize supported groups on the basis of priorities. To select supported group on the basis of priorities, you must write the supported group values in the decreasing order of priority.
- If you want to provide values for the signature_algorithms extension using the `clientSignatureSchemes` parameter, the following comma-separated values must be provided to deploy the pods:
  - rsa_pkcs1_sha512
  - rsa_pkcs1_sha384
  - rsa_pkcs1_sha256
- The mandatory extensions as listed in RFC 8446 cannot be disabled on the client or server side. The following is the list of the extensions that cannot be disabled:
  - supported_versions
  - key_share
  - supported_groups
  - signature_algorithms
  - pre_shared_key

The following digital signature algorithms of TLS 1.2 and TLS 1.3 are supported in TLS handshake:

Table 3-3 Digital Signature Algorithms

Algorithm	Key Size (Bits)	Elliptic Curve (EC)
RS256 (RSA)	2048	NA
	4096 This is the recommended value.	NA
ES256 (ECDSA)	NA	SECP384r1 This is the recommended value.

Note

The following functionalities from TLS 1.3 specifications are not supported:

- Zero round-trip time (0-RTT) mode.
- Pre-Shared Key (PSK) exchange.

3.4.1 Support for TLS Using HTTPs

BSF uses Hypertext Transfer Protocol Secure (HTTPS) to establish secured connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS).

Enable

This feature is enabled by default at the time of Gateway Services deployment by completing the required Helm configurations.

Configure

You can configure this feature using Helm. For information about Helm configurations, see "Global Parameters" in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Observe

The following metrics are available for this feature:

- oc_ingressgateway_incoming_tls_connections
- oc_egressgateway_outgoing_tls_connections
- security_cert_x509_expiration_seconds

For more information about metrics, see TLS Metrics section.

The following alerts are available for this feature:

- CERTIFICATE_EXPIRY
- BSF_CONNECTION_FAILURE

For more information about alerts, see Configuring BSF Alerts section.

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

In case the alert still persists, perform the following:

1. **Collect the logs and Troubleshooting Scenarios**: For more information on how to collect logs and troubleshooting information, see *Oracle Communications Cloud Native Core, Binding Support Function Troubleshooting Guide*.
2. **Raise a service request**: See My Oracle Support for more information on how to raise a service request.

3.4.2 Support for TLS in Diameter Gateway

BSF uses Diameter Gateway to establish secured connections with consumer NFs and producer NFs, respectively. These communication protocols are encrypted using Transport Layer Security (TLS).

Enable

This feature is disabled by default. It can be enabled using `TLS_ENABLED` parameter using Helm configurations. For information about Helm configurations, see "Global Parameters" in

Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide.

Configure

You can configure this feature using Helm. For information about Helm configurations, see "Global Parameters" in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Peer level support for TLS versions can be configured using CNC Console. For more information, see Peer Nodes section.

Observe

The following metrics are available for this feature:

- diam_conn_network
- diam_failed_conn_network
- diam_conn_network_responder
- dgw_tls_cert_expiration_seconds

For more information about metrics, see TLS Metrics section.

The following alerts are available for this feature:

- DGW_TLS_CONNECTION_FAILURE
- DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR
- DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR
- DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

For more information about alerts, see Configuring BSF Alerts section.

Following extensions are available for TLS in Diameter Gateway:

- status_request (0x0005)
- status_request_v2 (0x0011)
- supported_groups (0x000A)
- ec_point_formats (0x000B)
- extended_master_secret (0x0017)
- session_ticket (0x0023)
- signature_algorithms (0x000D)
- signature_algorithms_cert (0x0032)
- supported_versions (0x002B)
- psk_key_exchange_modes (0x002D)
- key_share (0x0033)
- renegotiation_info (0xFF01)

Maintain

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

In case the alert still persists, perform the following:

1. **Collect the logs and Troubleshooting Scenarios**: For more information on how to collect logs and troubleshooting information, see *Oracle Communications Cloud Native Core, Binding Support Function Troubleshooting Guide*.
2. **Raise a service request**: See My Oracle Support for more information on how to raise a service request.

3.5 Enhancements to Error Response

BSF sends error responses to consumer NFs due to some exceptions, such as signaling, validations, and internal errors. These error responses have payloads containing the problem title, status, details, and cause of the error that are used to investigate the error. The details section is now enhanced with application error IDs.

The error handling module gives provision to configure the error response dynamically and the same is responded when BSF is producer of the call flow.

With the enhanced error response mechanism, BSF sends additional information such as server FQDN, micro-service ID, error category, and application error ID in the `detail` attribute of the `ProblemDetails`. This enhancement provides more information about the error and troubleshoot them.

Application error ID follows the below format.

[EC] [NF ID] [Microservice ID] [Category] [Error ID]

An error code dictionary will be provided to identify the cause and possible solution of the error. For more details of the error code dictionaries for BSF management service, Egress Gateway, Ingress Gateway, and NRF Client, see Error Code Dictionary .

Managing Enhancements to Error Response

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

Enable

By default, this feature is disabled. The operator can enable this feature through the CNC Console configurations.

Configure

You can configure error handling functionality under **Error Handling** on CNC Console for BSF. For information about how to configure for BSF Management Service in CNC Console, see Error Configurations .

Observe

The following metrics have been added in BSF Management Service for this feature:

- error_handler_exec_total
- error_handler_in_total
- error_handler_out_total

For more information, see BSF Management Service.

3.6 Validating Destination-Realm Attribute-Value Pair (AVP) Received in AAR-I Message

The destination-realm Attribute-Value Pair (AVP) received in the AAR-I message from an AF must be validated at the BSF Diameter Gateway before processing and forwarding the AAR-I message to a corresponding PCF instance.

> **Note**
>
> This validation applies exclusively to the AAR-I message within the BSF. For subsequent AAR-U and STR messages, it is assumed that the AF will send the correct Destination-Host and the destination-realm Attribute-Value Pair (AVP) values based on the AAA response received.

Figure 3-3 Diameter Gateway for BSF

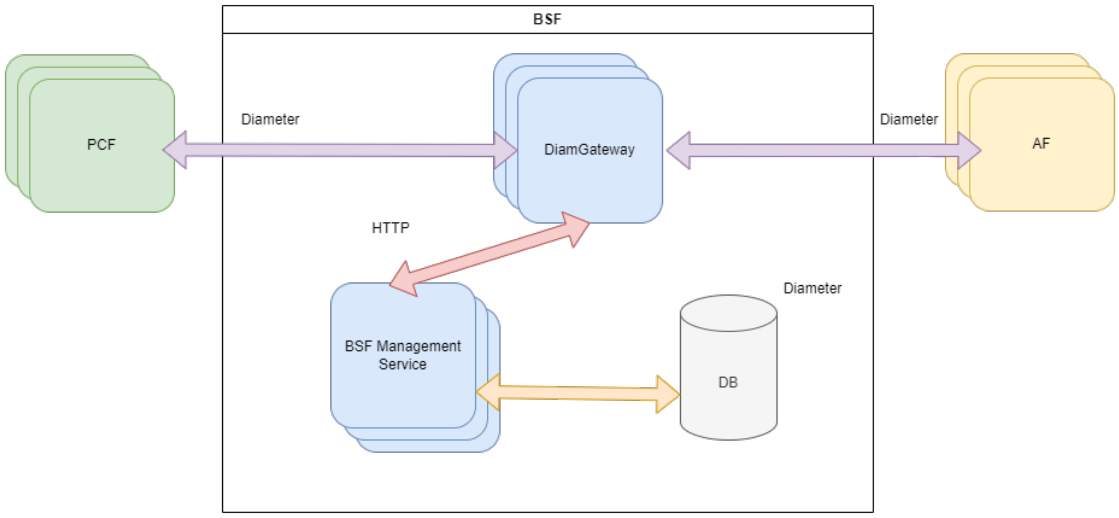
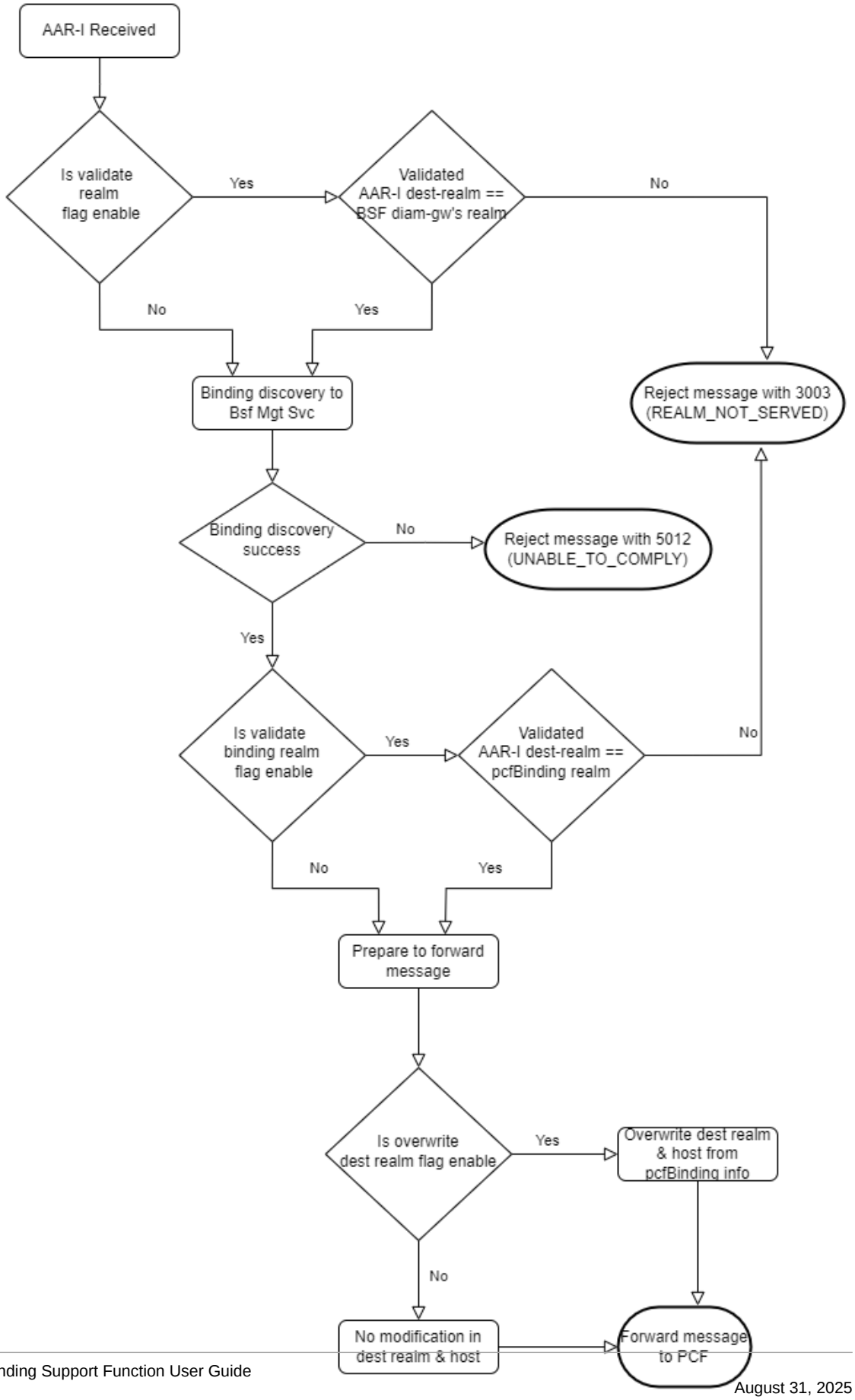


Figure 3-4 destination-realm Validation Process



1. When Diameter Gateway receives an AAR-I message from an AF, it checks if the validation realm flag is enabled.
2. If the validation realm flag is enabled, it validates the destination-realm AVP received in the AAR-I message against the BSF Diameter Gateway realm.

   If the validation is successful, it proceeds with the message processing and the Diameter Gateway sends a Binding Discovery message to BSF Management Service.

   If the validation fails, the Diameter Gateway rejects the AAR-I message with error code 3003 (REALM_NOT_SERVED).

   > **Note**
   >
   > The Diameter Gateway error code configuration for BSF is applicable and the default result code 3003 can be modified to any other error codes.

3. If the validation realm flag is disabled, the Diameter Gateway sends a Binding Discovery message to BSF Management Service without validating the destination-realm AVP.
4. After receiving a successful response to Binding Discovery request from BSF Management service, the Diameter Gateway checks if the validate binding realm flag is enabled.

   If the validate binding realm flag is enabled, the Diameter Gateway validates the destination-realm against the pcfBinding realm.

   If the validation is successful, the Diameter Gateway forwards the message for further processing.

   If the validation fails, the Diameter Gateway rejects the AAR-I message with error code 3003 (REALM_NOT_SERVED).

   If the validate binding flag is disabled, the Diameter Gateway forwards the message for further processing without validating the destination-realm against the pcfBinding info.
5. If the Binding Discovery request fails, the Diamter Gateway rejects the AAR-I message with error code 5012 (UNABLE_TO_COMPLY).
6. After the successful validation of the destination-realm against pcfBinding info, the Diameter Gateway checks if overwrite diam-realm flag is enabled. If this flag is enabled, it overwrites the destination-realm received in the AAR-I message with the pcfBinding info received in the binding discovery response.

   > **Note**
   >
   > If Overwrite Realm configuration is enabled, the diam_response_network metric for AAA message will show the new realm that was overwritten as the 'reqDestRealm', and not the original realm that was sent in the AAR message.

7. If overwrite diam-realm flag is disabled, there is no modification made to the destination-realm.
8. The message is forwarded to PCF.

> **Note**
>
> Fake AVP validation will not be performed if routing table is configured. That is, if the above mentioned fake AVP parameters are configured and the routing tables are also configured, AVP validation will not be performed. The call will be processed as per the routing table configuration.

Managing Validation of destination-realm in AAR-I Message

The following Advanced Settings for Diameter Gateway are used to enable and validate the destination-realm in AAR-I message:

- DIAMETER.Enable.Validate.Realm
- DIAMETER.BSF.Enable.Validate.Binding.Realm
- DIAMETER.BSF.Enable.Overwrite.Realm

For more details on the above mentioned advanced settings keys, see Settings.

Observability

Metrics

ocbsf_diam_realm_validation_failed_total metric is used to count the number of failed destination-realm validation at Diameter Gateway for BSF. For more details, see Diameter Gateway Metrics.

Alerts

The following alerts are used for Validating destination-realm Received in AAR-I Message feature:

- DIAM_RESPONSE_REALM_VALIDATION_ERROR_MINOR
- DIAM_RESPONSE_REALM_VALIDATION_ERROR_MAJOR
- DIAM_RESPONSE_REALM_VALIDATION_ERROR_CRITICAL

3.7 Support for Automated Certificate Lifecycle Management

Public Key Interface (PKI) is the set of elements such as public/private keys, certificate signing request, and certificates that are required to handle secure communications and transactions. BSF uses secure protocols for its communications, such as HTTPS and Secure Socket Layer (SSL) / Transport Layer Security (TLS) technologies to handle these secure communications. This is achieved with the use of Public and Private Keys, and the presence of trusted authorities, also known as Certificate Authorities (CA), which create and issue certificates. These certificates have a determined validity period. These certificates must be renewed before expiry. They can also be revoked when the CA or its keys are compromised. These certificates must be recreated when required.

This feature enables BSF to support automation of certificate lifecycle management in integration with Oracle Communications Cloud Native Core, Certificate Manager (OCCM).

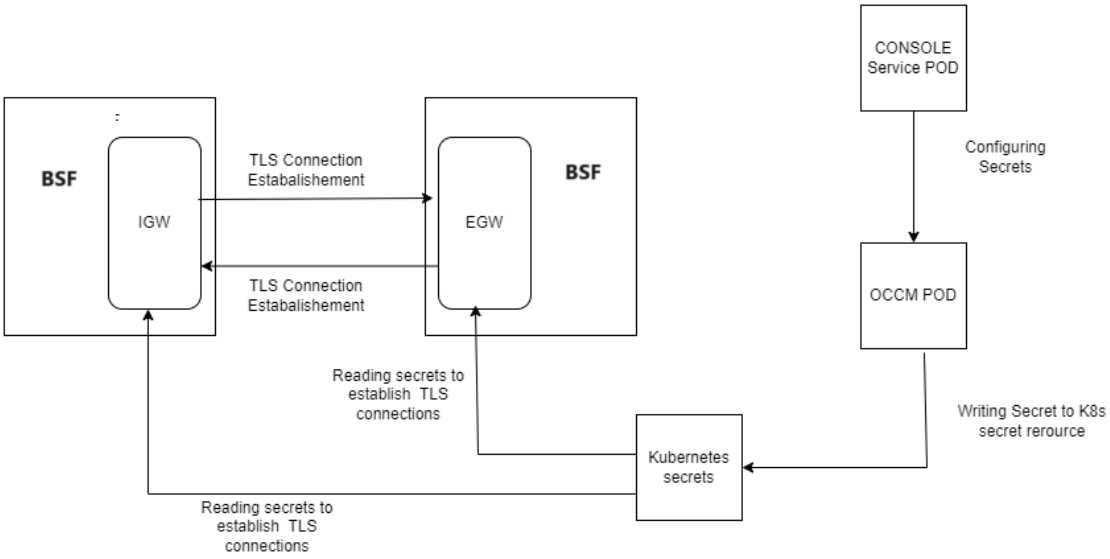
OCCM provides the option to automatically create, renew, and delete certificates for a given CA, with the possibility to track previously created certificates and renew/delete them when required.

The certificate lifecycle management includes:

- Certificate Creation,
- Certificate Deletion,
- Certificate Monitoring (including the ones that were created using a different tool from OCCM),
- Certificate Renewal.

> **Note**
>
> OCCM does not support OAuth token generation and distribution (currently handled by NRF) used for SBI signalling.

Figure 3-5 BSF Integration with OCCM



There is no direct communication between OCCM and BSF. All the communications are handled using Kubernetes Secrets.

All the required certificates are configured using OCCM.

After OCCM creates these Kubernetes Secrets, or monitors the already existing ones, the Ingress and Egress Gateways monitor these Secrets and keep track of their current status:

- **VALID**: A Kubernetes Secret which holds a certificate that has not expired and it is properly signed
- **EXPIRED**: A Kubernetes Secret which holds a certificate that has met its expiration date (the value determined in its `notAfter` value)
- **MISSING**: A Kubernetes Secret which has its certificate missing, or any other essential file for the TLS/SSL bundle
- **CORRUPT**: A Kubernetes Secret which has its certificate corrupt, either invalid file, invalid signature, or invalid format

Managing the keys and certificates

Install Guide Considerations

- Upgrade: When BSF is deployed with OCCM, follow the specific upgrade sequence as mentioned in the *Oracle Communications, Cloud Native Core Solution Upgrade Guide*.
- Rollback: You can remove Kubernetes secrets if the current version of BSF does not use that secret by checking the `ocbsf_custom_values.yaml` file. Before deleting, please make sure that there is no plan to rollback to the BSF version which uses these secrets. Otherwise Rollback will fail. For more information on migrating the secrets from BSF to OCCM and removal of Kubernetes secrets from the yaml file, see *Upgrade Strategy* in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Configure

To configure HTTPS in ingress-gateway, the following parameters must be configured in custom-value.yaml file in the ingress-gateway section:

- ingress-gateway.enableIncomingHttps
- ingress-gateway.service.ssl.privateKey.k8SecretName
- ingress-gateway.service.ssl.privateKey.k8NameSpace
- ingress-gateway.service.ssl.privateKey.rsa.fileName
- ingress-gateway.service.ssl.certificate.k8SecretName
- ingress-gateway.service.ssl.certificate.k8NameSpace
- ingress-gateway.service.ssl.certificate.rsa.fileName
- ingress-gateway.service.ssl.caBundle.k8SecretName
- ingress-gateway.service.ssl.caBundle.k8NameSpace
- ingress-gateway.service.ssl.caBundle.fileName
- ingress-gateway.service.ssl.keyStorePassword.k8SecretName
- ingress-gateway.service.ssl.keyStorePassword.k8NameSpace
- ingress-gateway.service.ssl.keyStorePassword.fileName
- ingress-gateway.service.ssl.trustStorePassword.k8SecretName
- ingress-gateway.service.ssl.trustStorePassword.k8NameSpace
- ingress-gateway.service.ssl.trustStorePassword.fileName

For more information, see *Basic Configurations in Ingress Gateway* section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

To configure HTTPS in egress-gateway, configure the following parameters under *egress-gateway* section in *custom-value.yaml* file:

- egress-gateway.enableOutgoingHttps
- egress-gateway.egressGwCertReloadEnabled
- egress-gateway.egressGwCertReloadPath
- egress-gateway.service.ssl.privateKey.k8SecretName
- egress-gateway.service.ssl.privateKey.k8NameSpace

- egress-gateway.service.ssl.privateKey.rsa.fileName
- egress-gateway.service.ssl.privateKey.ecdsa.fileName
- egress-gateway.service.ssl.certificate.k8SecretName
- egress-gateway.service.ssl.certificate.k8NameSpace
- egress-gateway.service.ssl.certificate.rsa.fileName
- egress-gateway.service.ssl.certificate.ecdsa.fileName
- egress-gateway.service.ssl.caBundle.k8SecretName
- egress-gateway.service.ssl.caBundle.k8NameSpace
- egress-gateway.service.ssl.caBundle.fileName
- egress-gateway.service.ssl.keyStorePassword.k8SecretName
- egress-gateway.service.ssl.keyStorePassword.k8NameSpace
- egress-gateway.service.ssl.keyStorePassword.fileName
- egress-gateway.service.ssl.trustStorePassword.k8SecretName
- egress-gateway.service.ssl.trustStorePassword.k8NameSpace
- egress-gateway.service.ssl.trustStorePassword.fileName

For more information, see *Basic Configurations in Egress Gateway* section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Observability

Monitoring the keys and certificates

BSF supports monitoring and automatic renewal of its' TLS certificates in integration with OCCM.

It is validated that the renewed certificate and key are picked up for any new TLS connections.

Also, the existing TLS connections using the previous key and certificate are gracefully brought down.

Clean up of the certificates are also handled through OCCM.

For information about enabling HTTPS, see *Configuring Secrets for Enabling HTTPS* in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

.

Metrics

The oc_certificatemanagement_tls_certificate_info metric is used to support automated certificate lifecycle management.

For more information, see Metrics for Automated Certificate Lifecycle Management.

3.8 Support for cnDBTier Functionalities in CNC Console

With the implementation of this feature, cnDBTier functionalities are integrated into the CNC Console, and BSF users can view specific cnDBTier functions, such as checking the cnDBTier version, status of cnDBTier clusters, and georeplication status on the CNC Console.

> **Note**
>
> This **cnDBTier** options can be accessed only through CNC Console.

The following cnDBTier functionalities are read only and can be viewed on the CNC Console:

- Backup List: This API displays the details of stored backups, such as the ID and size of the backup.
- Database Statistics Report: This API displays the number of available database.
- Georeplication Status:
  - Real Time Overall Replication Status: This API displays the overall replication status in multisite deployments. For example, in a four-site deployment, it provides the replication status between the following sites: site1-site2, site1-site3, site1-site4, site2-site3, site2-site4, and site2-site1. This is applicable for all other sites.
  - Site Specific Real Time Replication Status: This API displays the site-specific replication status.
- HeartBeat Status: This API displays the connectivity status between the local site and the remote site to which BSF is connected.
- Georeplication Recovery: This API provides the recovery status of georeplication for the cnDBTier cluster:
  - Update Cluster As Failed: This API is used to mark a disrupted cluster as failed.
  - Start Georeplication Recovery: This API is used to start the georeplication recovery process.
  - Georeplication Recovery Status: This API is used to monitor the recovery status of georeplication for both FAILED and ACTIVE cnDBTier sites.
- Local Cluster Status: This API displays the status of the local cluster.
- On-Demand Backup: This API provides options to initiate as well as the display the status of the on-demand backup. It also displays the status of initiated on-demand backups.
- cnDBTier version: This API displays the cnDBTier version.

Managing cnDBTier Functionalities at CNC Console

Enable

This feature is enabled automatically when cnDBTier is configured as an instance during the CNC Console deployment. For more information about integrating cnDBTier functionalities with CNC Console, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

Configure

You can view cnDBTier functionalities at CNC Console in the Support for cnDBTier Functionalities in CNC Console section.

Maintain

If you encounter alerts at the system level, see the BSF Alerts section for resolution steps.

In case the alerts persist, perform the following tasks:

1. **Collect the logs**: For information about how to collect logs, see *Oracle Communications Cloud Native Core, Binding Support Function Troubleshooting Guide*.

2. **Raise a service request**: For information about how to raise a service request, see My Oracle Support.

3.9 Diameter Session Retry

BSF Diameter gateway sends the Authorization-Authentication Request (AAR) messages to PCF Diameter gateway. PCF Diameter gateway acknowledges these requests by sending a successful or failed Authorization-Authentication Answer (AAA) messages to BSF.

If BSF Diameter gateway recevies Authorization-Authentication Answer (AAA) message with errors like 5065 (IP-CAN_SESSION_NOT_AVAILABLE), 5012 (DIAMETER_UNABLE_TO_COMPLY) or any other error code or a session timeout then the CNC console has configurations that can be used to resend this failed message to a different/ alternate PCF Diameter gateway.

The BSF Diameter gateway on receving the failed message from Diameter Routing Agent (DRA) captures the failed error context and the error details. The error details are sent to the error handling framework implemented in diameter gateway. The error handling framework provides specific action (such as to try resending the message to an alternate route or peer) that needs to be carried out by the gateway to handle the error that has occurred. The error actions are configured in the CNC Console as Diameter gateway configurations from the user.

Diameter message retries for Rx AAR messages are enabled through the Error Mapping Framework feature in BSF. This framework resolves application errors and takes necessary action based on the error context. The error handler framework tries to find alternate solutions based on the configurations in the CNC Console. If the error is resolved, it sends back the success result to the caller, else it either retries based on the maximum number of resolution attempts configured in CNC Console or terminates the requests by forwarding the last known error.

The operator should have configured a host and realm in the diameter routing table to retry sending the failed diameter messages. Diameter gateway finds the alternate peer from the routing table. If the diameter routing table is not configured, then there is no retry behavior from Policy.

By default, the diameter message retry behavior is disabled for Rx interface. The operator can enable this feature through the CNC Console configurations.

> **Note**
>
> Default number of retry attempts is 0, that is, there is no retry. The retry attempts ranges from 0-10.

BSF retries resending Rx AAR diameter messages for the following configurable error code series:

- 3xxx (Protocol Errors)
- 4xxx (Transient Failures)
- 5xxx (Permanent Failure)

For more information about these error codes, refer to Diameter Error Codes in *Oracle Communications Cloud Native Core, Binding Support Function User Guide*.

Retry Attempts

The user configures the number of retries to be performed for Rx AAR diameter messages in the CNC Console. The retry attempt happens only when the alternate peers are available. If alternate peers are not available, then there is no retry attempt made. The value for number of retries ranges from 1 to 10 times.

The number of retries is set through the advance settings configurations, using the advance setting key `DIAMETER.ErrorHandler.MaxRetryCount.Rx.AAR`.

Peer Cycle Back Retry

In case of the configured number of retry count is more than the total available alternate peers, the user can configure to cycle back the alternate peers. User configures this in CNC Console by setting `retry peer cycle back` field to true. This field value is either true or false.

This peer cycle back retry configuration is set through the advance settings configurations using the advance setting keys `DIAMETER.ErrorHandler.CycleBackRetry.Rx.AAR`. If advance settings configuration are not supported in the CNC Console, then the default peer cycle back retry is false.

For Example: Number of configured retry = 2 and only 2 PCF (PCF1, PCF2) Diameter gateway are configured as alternate peers in BSF.

If Rx AAR message was sent BSF - PCF1 Diameter gateway and the response has failed error code such as 5065/timeout/3002/3004.

Then the first retry uses BSF - PCF2-Diam-Gateway and the response has failed error code such as timeout/3002/3004.

Then the second retry uses BSF - PCF1-Diam-Gateway and thus uses the peer cycle back retry mechanism.

Error Originator Peer

The Error Originator Peer indicates as to where the Rx AAR failed message error occured/ originated when sending or retry sending the Diamter messages. The user can customize the error origination peer by using `Error Response Originator` filed in the CNC Console and the customizing options are based on:

- The error received from an intermediate peer (INTERMEDIATE PEER).
- The error received from the destination peer, which is not an intermediate peer (DESTINATION PEER).
- The error received from any peer (ANY).

By default the error originator peer option is `any` peer.

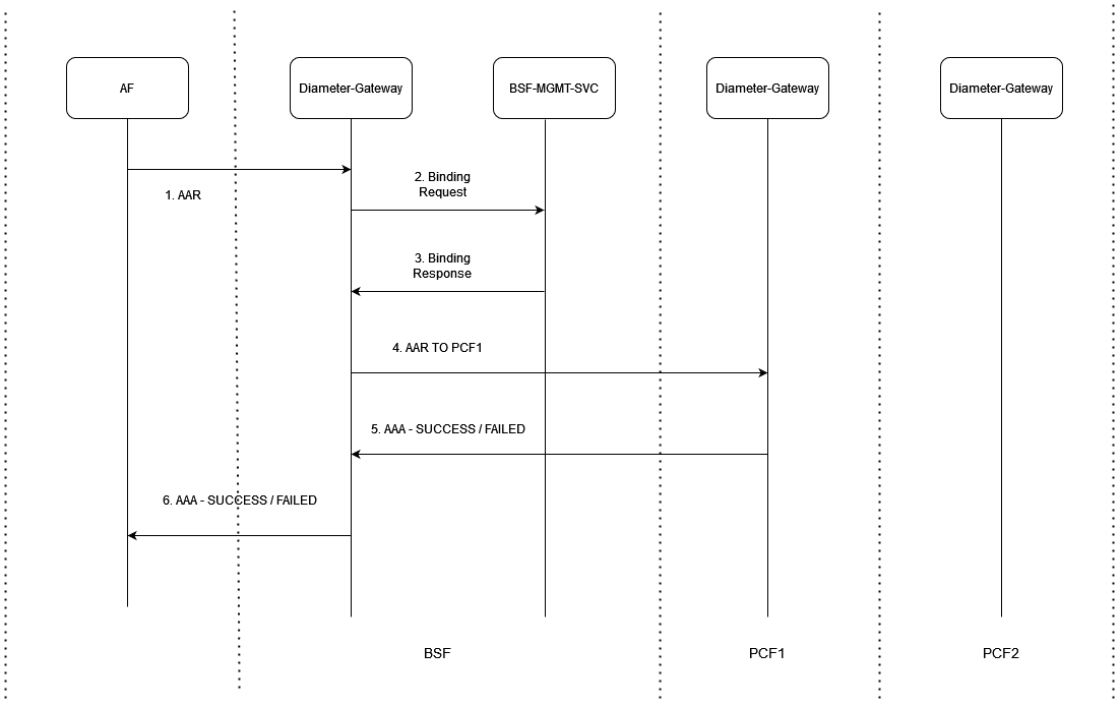
In response timeout cases the error originator option is not available since the origination of error cannot be found.

Call Flows in Diamter Session Retry

Call Flow of Rx AAR Existing Success or Failed Case - When Binding is Found

The call flow describes the scenario where BSF Diameter Gateway sends AAR request toward PCF1 Diameter Gateway on receiving the binding response from BSF Management service. On receiving the AAR request the PCF1 Diameter Gateway may send a successful or a failed AAA response toward BSF Diameter Gateway. The failed response is not handled by the BSF Diameter Gateway.

Figure 3-6 Rx AAR Existing Success/Failed Case - When Binding is Found

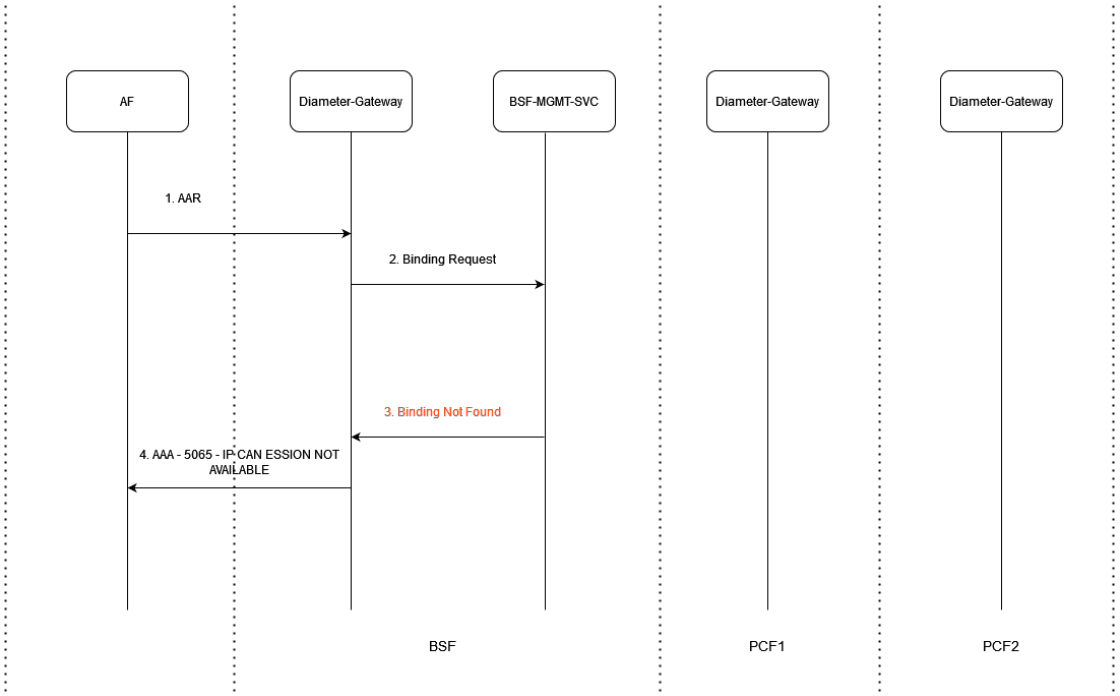


1. Application Function (AF) sends AAR request to BSF Diameter Gateway.
2. BSF Diameter Gateway sends binding request to BSF Management Service.
3. BSF Management service sends back binding response.
4. BSF Diameter Gateway sends AAR request to PCF1 Diameter Gateway.
5. PCF1 Diameter Gateway may send either a successful or failed AAA response and BSF Diameter Gateway do not handle the failed response.

Call Flow of Rx AAR No Retry Case - When Binding is Not Found

The call flow describes the scenario where BSF Diameter Gateway do not receive the binding response from BSF Management service.

Figure 3-7 Rx AAR No Retry Case - When Binding is Not Found

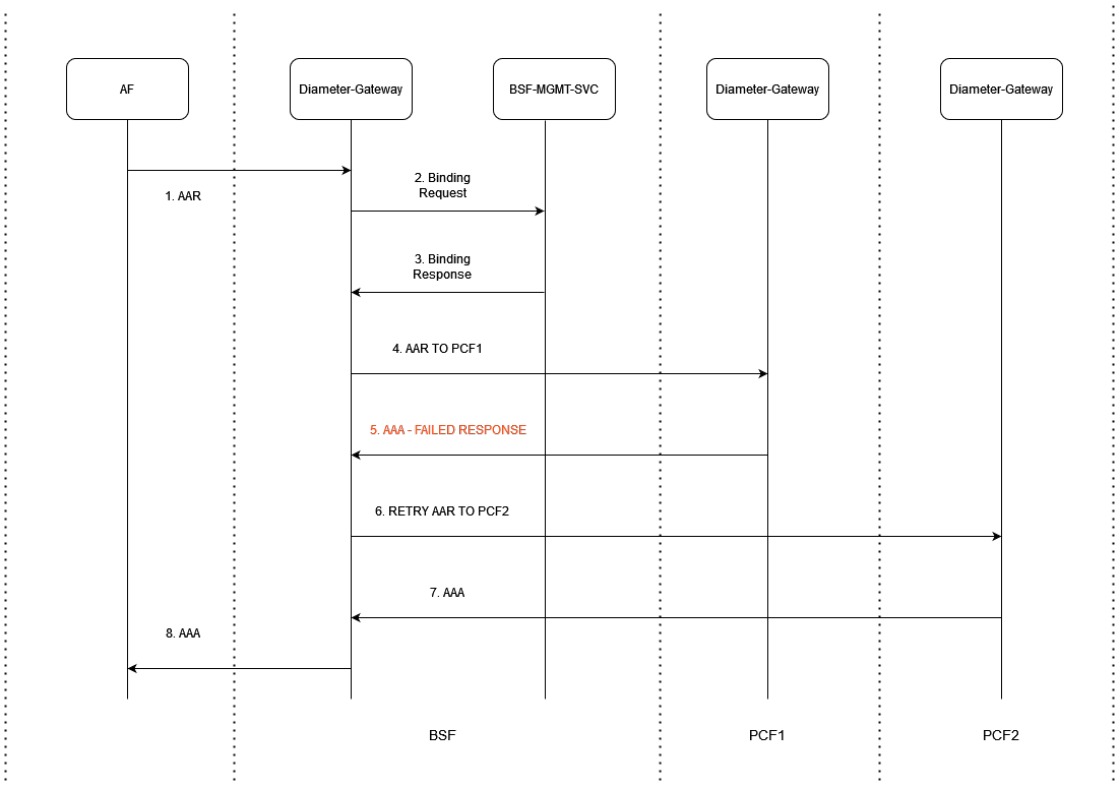


1. Application Function (AF) sends AAR request to BSF Diameter Gateway.
2. BSF Diameter Gateway sends binding request to BSF Management Service.
3. BSF Management service sends "Binding not found" response.
4. BSF Diameter Gateway responds to AF with error code 5065 (IP-CAN_SESSION_NOT_AVAILABLE).

Call Flow of Rx AAR Retry Case - When Binding is Found

The call flow describes the scenario where BSF Diameter Gateway sends AAR request toward PCF1 Diameter Gateway on receiving the binding response from BSF Management service. On receiving the AAR request, the PCF1 Diameter Gateway may send a successful or a failed AAA response toward BSF Diameter Gateway. The failed response is handled by the BSF Diameter Gateway.

Figure 3-8 Rx AAR Retry Case - When Binding is Found

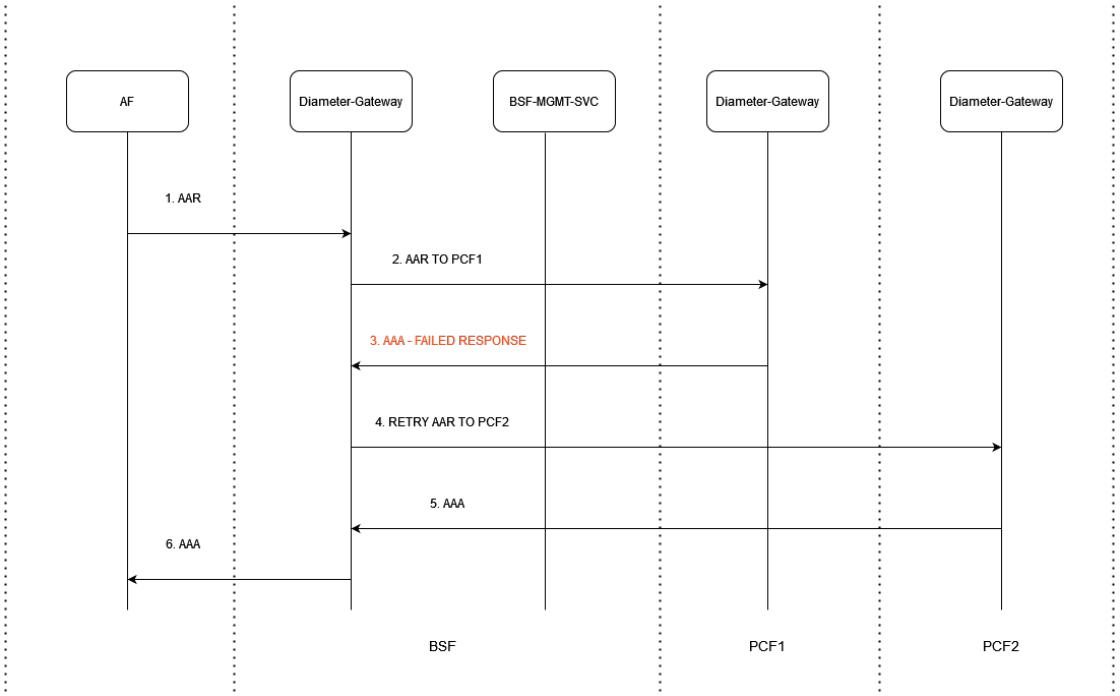


1. Application Function (AF) sends AAR request to BSF Diameter Gateway.
2. BSF Diameter Gateway sends binding request to BSF Management Service.
3. BSF Management service sends back binding response.
4. BSF Diameter Gateway sends AAR request to PCF1 Diameter Gateway.
5. PCF1 Diameter Gateway sends a failed AAA response to BSF Diameter Gateway.
6. BSF Diameter Gateway resends the failed AAA message to PCF2 Diameter Gateway.
7. PCF2 Diameter Gateway sends a successful AAA response to BSF Diameter Gateway.
8. BSF Diameter Gateway sends this AAA message to AF.

Call Flow of Rx AAR Retry Case - When Binding is Not Found

The call flow describes the scenario where BSF Diameter Gateway sends AAR request toward PCF1 Diameter Gateway on not receiving the binding response from BSF Management service. On receiving the AAR request the PCF1 Diameter Gateway may send a successful or a failed AAA response toward BSF Diameter Gateway. The failed response is handled by the BSF Diameter Gateway.

Figure 3-9 Rx AAR Retry Case - When Binding is Not Found

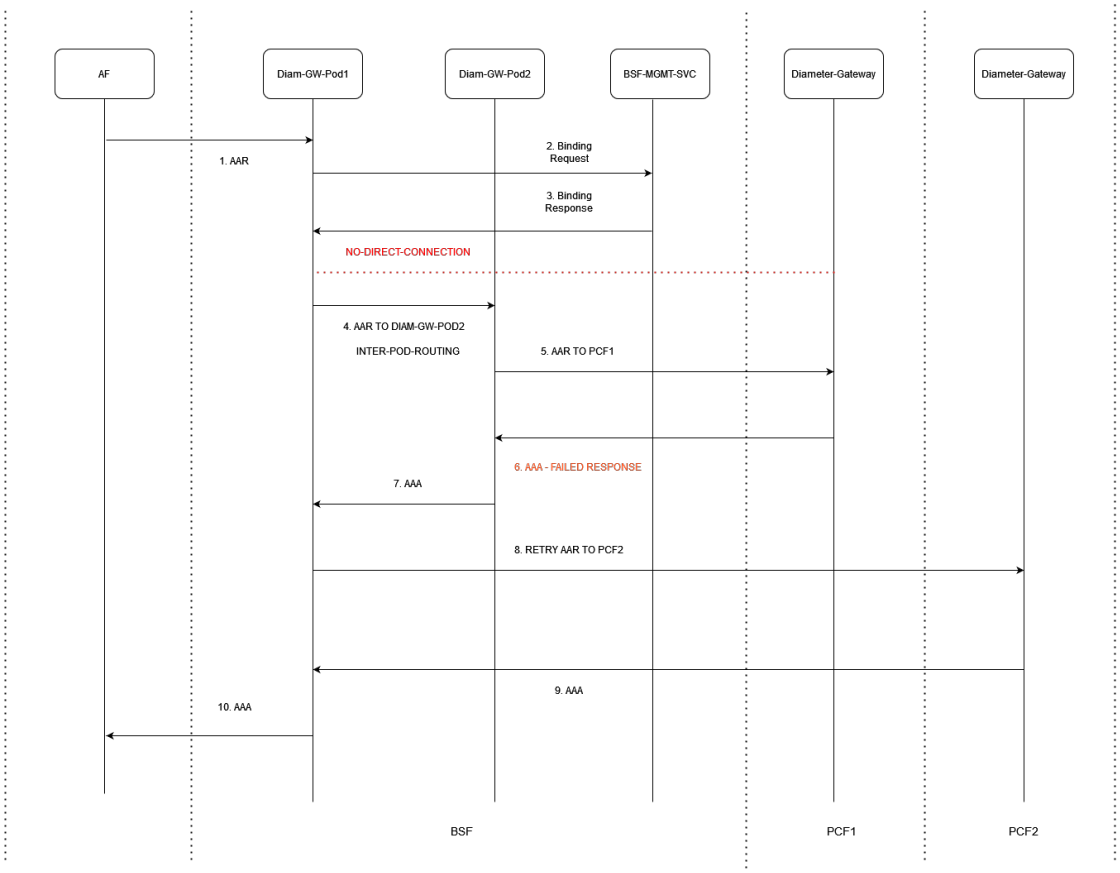


1. Application Function (AF) sends AAR request to BSF Diameter Gateway.
2. BSF Diameter Gateway sends AAR request to PCF1 Diameter Gateway.
3. PCF1 Diameter Gateway sends a failed AAA response to BSF Diameter Gateway.
4. BSF Diameter Gateway resends the failed AAA message to PCF2 Diameter Gateway.
5. PCF2 Diameter Gateway sends a successful AAA response to BSF Diameter Gateway.
6. BSF Diameter Gateway sends this AAA message to AF.

Call Flow of Rx AAR Retry Inter-Pod Routing Case - When Binding is Found

The call flow describes the scenario where BSF Diameter Gateway pods uses inter-pod routing to send AAR request toward PCF Diameter Gateway pods on receiving the binding response from BSF Management service. BSF Diameter Gateway pods handle the failed AAA response from PCF Diameter Gateway pods.

Figure 3-10 Rx AAR Retry Inter-Pod Routing Case - When Binding Found



1. Application Function (AF) sends AAR request to BSF Diameter Gateway pod (Diam-GW-Pod1).
2. It sends binding request to BSF Management service.
3. BSF Management service sends binding response.
4. BSF Diameter Gateway pod1 on not finding any connection to PCF Diameter Gateway pods (PCF1, PCF2), it uses inter-pod routing and sends the AAR request to BSF Diameter Gateway pod2 (Diam-GW-Pod2).
5. BSF Diameter Gateway pod2 sends AAR request to PCF1 Diameter Gateway.
6. PCF1 Diameter Gateway sends a failed AAA response to BSF Diameter Gateway.
7. BSF Diameter Gateway resends the failed AAA message to PCF2 Diameter Gateway.
8. PCF2 Diameter Gateway sends a successful AAA response to BSF Diameter Gateway.
9. BSF Diameter Gateway sends this AAA message to AF.

Default Error Handling Configuration

BSF provides the default error handling configuration to retry on all error codes (except diameter result code 2xxx) and timeout for Rx AAA failed diameter messages. When the diameter message retry feature is enabled on Rx interface, these default error handling configurations get applied by default. The user has an option to enable/disable these default configurations through the CNC Console edit configurations.

For all default error handling configurations, the value for retry attempt is 1 and peer cycle back retry is false. The value of retry ranges from 1 to 10 times.

Managing Diameter Session Retry

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

Enable

By default, Diameter Message Retry behavior is disabled for Rx interface and operator can enable this feature through the CNC Console configurations.

Configure Using CNC Console

Perform the feature configurations in CNC Console as described in Error Configurations section.

To enable over-writing of destination host on retry message, *DIAMETER.ErrorHandler.Enable.UpdateDestinationHost* key must be set to true in the Advanced Settings. For more information, see Settings.

Configure Using REST API

Perform the export/import error configurations as described in "Error Configurations" section in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Document*.

Observe

Observability

Metrics

Following metrics were updated with `retry` and `retryReason` dimensions in the Diameter Gateway Metrics section:

- `ocbsf_diam_request_network_total`
- `ocbsf_diam_request_inter_total`

Alerts

Following alerts are used by this feature:

- AAA_RX_FAIL_COUNT_EXCEEDS_CRITICAL_THRESHOLD
- AAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD
- AAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Maintain

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

In case the alerts still persist, perform the following:

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

3.10 Support for BSF Status on NRF on CNC Console

CNC Console for BSF shows health status information of BSF and other producer NF instances related to BSF. It provides a consolidated status of the BSF instances registered with NRF.

BSF CNC Console has a new **BSF NRF Status** page, added under **Status and Query** page. This page provides the consolidated status of BSF instances registered with NRF. The user can also see the health status of primary and secondary NRF instances, or the alternate NRF.

Managing Support for BSF status on NRF on CNC Console

Enable

BSF Status on NRF feature uses NRF Client service. Hence ensure that the NRF Client service is enabled by setting the value `global.nrfClientNfManagementEnable` as `true`.

For more information on NRF Client configurations, see *Configuring NRF Client* section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Configure Using CNC Console

To view the health status using CNC Console, see BSF NRF Status.

Configure Using REST API

Perform the feature configurations as described in "NRF Status" and "NRF Client" sections in *Oracle Communications Cloud Native Core, Binding Support REST Specification Guide*

Observability

Metrics:

Following metrics were updated in the NRF Client Metrics section.

- nrfclient_perf_info_nf_profile_load
- nrfclient_current_nf_status
- nrfclient_nf_status_with_nrf
- nrfclient_nrf_operative_status
- nrfclient_nrf_status_total
- nrfclient_nrf_successive_healthy_count
- nrfclient_nrf_successive_unhealthy_count
- nrfclient_on_demand_conn_in_request_total
- nrfclient_on_demand_conn_out_response_total
- nrfclient_on_demand_processing_latency_ms
- ocpm_nrf_tracing_request_timeout_total
- nrfclient_nw_conn_out_request_total
- nrfclient_nw_conn_in_response_total
- nrfclient_nw_conn_in_notify_request_total
- nrfclient_nw_conn_out_notify_response_total

- nrfclient_network_message_processing_latency

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

In case the alerts still persist, perform the following:

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

3.11 Network Policies

Network Policies are an application-centric construct that allows you to specify how a pod communicates with various network entities. It creates pod-level rules to control communication between the cluster's pods and services, and to determine which pods and services can access one another inside a cluster.

Previously, the pods under BSF deployment could be contacted by any other pods in the Kubernetes cluster without any restrictions. Now, Network Policies provide namespace-level isolation, which allows secured communications to and from BSF with rules defined in respective Network Policies. The Network Policies enforce access restrictions for all the applicable data flows except communication from Kubernetes node to pod for invoking container probe. For example, BSF internal microservices cannot be contacted directly by any other pods.

The following table lists the different access policies to be used by BSF traffic flows.

> **Note**
>
> This list is not exhaustive but tries to represent all the traffic flows supported by BSF.

Microservice	Direction	Client/Server	Port	Access Policy
Configuration Svc	Egress	• Database • K8s API server for K8s secret	3306, K8s API Server Port	K8s Network Policies
Configuration Svc	Egress	• Jaeger Agent	6831	K8s Network Policies
Configuration Svc	Ingress	• Console • Egress Gateway for configuration • Ingress Gateway for configuration • Perf-info for configuration • App-info for configuration • ATS • ARS • NrfClient	8081	K8s Network Policies

Microservice	Direction	Client/Server	Port	Access Policy
Configuration Svc	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Ingress Gateway	Egress	• Jaeger Agent	6831	K8s Network Policies
Ingress Gateway	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
Ingress Gateway	Egress	• Coherence	8000, 7	K8s Network Policies
Ingress Gateway	Ingress	• Perf Info	8080	K8s Network Policies
Ingress Gateway	Ingress	• SBI Peer	80, 443	3GPP-defined Access Policies
Ingress Gateway	Ingress	• Coherence	8000, 8095, 8096	K8s Network Policies
Ingress Gateway	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Egress Gateway	Egress	• Jaeger Agent	6831	No Access Policy due to SBI Egress*
Egress Gateway	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	No Access Policy due to SBI Egress*
Egress Gateway	Egress	• Coherence	8000, 8095, 8096	No Access Policy due to SBI Egress*
Egress Gateway	Egress	• SBI Peer	Decided at run-time	3GPP-defined Access Policies
Egress Gateway	Egress	• ARS	ARS Port	K8s Network Policies
Egress Gateway	Ingress	• Registration	8080	K8s Network Policies
Egress Gateway	Ingress	• Egress Gateway for coherence	8000	K8s Network Policies
Egress Gateway	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Egress Gateway	Ingress	• Coherence	8000, 8095, 8096	K8s Network Policies
Audit	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Audit	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies

Microservice	Direction	Client/Server	Port	Access Policy
App Info	Ingress	• Registration • Subscription • Auditor	5906	K8s Network Policies
App Info	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
diam-gateway	Egress	• Jaeger Agent	6831	K8s Network Policies
diam-gateway	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
diam-gateway	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
diam-gateway	Ingress	• Peer	3868	K8s Network Policies
Bsf-Management	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Bsf-Management	Egress	• Jaeger Agent	6831	K8s Network Policies
Bsf-Management	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
NRF-Client	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
NRF-Client	Egress	• Jaeger Agent	6831	K8s Network Policies
NRF-Client	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies
Query-Svc	Ingress	• Prometheus • Liveness • Readiness	9000	K8s Network Policies
Query-Svc	Egress	• Jaeger Agent	6831	K8s Network Policies
Query-Svc	Egress	• Database • K8s API Server for K8s Secret	3306, K8s API Server Port	K8s Network Policies

As an assumption when deploying BSF, the following labels are set by default:

Table 3-4 Default Labels

Pod	Label
All BSF Pods	app.kubernetes.io/part-of: ocbsf
Ingress Gateway Pod	app.kubernetes.io/name: ocbsf-ingress-gateway
Egress Gateway Pod	app.kubernetes.io/name: ocbsf-egress-gateway
Diam-gateway	app.kubernetes.io/name: diam-gateway
CM-Service	app.kubernetes.io/name: cm-service

BSF Security Policies:

- **deny-ingress-all**: To block all ingress traffic of pods presents in a BSF deployment.
- **allow-ingress-sbi**: To allow traffic on the Ingress Gateway Pods on container ports 8000 and 9443 to allow sbi traffic.
- **allow-diam-gateway**: To allow traffic on the Diameter-Gateway on port 3868.
- **allow-ingress-prometheus**: To allow the traffic flow from Prometheus service to the BSF with default ports (These ports can be changed by the customer).
- **allow-ingress-from-bsf-pods**: To allow ingress communication between the different microservices of the BSF.
- **allow-ingress-from-console**: To allow ingress communication between CNCC-Core and CM-Service on port 8081.
- **deny-egress-all-except-egw**: To block all egress traffic of pods present in a BSF deployment, except for Egress-Gateway and Diameter-Gateway.
- **allow-egress-database**: To allow the traffic flow from BSF to db sql port and db monitoring port with default ports (These ports can be changed by the customer).
- **allow-egress-k8s-api**: To allow the traffic flow from BSF to Kubernetes API server port (These ports can be changed by the customer).
- **allow-egress-jaeger**: To allow the traffic flow from BSF to Jaegar agent port and DNS service with default ports (These ports can be changed by the customer).
- **allow-egress-traffic-and-dns**: To allow the traffic flow from BSF to k8s DNS service with default ports (These ports can be changed by the customer).
- **allow-egress-to-bsf-pods**: To allow egress communication between the different microservices of BSF.

> **Note**
>
> The default Network Policies to be applied for BSF are the recommended even though they are not very granular but they keep operational overhead to the minimum and still achieve access control security.
>
> If a Network Policy is installed to restrict Prometheus escaping the metrics from the PODs, then a restart of the PODs is required. If the NP is installed before the PODs are up, then there is no need to restart the PODs.

Managing Network Policies

Enable

To use this feature, Network Policies need to be applied to the namespace wherein BSF is applied.

Configure

You can configure this feature using Helm. For information about configuring network policy for BSF deployment, see *Configuring Network Policy* section in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Observe

There are no specific metrics and alerts required for the Network Policies feature.

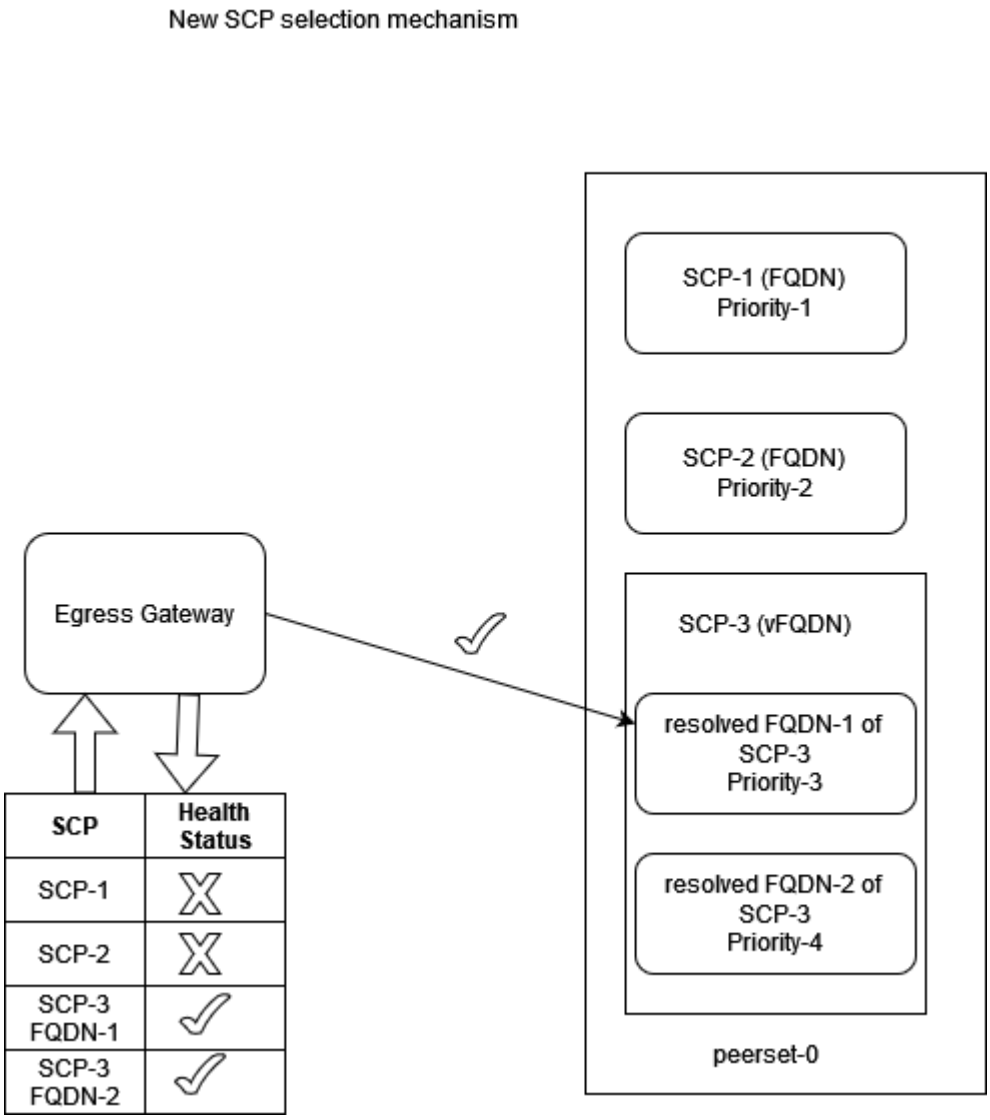
3.12 Monitoring the Availability of SCP using HTTP2 OPTIONS

BSF determines the availability and reachability status of all SCPs irrespective of the configuration types.

This feature is an enhancement to the existing SBI routing functionality. Egress Gateway microservice interacts with SCP on their health API endpoints using HTTP2 OPTIONS method. It monitors the health of configured SCP peers to ensure that the traffic is routed directly to the healthy peers. This enhancement avoids routing or rerouting towards unhealthy peers, thus minimizing the latency time.

Egress Gateway microservice maintains the health status of all available and unavailable SCPs. It maintains the latest health of SCPs by periodically monitoring and uses this data to route egress traffic to the most preferred healthy SCP.

Figure 3-11 New SCP Selection Mechanism



Once `peerconfiguration, peersetconfiguration, routesconfiguration, and peermonitoringconfiguration` parameters are configured at Egress Gateway microservice, and all SCPs (after Alternate Route Service (ARS) resolution, if any vFQDN is configured) are marked initially as healthy. The peers attached to the associated peerset are scheduled to run health API checks and update the health status continuously.

During the installation, the value of the parameter `peermonitoringconfiguration` is set to false by default. Since, this feature is an add-on to the existing SBI Routing feature and will be activated if the `sbirouteconfig` feature is enabled. To enable this feature, perform the following:

- configure `peerconfiguration` with `healthApiPath`
- configure `peersetconfiguration`
- configure `sbiroutingerroractionsets`
- configure `sbiroutingerroractionsets`

- configure `routesconfiguration`
- enable `peermonitoring`

If SBI Routing feature is enabled before upgrading, the `healthApi` in `peerconfiguration` should be attached manually to existing configured peers. If the operator tries to enable peermonitoringconfiguration and the targeted peers do not have the `healthApiPath` then an appropriate error response is sent.

Managing Monitoring the Availability of SCP Using SCP Health APIs

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

Configure

You can configure the Monitoring the Availability of SCP using the REST API.

Configure Using REST API: Perform the following feature configurations as described in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Document*:

- create or update peer `Peer Configuration` with health status endpoint details.
- create or update the peerset `peersetconfiguration` to assign these peers
- enable the feature using the below peermonitoring configuration `peermonitoringconfiguration`.

> **Note**
>
> Health Monitoring of the peer will start only after the feature is enabled and the corresponding peerset is used in `sbirouteconfig`.

Observe

Following metrics are added in the Metrics in Egress Gateway Metrics for SCP section:

- oc_egressgateway_peer_health_status
- oc_egressgateway_peer_health_ping_request_total
- oc_egressgateway_peer_health_ping_response_total
- oc_egressgateway_peer_health_status_transitions_total
- oc_egressgateway_peer_count
- oc_egressgateway_peer_available_count

Alert

Following alerts are added in the Alert section:

- SCP_PEER_UNAVAILABLE
- SCP_PEER_UNAVAILABLE

3.13 Supports 3gpp-Sbi-Correlation-Info Header

The 3gpp-Sbi-Correlation-Info header may be used to contain correlation information such as UE identity, that may be used by an operator in various offline network management,

performance analysis and troubleshooting tools/applications to identify messages (requests, responses, subscriptions, notifications) related to a particular subscriber.

By supporting this feature, BSF as a service consumer or as a service producer generates, forwards and sends the UE identity in 3gpp-Sbi-Correlation-Info header, to identify the UE related to the HTTP request or response.

BSF provides a global configurations page on CNC Console GUI to enable or disable the correlation-info header feature. On enabling,

- BSF receives the correlation-info header and forwards them to the producer NFs.
- BSF does not receive the correlation-info header, then BSF generates and forwards them to the producer NFs.

In BSF, generation of new correlation-info header is managed by the **Management services** configuration page. This allows enable or disable of header generation along with the flexibility of selecting correlation type to use for the header. The correlation-types such as SUPI, GPSI, or both are supported for this release.

The generated or received headers can only be forwarded when the setting *Send Correlation-Info Header* as part of **Management services** is enabled.

3gpp-Sbi-Correlation-Info

The header contains correlation information such as UE identifier related to the HTTP request or response.

> **Note**
>
> 1. The possibility to include more than 1 correlationinfo parameter in the 3gpp-Sbi-Correlation-Info header is kept for future extensibility.
>   correlationinfo = ctype "-" cvalue
>
>   ctype = "imsi" / "impi" / "suci" / "nai" / "gci" / "gli" / "impu" / "msisdn" / "extid" / "imei" / "imeisv" / "mac" / "eui" / token
> 2. The token is defined for future extensibility.
>   The token of ctype shall not use the dash ("-") character.
>
>   cvalue = 1*tchar

Table 3-5 The format of cvalue shall comply with the data type description.

ctype	Description
SUPI	VarUeId format defined for IMSI and starting after the string "imsi-"
GPSI	VarUeId format defined for MSISDN and starting after the string "msisdn-"

Table 3-6 3GPP defined Custom HTTP Headers

Header	Description	Example
3gpp-sbi-correlation-info	This header may be used to contain correlation information such as UE identity, that may be used by an operator in various offline network management, performance analysis and troubleshooting tools/applications to identify messages (requests, responses, subscriptions, notifications) related to a particular subscriber.	EXAMPLE 1: When UE identifier used is SUPI and SUPI type is an IMSI: 3gpp-Sbi-Correlation-Info: imsi-345012123123123 EXAMPLE 2: When UE identifier used is GPSI and GPSI type is an MSISDN:3gpp-Sbi-Correlation-Info: msisdn-1234567890 EXAMPLE 3: When UE identifiers used are SUPI and GPSI where SUPI type is an IMSI and GPSI type is an MSISDN:3gpp-Sbi-Correlation-Info: imsi-345012123123123; msisdn-1234567890

Managing SBI messages correlation using Subscriber Identity

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

Configure

In CNC Console, enable this feature in the general settings page.

For more details on enabling or disabling the correlation-info header on GUI, see General Settings.

Configure Using REST API

For configuring parameters for SBI messages correlation using Subscriber Identity feature using REST APIs, see *Oracle Communications Cloud Native Core, Binding Support Function REST API Specification Guide*.

Observe

Following metrics are added in Correlation-Info Header Metrics section:

- ocbsf_correlation_info_header_received
- ocbsf_correlation_info_header_forwarded
- ocbsf_correlation_info_header_generated

3.14 Configurations for Pre and Post Upgrade/Install Validations

This feature applies validation checks that are required on the application, databases, and its related tables before and after the upgrade/installation of BSF application.

On enabling this mandatory pre-flight and post-flight validation checks, for successful upgrade/installation following are validated:

- does the related database exists
- does all the required tables exist

- does the required table schema exist for all the required tables
- does all the required infrastructure exists

This pre-flight and post-flight checks ensures that all the dependent databases, tables, schema, applications are in right order for performing successful update/installation.

For more information on how to how to set the parameter value for pre and post flight checks, see *Upgrade Hardening, Pre and Post Flight Checks* section in *Oracle Communications Cloud Native core, Binding Support Function (BSF) Installation, Upgrade and Fault Recovery Guide*.

3.15 Detection and Handling of Late Arrival Requests

BSF receives requests from Ingress Gateway with the 3GPP headers. These requests help in detecting the response time for the BSF Management Service. The Ingress Gateway receives the following headers:

- 3gpp-Sbi-Origination-Timestamp- It contains the timestamp when the originating entity initiates the request
- 3gpp-Sbi-Max-Rsp-Time- The header indicates the duration (expressed in milliseconds) during which the HTTP client waits for a response.

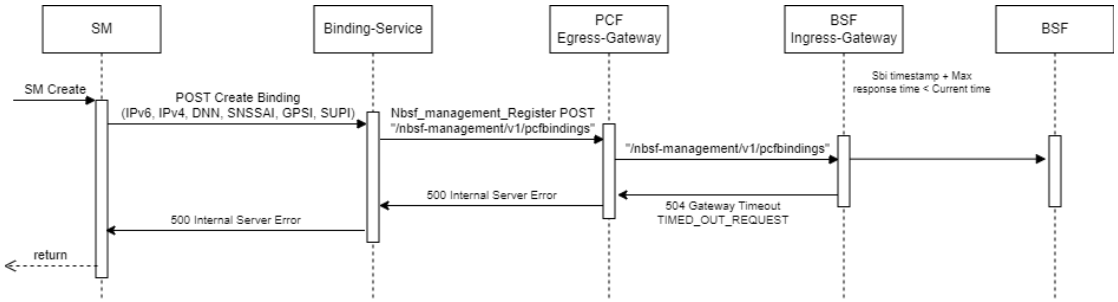
If the configuration for determining the late Arriving requests is enabled and BSF does not receive the required headers, the requests are valid and processed. The call flow will continue as normal.

BSF must be able to read the 3gpp-Sbi-Origination-Timestamp and 3gpp-Sbi-Max-Rsp-Time headers to respond to the request. Consider the following scenarios:

- If the sum of 3gpp-Sbi-Origination-Timestamp and 3gpp-Sbi-Max-Rsp-Time is less than the current time, the PCF service rejects the message with a 504 HTTP code and sends the message "TIMED_OUT_REQUEST".
- If the request does not include either 3gpp-Sbi-Origination-Timestamp or 3gpp-Sbi-Sender-Timestamp, or 3gpp-Sbi-Max-Rsp-Time headers, then the request is accepted. There are no changes in the call flow with the inclusion of collision detection.
- If 3gpp-Sbi-Max-Rsp-Time receives a negative value, the header is considered invalid. In this case, the service fallbacks to the default behavior and accepts the request irrespective of the 3gpp-Sbi-Origination-Timestamp or 3gpp-Sbi-Sender-Timestamp value.

The following diagram illustrates the request timeout in BSF:

Figure 3-12 Request Timeout in BSF



For handling and detection of Late Arrival and Collision Detection functionality in BSF, it is necessary that these headers and the new Custom header are transmitted from PCF to BSF.

Custom Header Enhancement adds the Time Stamp as a default value in the request and response custom headers with specific time formats and time zones. A valid function definition for timestamp in the configuration is: func: currentTime(time-format,time-zone).

Note: Here, only the GMT, IST, PST, and UTC time zones are to be considered for all 5G timestamps.

The only date format supported for the headers is RFC 7231: EEE, dd MMM yyyy HH:mm:ss.SSS zzz (Sun, 04 Aug 2019 08:49:37.845 GMT).

Any other format will result in a parse error which leads to not using the header for the feature (taking it as null value).

Collision Detection

BSF may encounter a colliding or duplicate request for a binding registration from a different PCF. BSF shall consider a request as colliding or duplicate binding registration when two registrations are for the same subscriber (SUPI), DNN, SNSSAI, IPV4/IPv6 prefix, or IpDomain (in case IPv4Address is present) but from different PCF instances (ID/pcfDiamHost/pcfFqdn or pcfIpEndPoints).

In case support for timer headers is enabled:

- If 3gpp-Sbi-Origination-Timestamp header support is enabled and the colliding or the duplicate requests contain the header with an appropriate value, compare the values. If the values are different, it will consider the request with the more recent timestamp in the header.
- If the value of 3gpp-Sbi-Origination-Timestamp in both the requests is the same, then if Custom-Sbi-Sender-Timestamp header support is enabled and the colliding or the duplicate requests contain the header with an appropriate value, compare the values. It will consider the request with the more recent timestamp in the header.

In case support for timer headers is disabled:

- If 3gpp-Sbi-Sender-Timestamp header support is enabled and the colliding or the duplicate requests contain the header with an appropriate value, compare the values. If the values are different, it will consider the request with the more recent timestamp in the header.
- If the value of 3gpp-Sbi-Sender-Timestamp in both requests is the same, it will consider the later request.

If the incoming colliding or duplicate request has an older timestamp than the ongoing or existing request or record, it will reject the request with an HTTP "403 Forbidden" status code. The condition name for the error in the GUI is "Existing binding information found in DB" on the SBI Error Codes configuration page. The BSF function to detect and resolve collision requests is configurable.

If Late Arrival functionality is not enabled, the headers must be propagated to bsf-management-service if collision detection is required or enabled. For this, Ingress Gateway should populate three new collision headers following the required criteria:

Table 3-7 Collision Headers

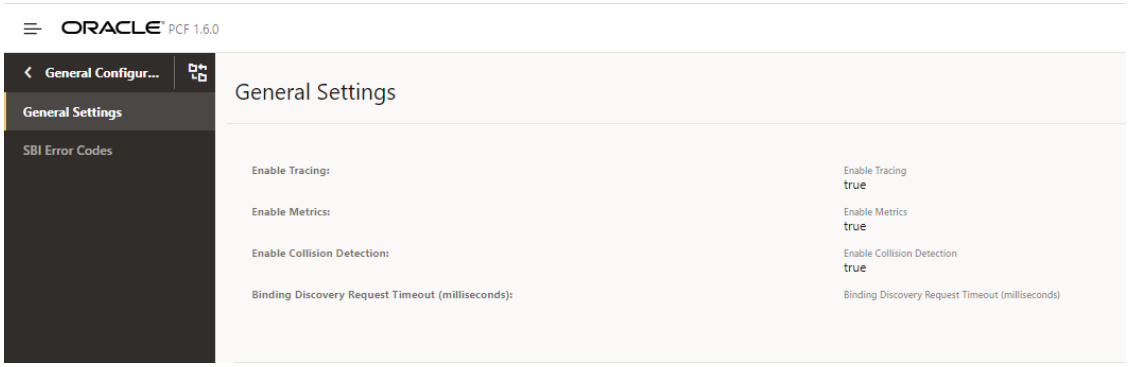
At Ingress Gateway	At bsf-management-service
3gpp-Sbi-Origination-Timestamp	collision-3gpp-origination-timestamp
Custom-Sbi-Sender-Timestamp	collision-custom-sender-timestamp
3gpp-Sbi-Sender-Timestamp	collision-3gpp-sender-timestamp

> **Note**
>
> These collision headers implement collision detection at BSF.

Enable

You can enable or disable the collision detection in the General Settings of the General Configuration window of the CNC Console.

Figure 3-13 Enabling Collision Detection



You can enable or disable the collision detection feature using the REST API for BSF. Use the General Settings REST API to enable or disable this feature.

REST API Path: `/oc-bsf-configuration/v1/general`

For more information, see the *Oracle Communications Cloud Native Core Binding Support Function User Guide*.

Configuration

To create the collision headers that are used for collision detection in BSF it is necessary to add the following configuration to BSF Ingress Gateway.

```
routesConfig:
    - id: bsf_management_register
      uri: http://{{ template "service-name-bsf-management" . }}:
{{ .Values.global.servicePorts.bsfManagementServiceHttp }}
      path: /nbsf-management/**
      order: 1
      method: POST
      filters:
        customReqHeaderEntryFilter:
          headers:
            - methods:
              - POST
              headersList:
                - headerName: 3gpp-Sbi-Message-Priority
                  defaultVal: 24
                  source: incomingReq
                  sourceHeader: 3gpp-Sbi-Message-Priority
                  override: false
                - headerName: collision-3gpp-origination-timestamp
```

```
    source: incomingReq
    sourceHeader: 3gpp-Sbi-Origination-Timestamp
    override: false
  - headerName: collision-custom-sender-timestamp
    source: incomingReq
    sourceHeader: Custom-Sbi-Sender-Timestamp
    override: false

- headerName: collision-3gpp-sender-timestamp
    source: incomingReq
    sourceHeader: 3gpp-Sbi-Sender-Timestamp
    override: false
```

Observe

To observe the collision detection functionality, you can use metrics that are specific to BSF management service. For information, see Binding Support Function Metrics.

3.16 Support for Timer Configuration

BSF supports the configuration of Diameter interfaces or Rx interfaces timers for all the applicable Diameter messages. The timer configuration needs to be configured for AAR, RAR, STR, and ASR messages. The timer configuration is an option to configure the diameter response timeout value for diameter messages. If the timer value is not configured, then the BSF Diameter gateway works with the default value of 4000 milliseconds for AAR, RAR, STR, and ASR messages.

The Diameter response timeout or the timer value is configured per Diameter interface level. This value can also be configured per message level of the Diameter interface. The timer configuration needs to be configured for Authentication Request (AAR), Re-Auth-Request (RAR), Session-Termination-Request (STR), and Abort-Session-Request (ASR) messages.

For BSF, currently Diameter Rx interface is applicable. The response timeout value is configured using the Rx application level and its messages (AAR, RAR, STR, and ASR) level.

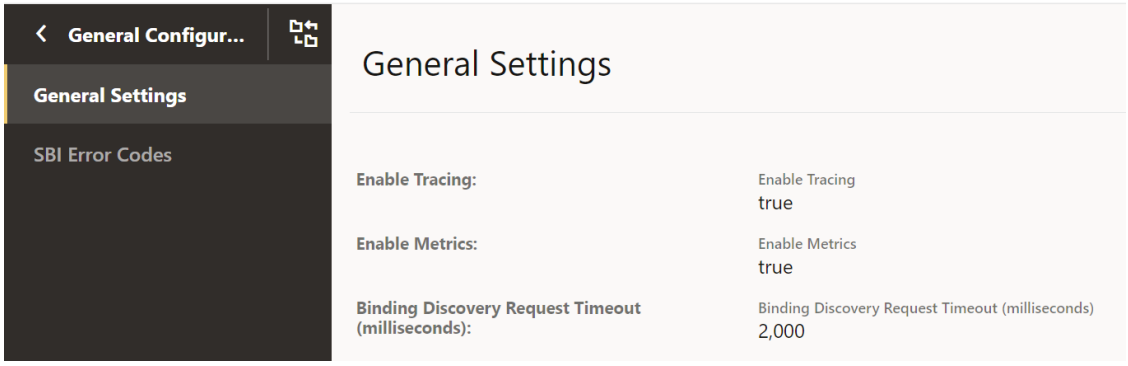
Enable

The timer configuration is a functionality supported by Binding Support Function configurations. You do not need to enable or disable this feature.

Configure

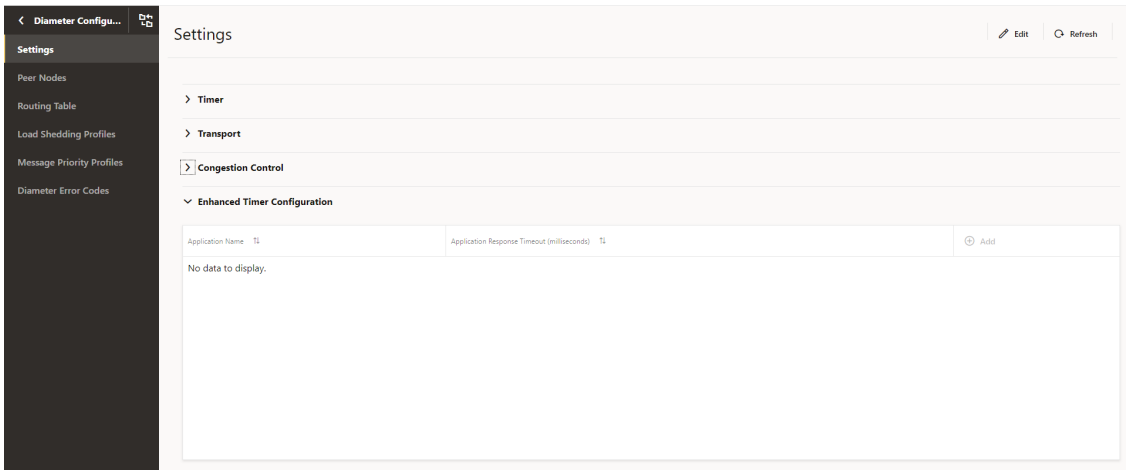
The `Binding discovery request timeout` configuration parameter is used for request timeout value for the discovery request sent by the BSF Diameter Gateway towards the BSF Management Service.

Figure 3-14 General Settings



The Enhanced Timer Configuration is available on the settings of the Diameter Configuration page.

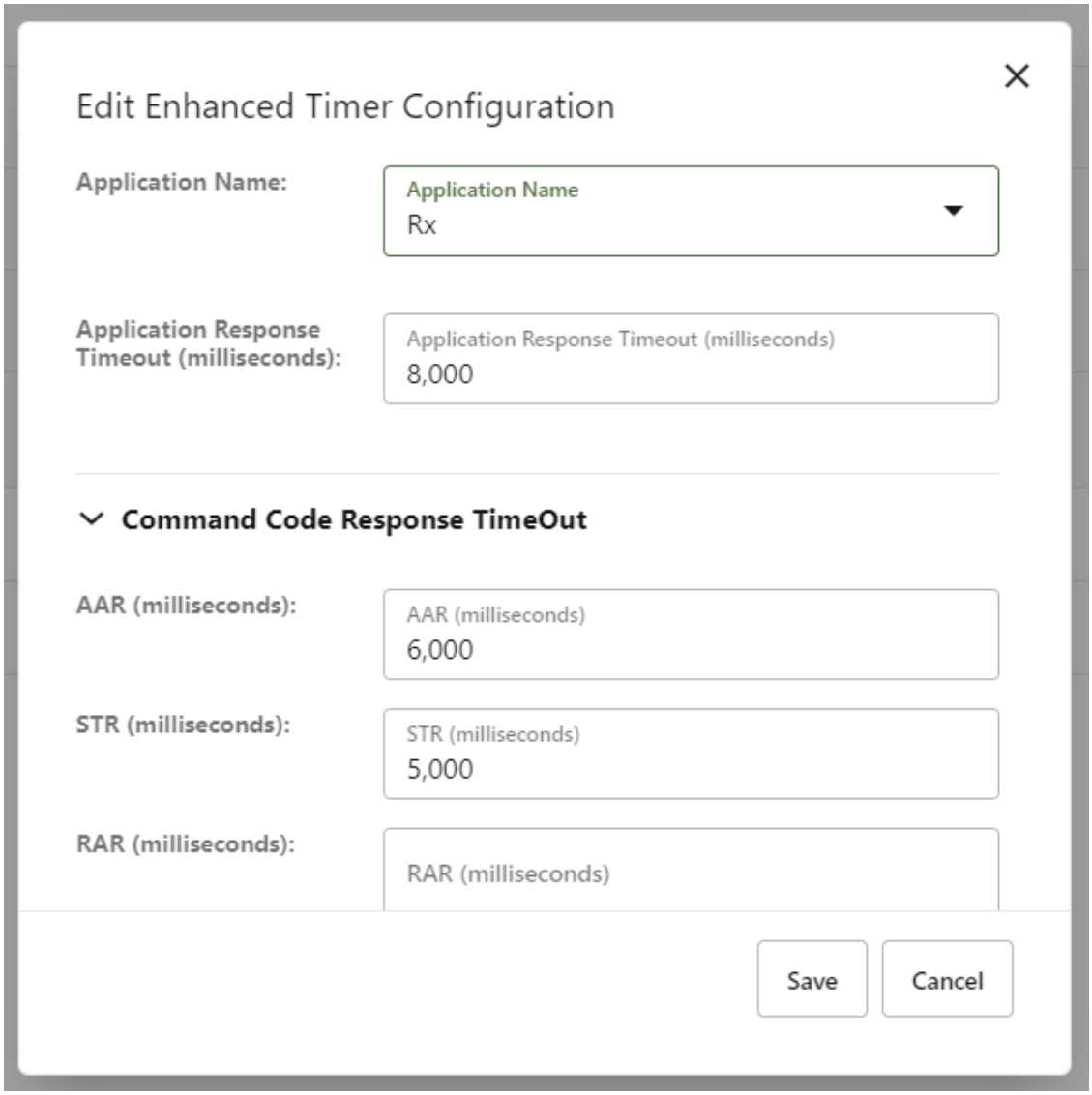
Figure 3-15 Enhanced Timer Configuration



This configuration accepts interface level Diameter response timeout value. If the Diameter interface level timeout is configured, then the user is able to configure message level response timeout value for the corresponding Diameter interface.The response timeout value range for interface and message level is 3000 milliseconds to 2147483647 milliseconds.

In the CNC Console, you can specify the Command Code Response TimeOut value for the AAR, RAR, STR, and ASR message types.

Figure 3-16 Edit Enhanced Timer Configuration



You can customize the configurations related to this feature using the CNC Console or REST APIs for BSF.

- **Configure using CNC Console:** Perform the feature configurations on the General Configurations and Diameter Configurations page. For more information about the configurations, see General Settings and Diameter Configurations.
- **Configure using REST API:** Perform the configurations using GET and PUT operations. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Document*.

Observe

To observe the timer configuration functionality, you can use metrics that are specific to BSF management service. For information, see Binding Support Function Metrics.

3.17 Support for Server Header

BSF handles various requests from consumer Network Functions (NFs) and other network entities over HTTP protocol. On receiving these requests, BSF validates and processes them before responding to these requests. In case, BSF sends an error response, then the consumer NFs need to know the source of the error to trouble shoot the error and take corrective measures. The integration of this feature at BSF helps to determine the originator of the error response.

This feature offers the support for Server Header in BSF responses, which contains information about the origin of an error response and the type of the error encountered. The Server Header includes the type of NF as "NF Type", followed by a “-” and the identity of the NF or the network entity. It is expected to be present in all BSF responses in the following format:

<NF_Type>-<NF_Instance_Id>

Where,

- `<NF Type>` is the type of the NF generating the error.
- `<NF Instance-Id>` is the unique identifier of the NF instance generating the error response.

For example: BSF-54804518-4191-46b3-955c-ac631f953ed8

The inclusion of the Server header in the BSF response is configurable, and can be enabled or disabled using a flag. Also the error codes that are included as part of the Server header in the error response are also configurable. The configuration of these parameters are done through either with REST APIs that are exposed through configuration server or Helm Configurations.

The operation mode that is either `REST` or `HELM` for Server Header configuration is done using the below flag:

```
ingress-gateway:
  serverHeaderConfigMode: REST # Possible values: HELM, REST. Based on this
value, the feature flag for "server"  header will need to be enabled either
in Helm configuration or Rest  configuration.
```

> **Note**
>
> Nf Type and Nf Instance Id are mandatory fields for Server Header to get included in the error response. If either of the fields Nf Type or Nf Instance Id are configured as empty, then the Server Header will not get included in the error response.

Managing Server Header

Enable

By default, this feature is disabled.

You can enable the Server Header feature using Helm or REST API configurations:

- **Helm:** To enable the server header feature using Helm configuration, set the value for parameter `serverHeaderConfigMode` to `HELM` in the `custom-values.yaml` file. Then, set

the value for parameter `serverHeaderDetails.enabled` to `true` under global and routesConfig for `ingress-gateway`.

- **REST API:**To enable the server header feature using REST configuration, set the value for parameter `serverHeaderConfigMode` to `REST` in the `custom-values.yaml` file. Using REST API, set the `enabled` parameter to `true` in the following resource URI:
  {apiRoot}/BSF/nf-common-component/v1/igw/serverheaderdetails

Configure

You can configure the server header feature using the REST API or CNC Console:

- **Configure using REST API:**
  Perform the REST API configurations in the following sequence to configure this feature:
  1. Configure **serverheaderdetails** to enable the feature.
     {apiRoot}/BSF/nf-common-component/v1/igw/serverheaderdetails
  2. Configure **routesconfiguration** to map route ID and its corresponding route-level configuration.
     {apiRoot}/BSF/nf-common-component/v1/igw/routesconfiguration
  3. Configure **errorcodeserieslist** to update the **errorcodeserieslist** that are used to list the configurable exception or error for an error scenario in Ingress Gateway.
     {apiRoot}/BSF/nf-common-component/v1/{serviceName}/errorcodeserieslist

  > **Note**
  >
  > If you define server header configuration at both global and route levels, the route level configuration takes precedence over the global level configuration.

  For more information, see the "Server Header at Ingress Gateway" section in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*.

- **Configure using Helm:** When parameter `serverHeaderConfigMode` is set to `HELM` and to configure the Server Header at Ingress Gateway, you need to perform the helm configurations either at Global or at Route level.
  Following Helm Configuration performed at Globel Level:

```
# All attributes under "serverHeaderDetails" will need to be configured
only if "serverHeaderConfigMode" is set as "HELM"
serverHeaderDetails:
  enabled: true
  errorCodeSeriesId: E1
  configuration:
    nfType: BSF
    nfInstanceId: INS-1

# Use below configuration to define errorCodeSeries list
errorCodeSeriesList:
  # Value of "id" attribute will need to used for assigning
"errorCodeSeriesId" either at Global or Route level conf for Server header.
- id: E1
  errorCodeSeries:
  - errorSet: 4xx
    errorCodes:
    - 400
```

```
    - 408
  - errorSet: 5xx
    errorCodes:
    - 500
    - 503
- id: E2
  errorCodeSeries:
  - errorSet: 4xx
    errorCodes:
    - -1
```

Following Helm Configuration performed at Route Level:

```
routesConfig:
- id: backend_ms1_route
  uri: https://backend-ms1:8440/
  path: /ms1/**
  order: 1
  metadata:
    # All attributes under "serverHeaderDetails" will need to be
configured only if "serverHeaderConfigMode" is set as "HELM" and Route
level configuration is required. If not defined, Global configurations
will be used
    serverHeaderDetails:
      enabled: true     # Since this flag is set to true at Route level,
"server" header configuration will be enabled for this Route with
respective "errorCodeSeriesId" as E2
      errorCodeSeriesId: E2 # This attribute will need to be defined if
"server" header configuration is enabled at Route level.
- id: backend_ms2_route
  uri: https://backend-ms2:8550/
  path: /ms2/**
  order: 2
  metadata:
    # All attributes under "serverHeaderDetails" will need to be
configured only if "serverHeaderConfigMode" is set as "HELM" and Route
level configuration is required. If not defined, Global configurations
will be used
    serverHeaderDetails:
      enabled: false    # Since this flag is set to false at Route level,
"server" header configuration will be disabled for this Route altogether.
```

> **Note**
>
> If you define server header configuration at both global and route levels, the route level configuration takes precedence over the global level configuration.

For more information, see the "Server Header Configurations" section in the *Oracle Communications Cloud Native Core, Binding Support Function Installation and Upgrade Guide*.

- **Configure using CNC Console:** A new group, **NF Server Settings** is added to the Management Service page. For more information, see see Service Configurations.

3.18 Support for Session Retry and Alternate Route Service

In previous releases, Binding Support Function was configured with primary and secondary Network Repository Function (NRF) statically and limiting to a specific number. Starting with Release 1.8.0 of BSF, session retry enables the alternate recovery mechanisms to mitigate the impact of any unavailable resource.

This feature allows you to configure virtual FQDNs and perform DNS SRV Lookup to retrieve alternate failover NRF which can be maintained dynamically at the DNS Server.

Managing Session Retry and Alternate Route Service

Enable
To enable the Session Retry and Alternate Routing functionality, set the value of `enableVirtualNrfResolution` to true in the custom-values.yaml file for BSF. For more information on setting the parameter value, see section "Configuring NRF Client" in *Oracle Communications Cloud Native Binding Support Function Installation Guide*.

Configure
You can configure the parameter for Session Retry and Alternate Routing functionality by updating the custom-values.yaml file for BSF.

- To configure the retry functionality, see "Configuring NRF Client" in *Oracle Communications Cloud Native Binding Support Function Installation Guide*.
- To configure alternate routing, see section "Alternate Route Service Configuration" in *Oracle Communications Cloud Native Binding Support Function Installation Guide*.

3.19 Turning off AccessToken signature Validation

OAuth access tokens grant an NF service consumer access to the services of an NF producer of a particular NFType, for a specific period. With this feature, BSF can turn off AccessToken signature validation at the application layer. For example when Aspen service mesh is integrated with BSF, the service mesh can perform the AccessToken validation. In such cases, operator may want BSF to skip validating the AccessToken signature. BSF checks audience and scope fields only, and sends 403 - Forbidden response code when any of the values do not match. In addition, when BSF receives a request without the AccessToken, it sends a 401 - Unauthorized response code. To turn off the AccessToken signature validation at BSF application, the user must perform configurations as described in the *Oracle Communications Cloud Native Core Binding Support Function Installation Guide*.

3.20 XFCC Header Validation

Overview

With XFCC Header Validation feature, Binding Support Function (BSF) as a producer, checks if the SCP that is sending the HTTP request is the same SCP that is configured in the BSF. BSF performs this check by comparing the FQDN of the SCP present in the “x-forwarded-client-cert” (XFCC) of http2 header with the list of FQDN of the SCPs configured in the PCF. This configured list contains all the host FQDNs resolved successfully via DNS-SRV as well as static SCPs. The header validation can be enabled at global as well as at the route level.

> **Note**
>
> This feature is applicable only when SCP is deployed in the network topology.

Configuring SCPs at BSF

To configure SCP, you need to customize `custom.yaml` at the time of deploying BSF.

In the earlier releases, users could only configure SCPs statitcally as shown in the following snippet:

```
xfccHeaderValidation:
    validation:

      enabled: false
      nfList:
        - scp.com
        - smf.com
        - amf.com
```

However, in BSF release 22.1.0 or later, users can configure single or multiple virtual FQDNs for the SCP along with the static configuration as shown in the following snippet:

```
global:
    xfccHeaderValidation:
      validation:
        enabled: false
        peerList:
          - name: scp.com
          - name: smf.com
          - name: amf.com
          - name: scp1.com
            enabled: true
          - name: scp2.com
          - name: scp3.com
            enabled: false
          - name: xyz.test.com
            enabled: true
            scheme: http
            type: virtual
          - name: abc.test.com
            enabled: true
            scheme: https
            type: virtual
          - name: xfcc.test.com
            enabled: false
            scheme: http
            type: virtual
```

Static SCP: To define an SCP instance statically, add the name and set enabled parameter to true in the peerList. If the enabled parameter is set to false for an instance, then it is not included in the list of configured FQDNs. If you do not specify enabled parameter then by default it is considered as true.

Virtual SCP: To define an SCP with virtual FQDN, add the name, scheme as http or https, type as virtual, and set enabled parameter to true. If the enabled parameter is set to false for an instance, then it is not included in the list of configured FQDNs.

Resolving FQDNs to find Authorized SCPs

During the bootup of Ingress Gateway, it tries to resolve the configured virtual FQDN via Alternate Route service using the following helm configuration:

```
dnsSrv:
    port: *svcAlternateRouteServiceHttp #Alternate-route port for scheme
'http'. Change is required if the scheme below changes.
    scheme: http
```

If Alternate Route service is unable to resolve the configured virtual host, Ingress Gateway stores it in the list of failed FQDNs and reattempts the request at 300 s (default value configured for **dnsResolutionInterval**).

The following metric is used when the request to resolve configured virtual FQDNs is unsuccessful:

- `oc_ingressgateway_dns_resolution`: This metric is pegged when DNS resolution for a given FQDN fails.
- `oc_ingressgateway_dns_resolution_failure`: This is a gauge metric that is triggered when DNS resolution for a given FQDN fails.

Handling Traffic Flow

The XFCC header is validated when:

- a single XFCC header present in the incoming request to IGW
- multiple XFCC headers are present in the incoming request to IGW

Validating single XFCC Header
The following figure describes the call flow for validation of a single XFCC header:

Figure 3-17 Call Flow Validation of Single XFCC Header

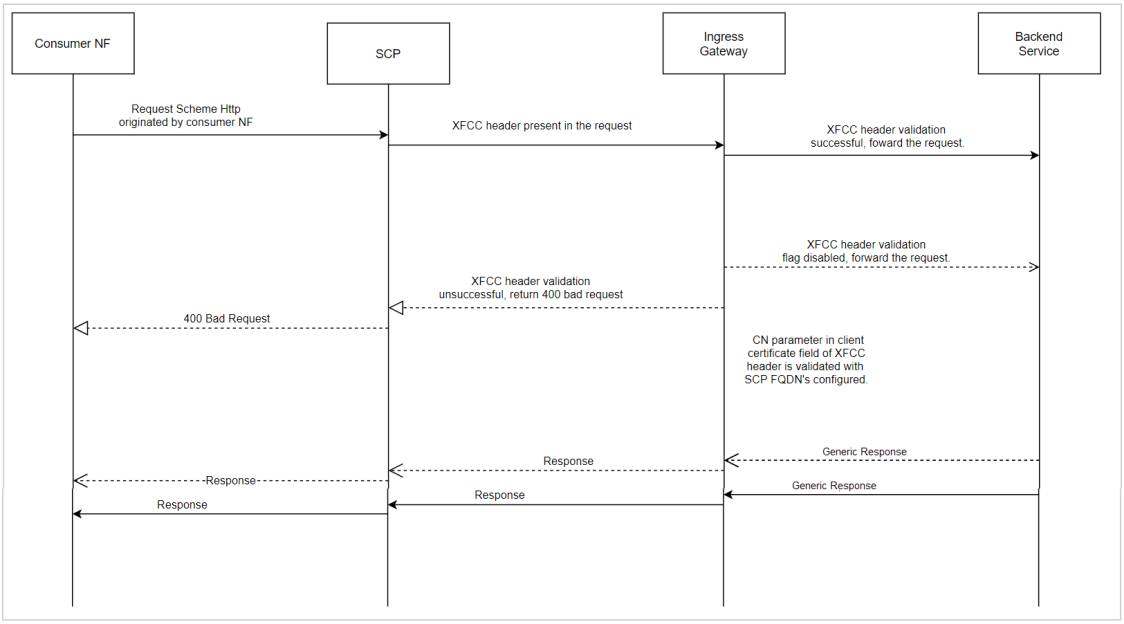


Table 3-8 Single XFCC Header Configuration

Scenario	Condition	Action
Ensure that the XFCC Header validation parameter is enabled for the corresponding route match and the matchCerts count is configured correctly.Given XFCC Header validation parameter is enabled for the corresponding route match and matchCerts count correctly configured.	When the matchField parameter of the client certificate field in XFCC header matches with one of the configured NF FQDNs .	Forwards the request to a back-end microservice and receives a corresponding response.
Given XFCC header validation parameter is enabled for the corresponding route match and matchCerts count correctly configured.	When matchField parameter of client certificate field in XFCC header does not match with the configured NF FQDNs.	Return a 400 Bad Request response from Ingress Gateway. For more infirmation about error codes, see SBI Error Codes Configurations
Given XFCC header validation parameter disabled for the corresponding route match.	NA	Forwards the request to the back-end microservice and receives a corresponding response.

Example of a single XFCC header request:

```
x-forwarded-client-cert: By=http://
router1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8de68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=Test Client"; URI=http://testenv1.blr.com;DNS=blr.com; DNS=www.blr.com
```

Validating multiple XFCC Headers

The following figure describes the call flow for validation of multiple XFCC headers for the following scenarios:

Figure 3-18 Call Flow Validation of Multiple XFCC Headers

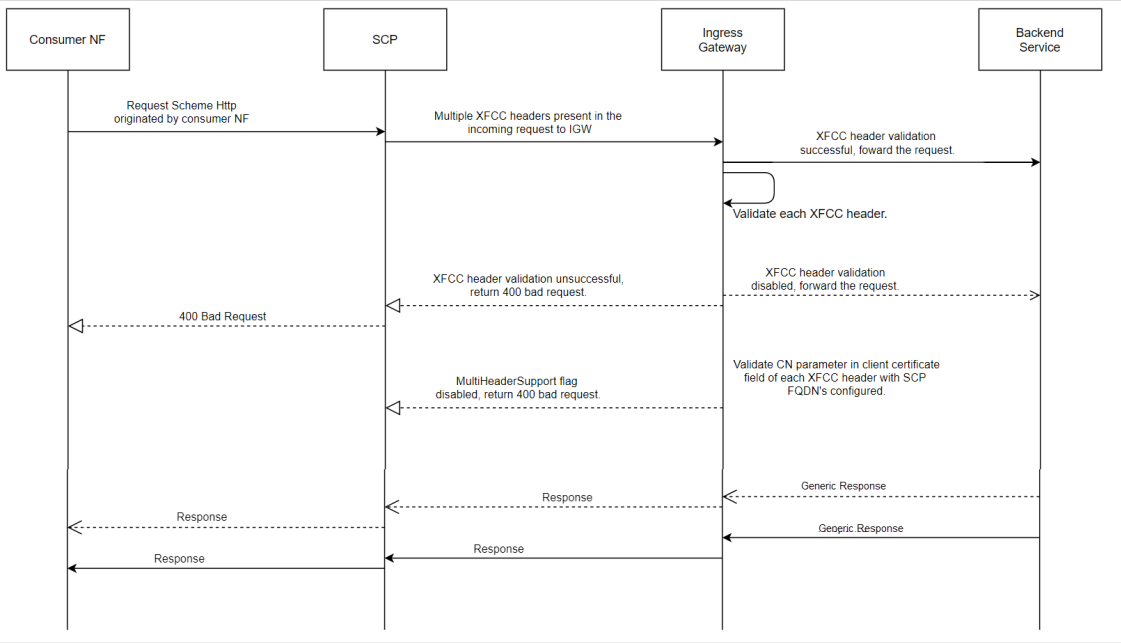


Table 3-9 Multiple XFCC Headers Configuration

Scenrio	Condition	Action
Given XFCC header validation parameter is enabled and matchCerts count correctly configured to validate across XFCC header certificates from the right most entry.	When matchField parameter of the corresponding client certificate field being validated against currently in the corresponding XFCC header matches with the NF FQDN's configured at Ingress Gateway.	Consider the request as a valid request and forward the request to the back-end micro-service and receive a corresponding response.
Given XFCC header validation parameter is enabled and matchCerts count correctly configured to validate across XFCC header certificates from the right most entry.	When matchField parameter of client certificate field in corresponding XFCC headers do not match with the NF FQDN's configured at Ingress Gateway for the corresponding matchCerts count.	Consider the request as an invalid request and return a 400 Bad Request response from IGW. For more infirmation about error codes, see SBI Error Codes Configurations
Given XFCC header validation parameter is enabled and matchCerts count -1.	NA	Consider the request as valid request and match against the corresponding match field in all XFCC headers, if validation successful then forward the request else return 400 BAD Request.
Given XFCC header validation parameter is disabled.	NA	Forward the request to back-end microservice and receive a corresponding response.

Example of multiple XFCC header request:

```
x-forwarded-client-cert:By=http://
router1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8d
```

```
e68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=nf1.com"; URI=http://
testenv1.blr.com; DNS=nf8.com; DNS=nf1.com; DNS=nf6.com, By=http://
router1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8d
e68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=nf10.com"; URI=http://
testenv1.blr.com; DNS=nf10.com; DNS=nf8.com; DNS=nf9.com, By=http://
routexr1.blr.com;Hash=468ed33be74eee6556d90c0149c1309e9ba61d6425303443c0748a02dd8
de68; Subject="/C=US/ST=CA/L=San Francisco/OU=Lyft/CN=nf4.com"; URI=http://
testenv1.blr.com; DNS=nf9.com; DNS=nf4.com;DNS=nf1.com
```

Managing XFCC Header Validation

- **Global Level**: To enable or disable the XFCC header validation feature, set the value of the `ingress-gateway.global.xfccHeaderValidation.validation.enabled` to true or false respectively.
- **Route Level**: To enable or disable the XFCC header validation feature at route level, set the value of the `xfccHeaderValidation.validationEnabled` under routesConfig to true or false respectively.

> **Note**
>
> If the `xfccHeaderValidation.validationEnabled` parameter is defined at route level, then the configuration takes precedence over global configuration.

For instance, if you want to enable XFCC header validation for selected routes, then set the global parameter as false and make route specific configuration to true.

```
global:
    xfccHeaderValidation:
      validation:
        enabled: false


routesConfig:
    - id: reverse_bsf_service
      uri: http://{{ template "service-prefix" . }}-bsf-management:
{{ .Values.global.servicePorts.bsfManagementServiceHttp }}
      path: /nbsf-management/**
      order: 1
      metadata:
        xfccHeaderValidation:
          validationEnabled: true
```

For more information about setting the parameter values, see section "XFCC Header Validation Configuration" in *Oracle Communications Cloud Native Binding Support Function Installation Guide*.

Configure

You can configure the parameter for XFCC Header Validation by updating the custom-values.yaml file for BSF. For more information about configuring the parameter value, see the "XFCC Header Validation Configuration" section in *Oracle Communications Cloud Native Binding Support Function Installation Guide*.

Observe

To observe the XFCC header validation functionality, you can use metrics that are specific to Ingress Gateway. For information, see Ingress Gateway Metrics.

Configuring Error Codes

When the XFCC header validation feature is enabled and SCP FQDN in the incoming header does not match the configured FQDN in PCF, XFCC header is not present, or XFCC header is invalid, then PCF may return error in the response. Users have the ability to customize the error code returned in the response using the following helm configuration:

```
errorTrigger:
          - exceptionType: XFCC_HEADER_INVALID
            errorCode: '401'
            errorCause: xfcc header is invalid
            errorTitle: 'Invalid XFCC Header'
            errorDescription: 'Invalid XFCC Header'
          - exceptionType: XFCC_MATCHCERTCOUNT_GREATER_THAN_CERTS_IN_HEADER
            errorCode: '402'
            errorCause: matchCerts count is greater than the certs in the
request
            errorTitle: ''
            errorDescription: ''
          - exceptionType: XFCC_HEADER_NOT_PRESENT_OR_EMPTY
            errorCode: '403'
            errorCause: xfcc header is not present or empty in the request
            errorTitle: ''
            errorDescription: ''
```

If the configured error code in the errorCodeOnValidationFailure field lies in 3xx error series only then the values for retryAfter and redirectUrl if configured under XFCC Header Validation Configuration at Ingress Gateway are used to populate Retry-After and LOCATION headers correspondingly while sending error response from Ingress Gateway.

3.21 Georedundancy Support

The Cloud Native Core (CNC) architecture supports Geographically Redundant (Georedundant) BSF deployments to ensure high availability and redundancy. It offers a two or three sites georedundancy to ensure service availability when one of the BSF sites is down.

The specifications for georedundancy feature are as follows:

- All the georedundant sites must have Helm and REST based configurations except for NF InstanceId, BSF Endpoint, and port.
- The georedundant BSF sites must be reachable from NFs or Peers on all the sites.
- The same NFs or Peers must not communicate to other georedundant BSF sites simultaneously for the same session.
- All the sites must register with NRF independently and work in an active state.
- All BSF instances share the **Session State** data by using the DB Tier replication service. This enables service continuity during the failure of any of the sites.
- The NFs in a given site can discover BSF instances through NRF. However, local configurations such as DNS SRV or static configuration are required to determine the primary and secondary or alternate BSF configuration. When the primary instance is available, the NFs send service requests to the primary instance.

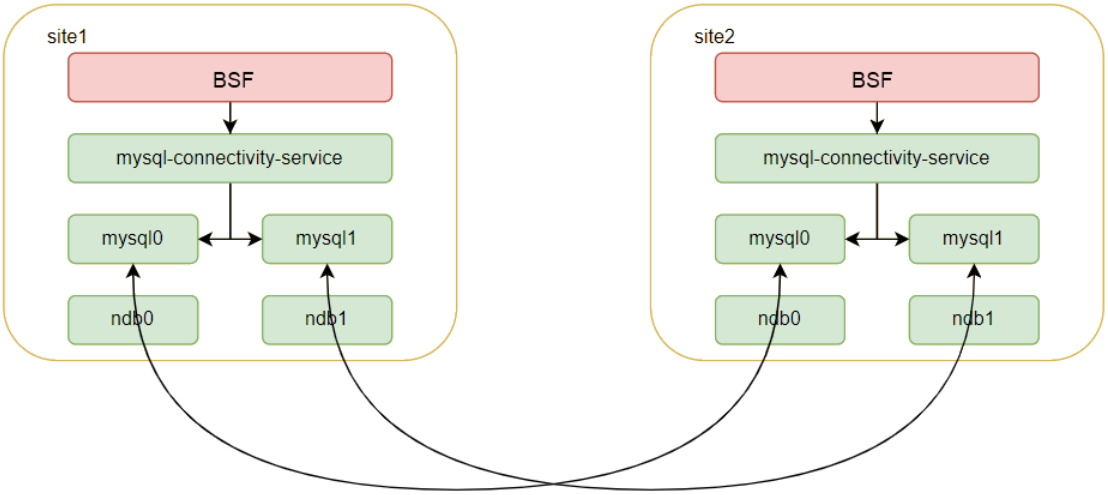
- NRF always reflects current functional status of a given BSF instance. Thus, during the failure of a given BSF instance, the value of `NfStatus` is updated to **SUSPENDED** by either NRF or BSF instance. Therefore, when NF detects failure of primary instance due to error response or status notification from NRF, the NF redirects its traffic to the secondary instance, until the primary instance becomes available again.

BSF supports the following types of georedundant deployment:

Two-Site Georedundancy Deployment

The following diagram depicts the topology for two-site georedundant BSF deployment:

Figure 3-19 Two-Site Georedundancy

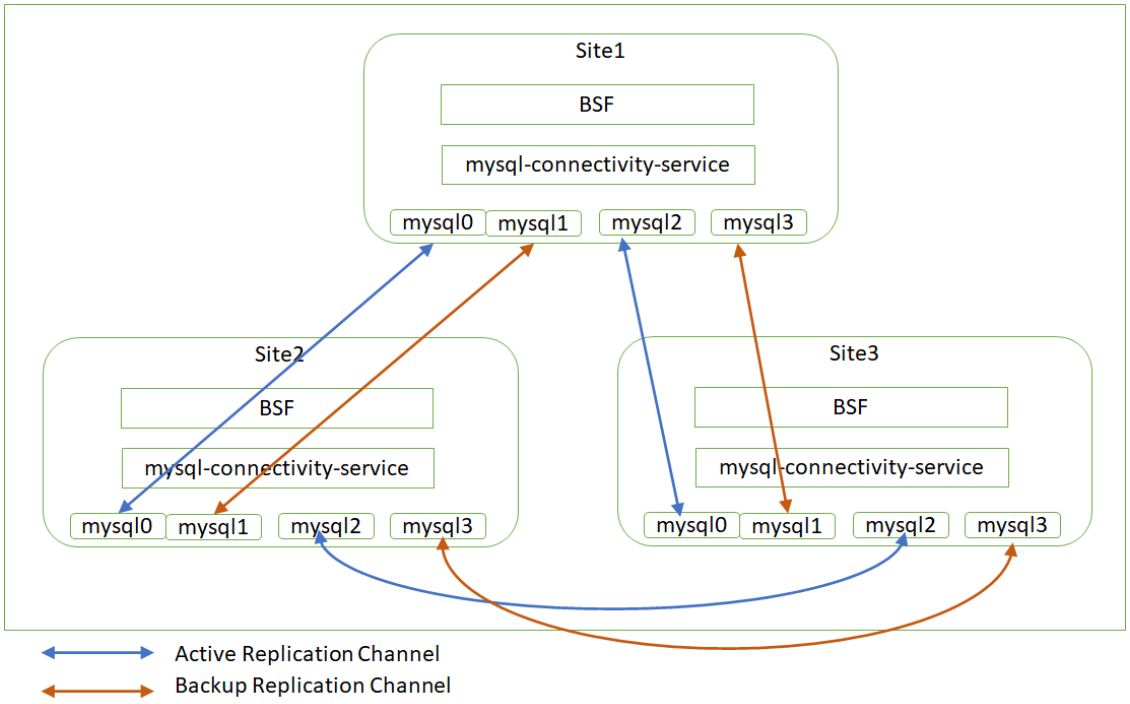


After the second site instance of the cnDBTier is created, you can establish the two site georedundant connections that provide bi-directional data replication between both sites. Therefore, when the records are updated at one site, these changes are replicated to the other remote site in real-time. These updates can be creating, changing, or deleting a record.

Three-Site Georedundancy Deployment

The following diagram depicts the topology for three site georedundant BSF deployment:

Figure 3-20 Three-Site Georedundancy



In case of three site georedundancy, bi-directional replication is established from each site to the other two sites. The database updates from each site are replicated to the other two sites over the replication channel.

The advantages of three-site georedundancy are:

- In case of a single site failure, the remaining two sites keep establishing the bi-directional replication.
- No action is required in case of a site failure.
- Requires 4 SQL pods and 2 rep-svc pods at each site

When the records are updated at one site, these changes are replicated to the other two remote sites in real-time. These updates can be creating, changing, or deleting a record.

Managing Georedundancy

Deploy

To deploy BSF in a georedundant environment:

1. Set up the replicated cnDBTier version 1.8.0.0.3 or above on two or three sites as required. For more information about installing cnDBTier, see "Installing cnDBTier" in *Oracle Communications cnDBTier Installation Guide*.
2. Deploy BSF over the replicated (two or three) cnDBTier sites. For more information about installing and deploying BSF, see *Oracle Communications Cloud Native Binding Support Function Installation Guide.*

Configure

To configure georedundancy:

You need to configure the georedundancy functionality while deploying the BSF instances on the replicated sites. The following parameters must be updated in the custom-values.yaml file for BSF:

Table 3-10 Georedundancy Parameters

Parameter	Description
global.envMysqlHost	The database instance for each site. BSF communicates to the database at the same site only.
global.nfInstanceId	The ID for the site
config-server.envMysqlDatabase	The database for the config server. The two sites must use different database names for config server
cm-service.envCommonConfigMysqlDatabase	The common configuration database. It must be different on the sites
nrf-client.configmapApplicationConfig.profile	Configuration data for nrf client. The `appProfile` and the `nfInstanceId` parameters must be aligned with `global.nfInstanceId`
nrf-client-nfdiscovery.dbConfig.dbName	The common configuration database. It must be different on the sites
nrf-client-nfmanagement.dbConfig.dbName	The common configuration database. It must be different on the sites
appinfo.dbConfig.dbName	The common configuration database. It must be different on the sites
perf-info.dbConfig.dbName	The common configuration database. It must be different on the sites
BSFds.envMysqlDatabaseConfigServer	The database for the config server. The two sites must use different database names for config server
ingress-gateway.dbConfig.dbName	The common configuration database for ingress gateway. It must be different on the sites
egress-gateway.dbConfig.dbName	The common configuration database for egress gateway. It must be different on the sites
alternate-route.dbConfig.dbName	The common configuration database for alternate route. It must be different on the sites

For more information about configuring the parameter value, see the "Alternate Route Service Configuration" section in *Oracle Communications Cloud Native Binding Support Function Installation Guide.*

Observe
cnDBTier generates critical alerts in case of application or database failure. For more information, see *Oracle Communications Cloud Native Core DBTier User Guide*.

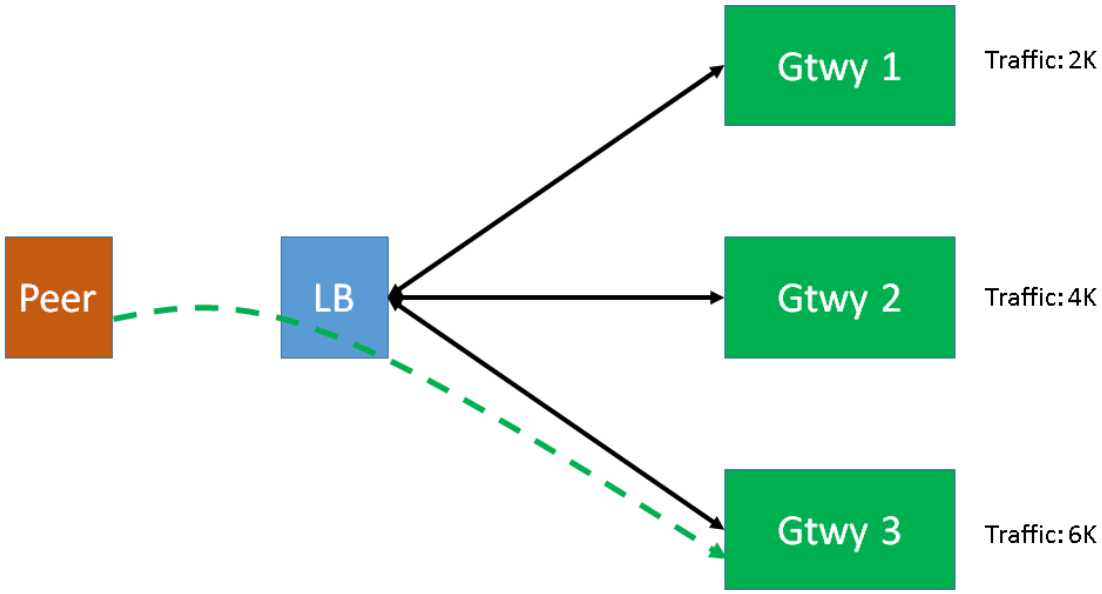
Maintain
BSF allows you to monitor the georedundancy deployment through cnDBTier alerts. Access the Prometheus GUI to check for new App alerts.

3.22 Diameter Gateway Pod Congestion Control

The Diameter Gateway is a diameter proxy agent for Binding Support Function (BSF). It is a front-end microservice for diameter traffic for both Ingress and Egress traffic and can get

congested due to higher traffic, higher CPU usage, and higher memory utilization. Thus, it is imperative to have suitable congestion control features in place for Diameter Gateway pods to avoid adverse impacts on latency and performance.

Another reason for the need for a congestion control mechanism for Diameter Gateway is the nature of diameter connections. An external LoadBalancer distributes these long-lived connections. As shown in the following image, when the LoadBalancer routes an incoming request from network to Diameter Gateway pod (indicated by green line), the balancer does not take health or load of the pod into consideration. As a result, uneven distribution of traffic can happen, and gateway pods experience congestion.



In Binding Support Function, a congestion control mechanism is implemented at pod level that allows the system to perform the following tasks:

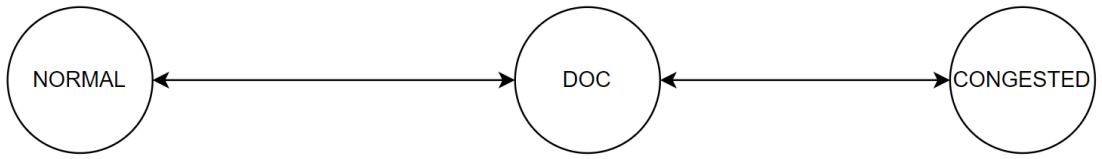
- Determine the pod congestion state
- Trigger Congestion Control

Determining Pod Congestion State

At any given point in time, a pod can be in any one of the following states:

1. Normal
2. DOC (Danger of Congestion)
3. Congested

Figure 3-21 Congestion states



To decide the state of a pod, the following points are taken into consideration:

1. Calculate the congestion state for the following resources:
   a. **Queue**: Compare the count of pending messages against the configured pending messages threshold for each congestion state (DOC, CONGESTED).
   b. **CPU** - The congestion state for CPU usage is calculated by comparing the CPU usage of the container (monitored using cgroup parameter - `cpuacct.usage` that provides current cpu usage in nano seconds) with the configured threshold. The following formula is used to calculate CPU usage:

$$\frac{\frac{CurrentCpuUsage - LastCpuUsage}{CurrentTime - LastSampleTime} * 100}{CPUs}$$

   c. **Memory** - The congestion state for memory usage is calculated by comparing the memory usage of the container with the configured threshold. The following formula is used to calculate memory usage:

$$\frac{memoryUsage}{memoryLimit} * 100$$

   where memory limit is monitored using `memory.limit_in_bytes` cgroup parameter and current memory usage is monitored using `memory.usage_in_bytes` cgroup parameter.
2. Based on the congestion state of resources, the congestion state for the pod is set to the maximum of congested states. The following table describes how the state of the pod is evaluated for various scenarios:

Table 3-11 Published Pod Congestion State

Queue	CPU	Memory	Pod
CONGESTED	NORMAL	DOC	CONGESTED
NORMAL	DOC	NORMAL	DOC
DOC	DOC	Normal	DOC

3. The current published congestion state of the pod is changed to calculated congestion state only when the calculated state remains same for the configured number of continuous sample counts (100 ms by default). By doing so, events like short bursts of traffic triggering a change in the congestion state and load shedding can be avoided. The exceptions to this rule are when:
   a. Current state is NORMAL, and the calculated state is CONGESTED.
   b. Current state is CONGESTED, and the calculated state is NORMAL.

Triggering Congestion Control

Every time a message is fetched from the queue for processing, the system checks the current congestion state of the pod. If the current state is either DOC or Congested, the congestion control mechanism is triggered. After verifying that the message type is a request, a priority is assigned to it. The priority value for a request can be between 0 to 15, where 0 is the highest priority, and 15 is the lowest priority. If the assigned priority is lower than or equal to discard priority, the message is rejected.

> **Note**
>
> Congestion control does not apply to response messages as they are always accepted.

Figure 3-22 Process flow for triggering congestion control

For priority based load shedding to happen, the load rule configured for current congestion state is taken into consideration. If there is no rule configured for a congestion state, the request is accepted by default. While defining load rules, the user can customize the result to reject the request. However, to reject requests from backend peers, the result code is always DIAMETER_TOO_BUSY.

Call Flow

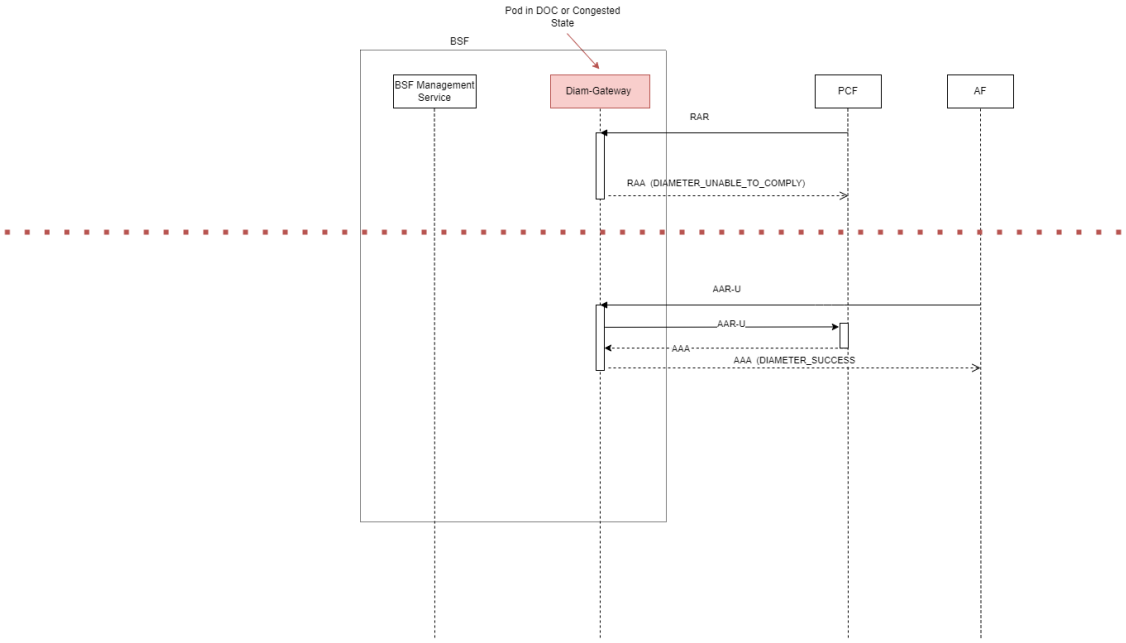
To understand how the diameter congestion control feature works, consider a scenario where the priority rules are configured as described in the following table:

Table 3-12 Priority Rules

Message	Priority
Default	6
RAR	10

For this call flow, discard priority is set as 10 for DOC and Congested state. The resulting code for rejecting request messages is set as DIAMETER_UNABLE_TO_COMPLY, that is applicable only for external peers.

Figure 3-23 Call flow diagram for Diameter Congestion Control



- When the Diameter Gateway is in DOC or Congested state, receives a RAR request, the priority is compared against discard priority. Since both message priority and discard the priority values are the same, the message is rejected with the DIAMETER_UNABLE_TO_COMPLY result code.
- When the Diameter Gateway is in DOC or Congested state, receives AAR request, the priority is compared against discard priority. Since no priority rule is configured for this message request, the message is accepted with the DIAMETER_SUCCESS result code.

Enable

The congestion control for diameter gateway pods is a functionality supported by Binding Support Function configurations. You do not need to enable or disable this feature.

Configure

You can customize the configurations related to this feature using the CNC Console or REST APIs for BSF.

- **Configure using CNC Console:** Perform the feature configurations on the Load Shedding Profiles and Message Priority Profiles page. For more information about the configurations, see Diameter Configurations.
- **Configure using REST API:** BSF provides the following REST API for configuring diameter gateway pod congestion control feature:
  Load Shedding Profiles: {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles

  Message Priority Profiles: {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypprofiles

  Congestion Threshold: {apiRoot}/oc-bsf-configuration/v1/threshold/{serviceType}

  You can perform the POST, PUT, or GET operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core Binding Support Function REST API Specification Guide*.

Observe

Binding Support Function uses the pod congestion metrics for this feature. For more information, see the Binding Support Function Metrics section. Alerts are raised when the following metrics are pegged:

- pod_congestion_state
- pod_resource_congestion_state

> **Note**
>
> Prometheus automatically injects name of the pod name with the label "kubernetes_pod_name" to the metric. This information is further used for alerting purposes.

Alerts
BSF uses the following congestion control alerts for this feature:

- PodDoC
- PodCongested
- PodPendingRequestDoC
- PodPendingRequestCongested
- PodCPUDoC
- PodCPUCongested
- PodMemoryDoC
- PodMemoryCongested

For more information, see the List of Alerts section.

Maintain

Warning logs are generated to indicate the congestion level. Error logs are generated when the system is congested and the actions are needed to be taken to bring the system back to normal. However, no error logs are generated when messages are rejected to avoid additional resource usage to write error logs.

3.23 Overload Control

Overload means when 100% of the planned capacity is exhausted. It can be due to uneven distribution of traffic towards a given policy service instance, network fluctuations leading to traffic bursts or unexpected high traffic volume at any given point of time.

During overload conditions, the service response times may grow to unacceptable levels, and exhaustion of resources can result in downtime or services exhibiting unexpected behavior. Overload management is a critical requirement for any telecom node, server, and service to protect against downtime and ensure serviceability during extreme overload conditions. Thus, overload management aims to prevent service performance from degrading in an uncontrolled manner under heavy loads. When BSF service starts approaching its saturation or planned limit, response times typically grow high and throughput may degrade substantially. Under such conditions, it is desirable to shed load based on the user's configuration, instead of causing all

messages and signaling flows to experience unacceptable response times, failures, or downtime.

BSF allows to configure a percentage of messages to be rejected. That is, messages are discarded based on configured percentage. This enables system's overload and congestion control to manage gauge system's load with better accuracy. Also, it allows the user to provide less rejections instead of providing 100% rejections.

Percentage of message rejections for each load level is configurable. Also, the rejection percentage for each message priority can be configured.

For example, if the discard value for CCR-I messages is 50% , when system is under load, only alternate CCR-I requests are processed rejected the rest. That is, 1st CCR-I is rejected and 2nd is accepted.

> **Note**
>
> All CCR-Ts are accepted.

Enable

To enable the overload control functionality, set value for the following parameter to `true` in the `custom-values.yaml` file for BSF:

- **perf-info.overloadManager.enabled**

Then, configure the values for the following parameters in the `custom-values.yaml` file:

```
perf-info:
  envMysqlDatabase: ''
  overloadManager:
    enabled: false
    ingressGatewaySvcName: occnp-ingress-gateway
    ingressGatewayPort: *svcIngressGatewayHttp
    # nfType is used to query configuration from common cfg server
    nfType: BSF
    # diam Gateway overload management feature configurations
    diamGWPort: *svcDiamGatewayHttp
```

For more information about setting the parameter values, see *Overload Manager Configurations* in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Configure

You configure the overload control feature either using CNC Console, or through REST API.

- **Configure using REST API:** BSF provides `overloadLevelThreshold` and `overloadLevelThresholdProfiles` API end points to configure overload control feature. You can perform the POST, PUT, or GET operations to configure the feature. For more information about REST API configuration, see *Overload Level Threshold Overload Level Threshold* sections in *Oracle Communications Cloud Native Core, Binding Support Function REST API Specification Guide*.
- **Configure using CNC Console**: Using CNC Console, you can configure the threshold values based on profiles. For more information, see Overload Control Threshold.

Recommended Overload Threshold Values - BSF Management Services

This section describes the recommended default overload threshold values for BSF Management Services. To calculate threshold values, you must consider the resource values for microservices. The following table lists the default resource values for BSF Management Services:

Table 3-13 Default Resource Values

Resources	Values
CPU (Limits)	4
CPU (Requests)	3
Maximum CPU Usage	1.6
Maximum CPU Usage (%)	61
Maximum Replicas	8
Maximum TPS	1500
Maximum TPS (all replicas)	12000
Worst RTT (assumed)	250 ms
Maximum Pending Transactions	2100

Based on the values in the aforementioned table, you can calculate the onset and abatement values for load levels - L1, L2, and L3, as shown in the following table:

Table 3-14 Formulas to Calculate Default Overload Threshold Levels

Load Level	CPU (%)	Pending Message Count (Absolute Value)	Failure Couunt (Absolute Value)
L1 - Onset	80% * C	60% * P	05% * T
L1 - Abatement	75% * C	50% * P	03% * T
L2 - Onset	90% * C	75% * P	10% * T
L2 - Abatement	85% * C	70% * P	08% * T
L3 - Onset	95% * C	90% * P	15% * T
L3 - Abatement	91% * C	85% * P	12% * T

Abatement value is the lower range where as the onset value is higher range for that particular level.

Note:

C denotes the maximum CPU utilization per pod of core-service

P denotes the maximum pending transaction size value based on worst RTT and max TPS, that is, 25K/s * 2000ms = 50000.

T denotes the maximum TPS of a given service.

> **Note**
>
> You can configure the memory for each of these services.

The following table lists the default overload threshold values for BSF Management Services:

> **Note**
>
> These are the recommended values. It can be modified as per the customer requirements.

Table 3-15 Default Overload Threshold Values - BSF Management Services

Load Level	CPU (%)	Pending Message Count	Failure Count
L1 - Onset	44	1260	420
L1 - Abatement	41	1050	252
L2 - Onset	49	1575	840
L2 - Abatement	47	1470	672
L3 - Onset	52	1890	1260
L3 - Abatement	50	1785	1008

Observe

BSF provides the following metrics specific to Overload Control feature:

- service_resource_stress
- service_resource_overload_level
- load_level
- system_overload_threshold_config_mode
- active_overload_threshold_fetch_failed

For more information, see Binding Support Function Metrics section.

Alerts

- BSF provides the following alerts for overload control feature on SBI interface:
  - `ServiceOverloaded` - This alert is raised whenever a given service is in overload state - L1, L2, and L3.
  - `ServiceResourceOverLoaded` - This alert is raised when a given service is in overload state - L1, L2, or L3 due to resource types such as memory, CPU, pending count, and failure count.
- BSF provides `PERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED` alert for overload control threshold configuration. This alert is raised when the service is unable to fetch the current active overload threshold data.

Maintain

Error logs are generated when the system is overloaded and the actions taken to bring the system back to normal. Warning logs are generated to indicate the change in load level.

3.23.1 Overload Control - Diameter

For Diameter Gateway, BSF provides the following means for overload management:

- Pre-defined threshold load levels.
- Tracks number of pending and failure messages from Diameter Gateway.
- Tracks CPU and memory usage of Diameter Gateway.
- Enforce load shredding during various overload levels based on priority and percentage discard value for each priority. The priority and pecentage discard value are configurable.

Configure

To configure the threshold values, discard priority, and error codes for the defined overload control levels, you may use CNC Console as well as REST API.

> **Note**
>
> Currently, threshold values can be configured using REST API only.

- **Configure using CNC Console:** Perform the feature configurations on the Load Shedding Profiles and Message Priority Profiles page. For more information about the configurations, see Load Shedding Profiles.
- **Configure using REST API:** BSF provides the following REST API for configuring Overload Control feature on Diameter Gateway:
  Load Shedding Profiles: {apiRoot}/oc-bsf-configuration/v1/diameter/loadsheddingprofiles

  Message Priority Profiles: {apiRoot}/oc-bsf-configuration/v1/diameter/messageprioritypro files

  You can perform the POST, PUT, or GET operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Binding Support Function REST API Specification Guide*.

The following are the recommended configurations for load shedding profile and message priority profile respectively for overload control:

```
{
  "name": "default_overload_control_load_shedding_profile",
  "type": "Overload Control",
  "overloadLoadSheddingRules": [{
    "level": "L1",
    "discardPriority": 13,
    "ansWithResultCode": "DIAMETER_TOO_BUSY"
  }, {
    "level": "L2",
    "discardPriority": 11,
    "ansWithResultCode": "DIAMETER_TOO_BUSY"
  }, {
    "level": "L3",
    "discardPriority": 6,
    "ansWithResultCode": "DIAMETER_TOO_BUSY"
  }]
}
```

```
{
  "name": "default_msg_priority_profile",
  "priorityRules": [{
```

```
    "ruleName": "Rx_AAR_I",
    "messagePriority": 13,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Rx",
      "message": "AAR",
      "preDefinedAVPConditions": [{
        "conditionName": "Rx-Request-Type",
        "conditionRxRTValue": ["INITIAL_REQUEST"]
      }]
    }
  }, {
    "ruleName": "Rx_STR",
    "messagePriority": 7,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Rx",
      "message": "STR",
      "preDefinedAVPConditions": []
    }
  }, {
    "ruleName": "Rx_AAR_U",
    "messagePriority": 11,
    "rulePriority": 1,
    "enableDRMPPriority": true,
    "conditions": {
      "application": "Rx",
      "message": "AAR",
      "preDefinedAVPConditions": [{
        "conditionName": "Rx-Request-Type",
        "conditionRxRTValue": ["UPDATE_REQUEST"]
      }]
    }
  }]
}
```

Observe

BSF provides the following metric specific to Overload Control feature:

- diam_overload_message_reject_total

For more information, see Binding Support Function Metrics section.

3.23.2 Overload Control - SBI

For HTTP signaling, BSF provides the following means for overload management:

- Pre-defined threshold levels
- Tracks number of pending messages for BSF service
- Tracks number of failed responses (configurable as error code) generated BSF service
- Tracks CPU and memory usage of BSF services

- Determines the overload level of the system using data collected from all the above mentioned points against planned threshold levels.
- Enforce load shedding at various overload levels

Configure

To configure the discard policies, Discard Policy mapping, and Error Code Profiles for overload control, you may use CNC Console as well as REST API.

> **Note**
>
> Currently, threshold values can be configured using REST API only.

- **Configure using CNC Console:** Perform the feature configurations on the Discard Policy Mapping, Discard Policy, and Error Code Profiles pages. For more information about the configurations, see Overload and Congestion Control Configurations.
- **Configure using REST API:** BSF provides the following REST APIs for configuring overload control feature on SBI interface:
  - **OC Policy Mapping**: {apiRoot}/BSF/nf-common-component/v1/igw/ocpolicymapping
  - **OC Discard Policies**: {apiRoot}/BSF/nf-common-component/v1/igw/ocdiscardpolicies
  - **Error Code Profiles**: {apiRoot}/BSF/nf-common-component/v1/igw/errorcodeprofiles

  You can perform the GET, PUT, or PATCH operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Binding Support Function REST API Guide*.

The following are the recommended configurations for default message priority values for overload control:

Table 3-16 Default Message Priority Values

Message Type	Priority
bsf_management_register	24
bsf_management_deregister	18
bsf_management_discovery	24

3.24 Rate Limiting - SBI

With the support for rate limiting, Ingress Gateway screens all configured routes and their respective rate limit configurations. Within the configured sampling period (configurable using CNC Console and REST APIs), Ingress Gateway calculates the rate for the required route along with the HTTP method. For BSF, the following routes and HTTP methods are supported:

- BSF Management Register - POST method
- BSF Management Deregister - DELETE method
- BSF Management Discovery - GET method

Then, it notifies the route level rate limiter with the calculated rate at the end of the sampling period. If the feature is enabled, any request with the sbi-priority header value greater than the configured value is discarded, and Ingress Gateway returns the error response with configured errorCode.

> **Note**
>
> Ingress Gateway determines the number of messages being dropped or rejected in the current sampling period based on extra unrejected messages received in the previous sampling period.

Managing Rate Limiting

Enable

Perform the following configurations to enable the rate limiting feature at Ingress Gateway:

- **CNC Console**: By default, this feature is disabled. To enable the rate limiting feature using CNC Console, set the **Enable Rate Limiting** parameter to `true` on the Rate Limiting Policy page.
- **REST API:** By default, this feature is disabled. To enable the rate limiting feature using REST API, set the `enabled` parameter to `true` in the following resource URI:

  Define rate limit: {apiRoot}/BSF/nf-common-component/v1/igw/routelevelratelimiting

  Define rate limit at route level: {apiRoot}/BSF/nf-common-component/v1/igw/routesconfiguration

  For more information, see *Rate Limiting at Ingress Gateway* section in *Oracle Communications Cloud Native Core, Binding Support Function REST API Guide*.

Configure

To configure the rate limiting policy, route level mapping, and error code profiles for rate limiting, you may use CNC Console as well as REST API.

- **Configure using CNC Console:** Perform the feature configurations on the Rate Limiting Policy, Route Level Mapping, and Error Code Profiles pages. For more information about the configurations, see Overload and Congestion Control Configurations.
- **Configure using REST API:** BSF provides the following REST API for configuring Overload Control feature on SBI interface:
  Define error code profiles: {apiRoot}/BSF/nf-common-component/v1/igw/errorcodeprofiles

  Define rate limit: {apiRoot}/BSF/nf-common-component/v1/igw/routelevelratelimiting

  Define rate limit at route level: {apiRoot}/BSF/nf-common-component/v1/igw/routesconfiguration

  You can perform the GET, PUT, or PATCH operations to configure the feature. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Binding Support Function REST API Specification Guide*.

3.25 Pod Protection at Ingress Gateway

This section describes how to protect the Ingress Gateway pods when they are overloaded with numerous incoming requests.

The Ingress Gateway pods are not protected against any incoming traffic congestion. As a result, the pods are overloaded and congested. This impacts system latency and performance. It also leads to stability issues due to uneven distribution of connections and traffic on Ingress Gateway pods. As a front end microservice for HTTP traffic, it is important for Ingress Gateway to have pod protection implemented.

To configure pod protection on Ingress Gateway, you can define threshold limit for DoC and Congested state through REST:

Table 3-17 Configuring Threshold Limit

Level	Resource
DoC	• CPU • Memory • Pending Message
Congested	• CPU • Memory • Pending Message

Configure

You need to perform the following configurations for pod protection feature:

- **Configure using REST API:** BSF provides the following REST API: {apiRoot}/BSF/nf-common-component/v1/igw/podprotection

  You can perform the GET, PATCH, or PUT operation to configure the feature. For more information about REST API configuration, see *Oracle Communications Binding Support Function REST API Specification Guide*.

3.26 Service Mesh for Intra-NF Communication

BSF leverages the Istio or Envoy service mesh (Aspen Service Mesh) for all internal and external communications. The service mesh integration provides inter-NF communication and allows API gateway co-working with service mesh. The service mesh integration supports the services by deploying a sidecar proxy in the environment to intercept all network communications between microservices.

The Aspen Service Mesh (ASM) configurations are classified into:

- Control Plane: It involves adding labels or annotations to inject sidecar.
- Data Plane: It helps in traffic management such as handling NF call flows by adding Service Entries (SE), Destination Rules (DR), Envoy Filters (EF), and other resource changes such as apiVersion change between versions. This is done manually depending on each NF requirement and ASM deployment.

Managing Service mesh for intra-NF Communication

Enable

To enable Aspen Service Mesh, configure the following parameters under nrf-client-nfdiscovery, ingress-gateway, egress-gateway, and alternate-route sections in the custom values file for BSF:

- serviceMeshCheck
- istioSidecarQuitUrl
- istioSidecarReadyUrl

For more information on enabling the parameter value, see "Aspen Service Mesh Configurations" in *Cloud Native Binding Support Function Installation and Upgrade Guide*.

Configure

The Aspen Service Mesh (ASM) configurations are classified into:

- Control Plane: For information on configuring the parameter value, see "Aspen Service Mesh Configurations" section in *Oracle Communications Cloud Native Binding Service Function Installation Guide*.
- Data Plane: For information about Data plane configurations, see "Aspen Service Mesh Data Plane Configurations" in *Cloud Native Binding Support Function Installation and Upgrade Guide*.

3.27 Automated Test Suite Support

BSF provides Automated Test Suite (ATS) for validating the functionalities. ATS allows you to run BSF test cases using an automated testing tool and compares the actual results with the expected or predicted results. The ATS requires no user intervention. For more information, see *Oracle Communications Cloud Native Core Automated Testing Suite Guide*.

3.28 SBI Error Codes

Oracle Communications Cloud Native Core Binding Support Function (BSF) can handle Protocol or Application errors and a few other additional defined errors for various scenarios. When BSF encounters an error in processing a request, it sends error codes in the response message to the request. With this enhanced functionality, BSF allows users to configure error codes by adding customized values, for a defined condition, for the following fields:

- Error Description
- HTTP Status Code
- Application Error Code

Configure

To configure error codes for BSF, users can use any of the following ways:

- **CNC Console**: Perform the configurations on the SBI Error Codes page. For more information, see SBI Error Codes Configurations.
- **REST API**: Perform the configurations using POST, PUT, or GET operations. For more information about REST API configuration, see *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Document*.

Observe

When BSF generates error codes, it also increments the associated metric, `ocbsf_ingress_response_total`. To support the SBI error codes feature, a new dimension, `application_error_code` is added to the metrics to enable the user to easily identify the failed message or procedure and the associated error code. Metrics also include the consumer (IP or FQDN) to whom the error would be sent. For more details, see Binding Support Function Metrics.

On generating error codes, logs are updated as well.

The following is a sample error log when optional parameter in binding data is invalid:

```
{
  "instant": {
    "epochSecond": 1628086282,
    "nanoOfSecond": 772064777
  },
  "thread": "XNIO-1 task-1",
```

```
  "level": "DEBUG",
  "loggerName": "ocpm.bsf.api.management.metrics.BsfMetrics",
  "message": "Pegging the Ingress Response Metric for Operation Type :
register, Response Code ProblemDetails [type=about:blank, title=Optional
parameter in binding data is invalid, status=411,
cause=OptionalInformationElementIsIncorrect, instance=http://b-ocbsf-ingress-
gateway.b/nbsf-management/v1/pcfBindings, details=Parameters in the request
is not correct , invalidParams=[InvalidParam {\n    param: pcfDiamRealm\n
reason: must match \"^([A-Za-z0-9]+([-A-Za-z0-9]+)\\.)+[a-z]{2,}$\"\n}]]",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 31,
  "threadPriority": 5,
  "messageTimestamp": "2021-08-04T14:11:22.772+0000"
}
```


Result: As mentioned in the `message` field of the sample log, the metric `ocbsf_ingress_response_total` is pegged.

3.29 Handling Stale Session in BSF

Overview

A session binding on BSF is considered as stale when the PCF binding is successfully registered on BSF but has no corresponding session on PCF. When you enable stale session handling feature, the Audit service detects stale sessions automatically at regular intervals.

During the audit, if the audit service finds records with a binding age greater than the configured value (default value is 3600 minutes), it marks such records as suspected stale and initiates a request to notify the BSF management service. Depending on the feature configurations, BSF may query PCF to confirm if the pcfBinding records are stale. If PCF confirms the record as stale, then BSF removes it from its local database. However, if PCF sends 2xx in the response, then BSF updates the last access time for the associated pcfBinding record.

If the audit service finds a pcfBinding record with binding age greater than the maximum binding age (default value is 7200 minutes), it notifies the BSF Management service. On receiving the notification, BSF deletes the specified record from its database.

For georedundant BSF deployments, binding records are replicated to other redundant sites after the audit cycle is complete. Logs are published when audit service detects and removes stale sessions.

Query PCF to confirm a record as stale
To query PCF for confirming stale pcfBinding records, BSF supports receiving vendor-specific-attribute in the binding register request. So, when PCF sends a register request to BSF for binding creation, it includes the notification URL in the vendor-specific-attribute, as shown below:

```
"vendorSpecific-000111": {
    "version": 1,
    "notificationUrl": "<PCF Notification Url>",
    "createBindingTime": "<Timestamp>",
  }
```

BSF, in turn, uses this notification URI to send audit notification towards Binding service on PCF. When PCF receives the notification, it checks whether any binding record exists by sending a query to the Query service using contextId (SmPolicyAssociationId). Based on the findings, PCF sends 2xx response if session exists and 404 if the session does not exist.

Enable

After performing the required Helm configurations, you can enable the handling stale sessions in BSF using the CNC Console or REST API.

- **Enable using Helm:** To enable this feature during BSF deployment, set the value of `auditServiceEnable` parameter as `true` in the `ocbsf-22.2.0-custom-values.yaml` file. Once the Audit service is enabled, set appropriate values for the following parameters:
  - global.servicePorts.auditServiceHttp
  - global.containerPorts.auditServiceHttp
  - audit-service.envMysqlDatabase

  For more information on how to customize these parameters, see *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
- **Enable using CNC Console:** To enable this feature, on the Management Service page, under the **Audit** group, set the value of **Enabled** field as true. For more information about enabling the feature through CNC Console, see Service Configurations.
- **Enable using REST API:** Set the **audit.enable** parameter value to **true** in the Management Service configuration API. For more information about enabling the feature through REST API, see the "Management Service" section in *Oracle Communications Core Binding Support Function REST Specification Guide*.

Configure

You can configure the Stale Session Handling functionality for BSF using the CNC Console or REST API.

- **Configure using CNC Console:** Perform the feature configurations on the **Management Service** page. For more information, see Service Configurations.
- **Configure using REST API:** BSF provides the following REST API for Stale Session Handling configuration:
  API: {apiRoot}/oc-bsf-configuration/v1/services/managementservice

  You can perform the GET and PUT operations to configure this feature. For more information about REST API configuration, see the "Management Service" section in *Oracle Communications Core Binding Support Function REST Specification Guide*.

Observe

BSF provides the following metrics for stale session handling feature:

- ocbsf_audit_notif_request_count_total
- ocbsf_audit_notif_response_count_total
- ocbsf_audit_delete_records_count_total
- ocbsf_diamgw_notification_request_count_total
- ocbsf_diamgw_notification_response_count_total
- ocbsf_query_request_count_total
- ocbsf_query_response_count_total

- ocbsf_bindingQuery_request_total
- ocbsf_bindingQuery_response_total
- ocbsf_bindingDelete_request_total
- ocbsf_bindingDelete_response_total

For more information, see the **BSF Management service** and **Audit service** metrics in the Binding Support Function Metrics section.

Maintain

BSF generates logs when audit service detects and removes stale sessions automatically. In addition, logs are printed for query requests towards PCF and the associated responses.

3.30 Support Multiple Cluster Deployment at CNC Console

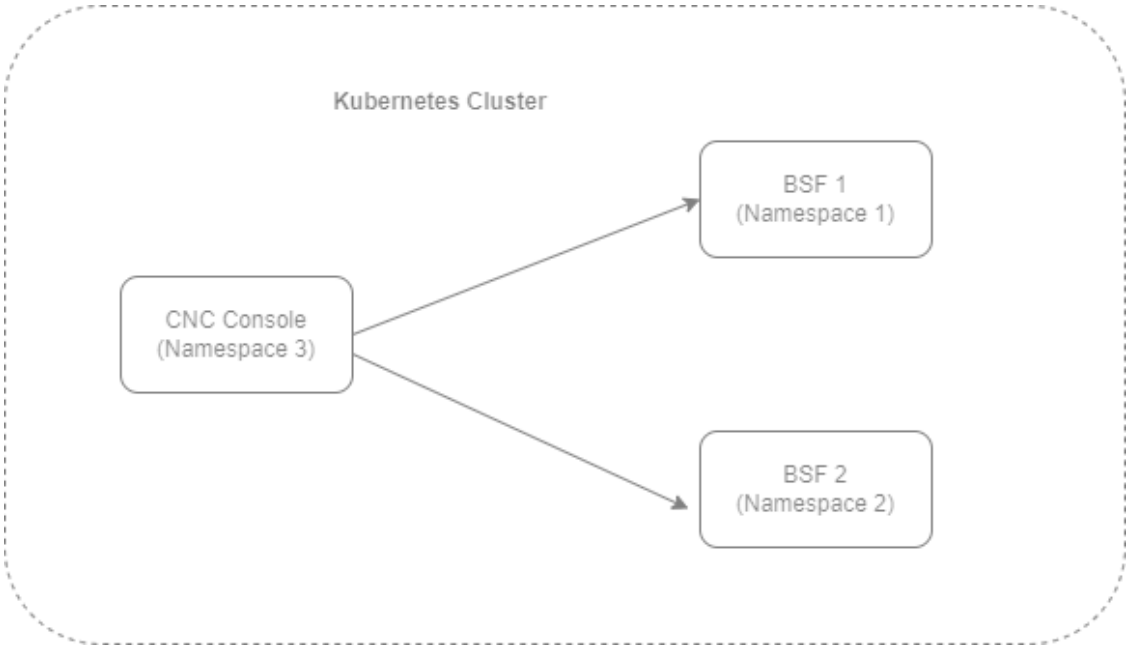
The CNC Console supports both single and multiple cluster deployments.

In a single cluster deployment, the CNC Console can manage NFs and Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) common services deployed in the local Kubernetes clusters.

In a multiple instances deployment, the CNC Console can manage multiple BSF instances and CNE common services deployed within a Kubernetes cluster. For more information about single and multiple cluster deployments, see *Oracle Communications Cloud Native Core, Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

The following image represents a Kubernetes cluster with one instance of CNC Console and two instances of BSF. The single instance of the CNC Console is configuring two instances of BSF with different namespaces.

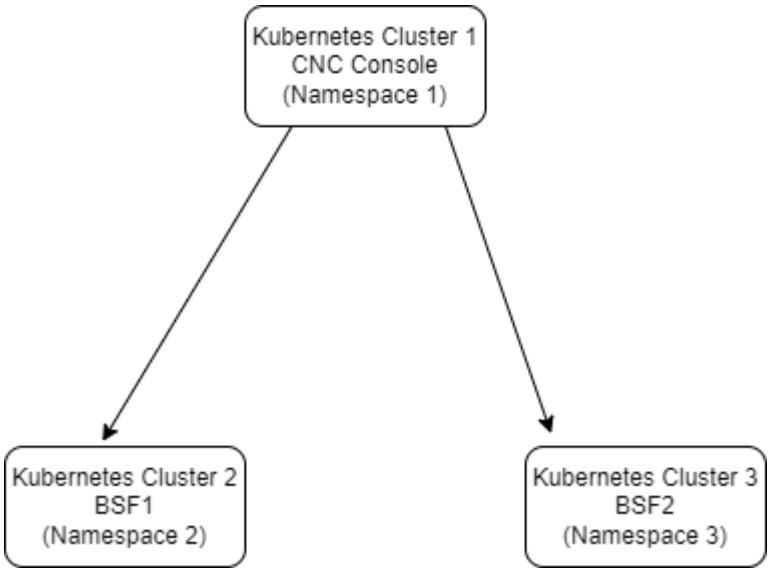
Figure 3-24 Support for Multiple Instance Deployment



With the support of multicluster deployment, BSF deployed in multiple Kubernetes clusters can be accessed using CNC Console. In a multicluster deployment, the CNC Console can manage BSF and OCCNE common services deployed in the remote Kubernetes clusters.

The following image represents multiple Kubernetes clusters with one CNC Console and two BSF deployments. The single instance of CNC Console is configuring two instances of BSF with different namespaces deployed in different clusters.

Figure 3-25 Support for Multicluster Deployment



3.31 Support for 3GPP NF Sets and Binding Headers

Oracle Communications Cloud Native Core Binding Support Function supports the 3GPP NF Sets and Binding Headers in Model-B (Direct communication) and Model-C (Indirect communication). Using this feature, BSF can construct and send a binding header in the response messages to PCF for successful call processing.

> **Note**
>
> Since BSF is a producer NF, it does not send any notifications to consumer NFs. BSF sends an HTTP request message only to NRF for management purpose.

NF Set: NF set is a group of interchangeable NF instances supporting similar services and network slices. In an NF set, the NF instances can be geographically distributed, but have access to the same context data. The NF instances can be deployed in such a pattern so that several instances are present within an NF set to provide distribution, redundancy, and scalability as a set. The NF instances of an NF set are equivalent and share the same MCC, MNC, NID (for SNPN), NF type, and NF Set ID.

Binding Headers: The Binding headers indicate the suitable target NF producer instance for NF service instance selection, reselection, and routing of subsequent requests associated with a specific NF producer resource or context. It allows the NF producer to indicate that the NF consumer, for a particular context, should be bound to an NF service instance, or NF set depending on local policies. Binding can also be used by the NF consumer to indicate the

suitable NF consumer instances for notification target instance reselection and routing of subsequent notification requests, associated with a specific notification subscription.

BSF supports the following binding header as defined in 3GPP:

Table 3-18 Supported Headers

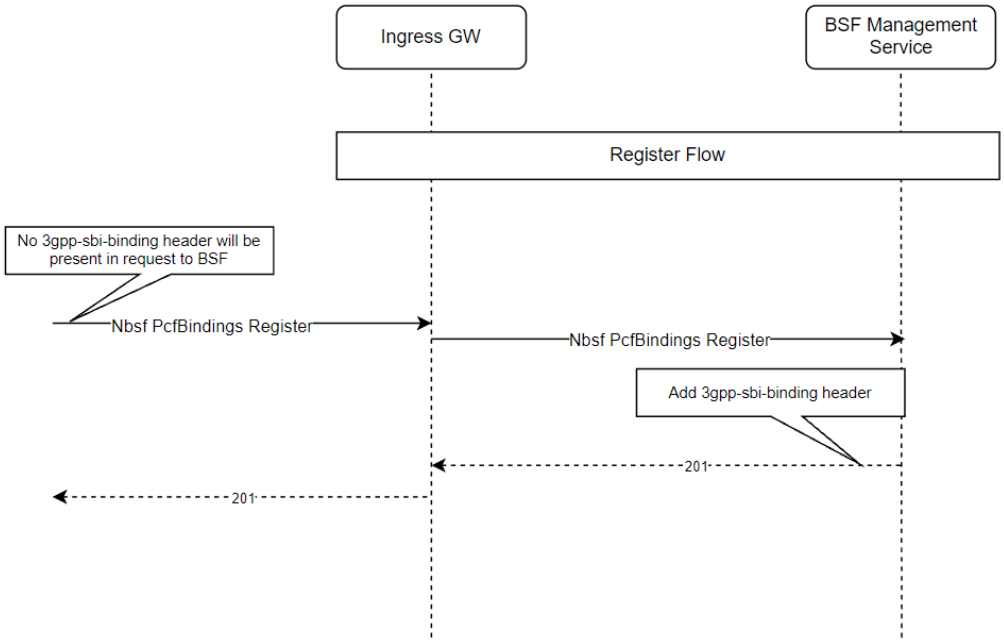
Header Name	Description
3gpp-Sbi-Binding	This header is used to communicate the binding information from an HTTP server for storage and subsequent use by an HTTP client. This header contains a comma-delimited list of Binding Indications from an HTTP server for storage and use of HTTP clients. The absence of this parameter in a Binding Indication in a service request is interpreted as "callback". **Note**: In the current release, the following are not supported: • Binding levels – `nfservice-instance` and `nfservice-set` • Attributes – `recoverytime` and `notif-receiver`

Binding Support Function supports the NF Set and Binding Header functionality in all SBI interfaces.

Example

The following diagram depicts an example where communication between PCF and BSF Management service takes place:

Figure 3-26 Example of NF Set and Binding Header in BSF



The above call flow diagram describes a scenario where PCF sends a request to register PcfBindings towards the BSF Management service through Ingress Gateway. The register request does not contain a `3gpp-sbi-binding` header.

Once the request is received at BSF, the BSF Management service adds `3gpp-sbi-binding` to the response and sends it back to the PCF with HTTP status code 201.

If the user does not want to add a binding header to response messages, then it can be configured through CNC Console or REST APIs for BSF.

Managing NF Sets and Binding Header Support

Enable and Configure

The NF Sets and Binding header support can be enabled and configured for the BSF Management service interface using any of the following two ways:

- **Using CNC Console:** Perform the feature configurations on the Management Service page. For more information about the configurations, see Service Configurations.
- **Using REST API:** BSF provides the following REST API for NF Sets and Binding Headers configuration:
  API: {apiRoot}/oc-bsf-configuration/v1/services/managementservice

  You can perform the GET and PUT operations to configure this feature. For more information about REST API configuration, see the "Management Service" section in *Oracle Communications Cloud Native Core Binding Support Function REST Specification Guide*.

Observe

BSF uses the Ingress metrics to contain information about the NF bindings used by PCF. The following metrics contains the information about NF bindings used by PCF:

- `ocpm_ingress_request_total` with the new dimensions – `pcf_id` and `pcf_set_id`

  > **Note**
  >
  > The dimensions are populated only for Nbsf_Management_Register requests.

- `ocpm_ingress_response_total` with the new dimensions – `binding_level` and `binding_id`

For more information, see the Binding Support Function Metrics section.

Maintain

The BSF logs include the NF binding information sent by BSF. The logs include information about the following headers:

- `location`
- `3gpp-sbi-binding`

The following is a sample log for PCF binding register request:

```
{
  "instant": {
    "epochSecond": 1636550691,
    "nanoOfSecond": 280882458
  },
  "thread": "XNIO-1 task-1",
  "level": "DEBUG",
  "loggerName":
```

```
"ocpm.bsf.api.management.controller.BindingSupportManagementServiceAPIControll
er",
  "message": "PCF binding: PcfBinding [supi=imsi-411411000000011,
gpsi=5084948001, ipv4Addr=10.10.10.16, ipv6Prefix=null, ipDomain=null,
macAddr48=null, dnn=internet, pcfFqdn=pcf-smservice.oracle.com,
pcfIpEndPoints=null, pcfDiamHost=pcf-smservice.oracle.com,
pcfDiamRealm=oracle.com, snssai=Snssai [sst=11, sd=abc123],
pcfId=fe7d992b-0541-4c7d-ab84-c6d70b1b0123,
pcfSetId=setxyz.pcfset.5gc.mnc015.mcc345, bindLevel=NF_SET]",
  "endOfBatch": false,
  "loggerFqcn": "org.apache.logging.slf4j.Log4jLogger",
  "threadId": 45,
  "threadPriority": 5,
  "messageTimestamp": "2021-11-10T13:24:51.280+0000"
}
```


3.32 Support for User-Agent Header

User-Agent header helps the producer Network Function (NF) to identify the consumer NF that has sent the request. To implement this, 3GPP introduced the use of User-Agent header for consumers to include the same in service requests. Additionally, producers may require to support the validation of the User-Agent headers to complete the request identification process in the network.

With the integration of this feature, User-Agent header helps the producer Network Function (NF) to identify the consumer NF that has sent the request.

The following format is used to generate User-Agent header:

<NF Type>-<Instance-Id> <FQDN>

where, `<NF Type>` is the type of the Network Function.

`<Instance-Id` is the instance ID of the NF.

`<FQDN>` is the FQDN of the NF.

Example: `BSF-54804518-4191-46b3-955c-ac631f953ed8 bsf1.east.5gc.mnc012.mcc234.3gppnetwork.org`

Following validations are made once the feature is enabled:

- If the user-agent header is present, then it is matched with the configured NF types. If a match is found, then validation is successful and request is allowed to pass. If a match is not found, then request is rejected with a configurable error code.
- If the user-agent header is present and has multiple values, then the request is rejected with a configurable error code. Hence, the user-agent header, if present should have a single value.
- If the user-agent header is not present and validationType is `relaxed`, then validation is not made and request is allowed to pass. If validationType is `strict`, then request will be rejected with a configurable error code.

Managing Support for User-Agent Header in Ingress Gateway

Enable

You can enable the User-Agent Header feature using REST or Helm configuration.

- Helm: Set the value of the parameter `userAgentHeaderValidationConfigMode` to Helm in the custom-values.yaml file. For more information, see the *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
- REST API: Set the value of the parameter `userAgentHeaderValidationConfigMode` to REST in the custom-values.yaml file. REST configuration from the JSON bodies sent to path: "*/bsf/nf-common-component/v1/igw/useragentheadervalidation*" is stored in a database under the common_config table. For more information, see the *Oracle Communications Cloud Native Core Binding Support Function REST Specification Guide*.

Configure

You can configure the User-Agent Header using REST or Helm.

To configure User-Agent header at Ingress Gateway using Helm, you need to perform the configurations:

```
#User-Agent header validator configuration
#Mode of configuration. Can be either HELM or REST
userAgentHeaderValidationConfigMode: HELM
userAgentHeaderValidation:
  enabled: true
# If User-Agent header is not present or it's value is null in the incoming
request then
validation type can be used to skip or perform validation. If set to strict
then validation will be performed.
# If set to relaxed then validation will be skipped.
 validationType: relaxed
# List of consumer NF Types to be matched against the value of User-Agent
header in the request
 consumerNfTypes:
   - "SMF"
   - "AMF"
   - "UDR"
      ...
```

To configure the User-Agent header at Ingress Gateway using REST API, see user-Agent Header in *Oracle Communications Cloud Native Core Binding Support Function REST Specification Guide*.

Managing Support for User-Agent Header in Egress Gateway

Enable

You can enable the User-Agent Header feature using REST or Helm configuration.

- Helm: Set the value of the parameter `userAgentHeaderConfigMode` to Helm in the custom-values.yaml file. For more information, see the *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.
- REST API: Set the value of the parameter `userAgentHeaderConfigMode` to REST in the custom-values.yaml file. REST configuration from the JSON bodies sent to path: "*/bsf/nf-common-component/v1/egw/useragentheader*" is stored in a database under the common_config table. For more information, see the *Oracle Communications Cloud Native Core Binding Support Function REST Specification Guide*.

Configure

You can configure the User-Agent Header using REST or Helm.

To configure User-Agent header at Egress Gateway using Helm, you need to perform the configurations:

```
userAgentHeaderConfigMode: HELM
userAgentHeader:
  enabled: false # flag to enable or disable the feature
  nfType: "PCF" # NF type of consumer NF
  nfInstanceId: "2d8e8e68-24ad-11ed-861d-0242ac120002" # NF type of consumer
NF
  addFqdnToHeader: true # Flag to add fqdn. If enabled then user-agent header
will be
generated along with the fqdn configured otherwise fqdn will not be added
  nfFqdn: "oracle1.pcf.pacific.org" #fqdn of NF. This is not the fqdn of
gateway
  overwriteHeader: true

oauthClient:
  enabled: false
  nfInstanceId: fe7d992b-0541-4c7d-ab84-c6d70b1b01b1
  nfType: PCF
```

To configure the User-Agent header at Egress Gateway using REST API, see user-Agent Header in *Oracle Communications Cloud Native Core Binding Support Function REST Specification Guide*.

Observe

BSF provides the following metric specific to User-Agent Header feature:

- oc.ingressgateway.http.requests

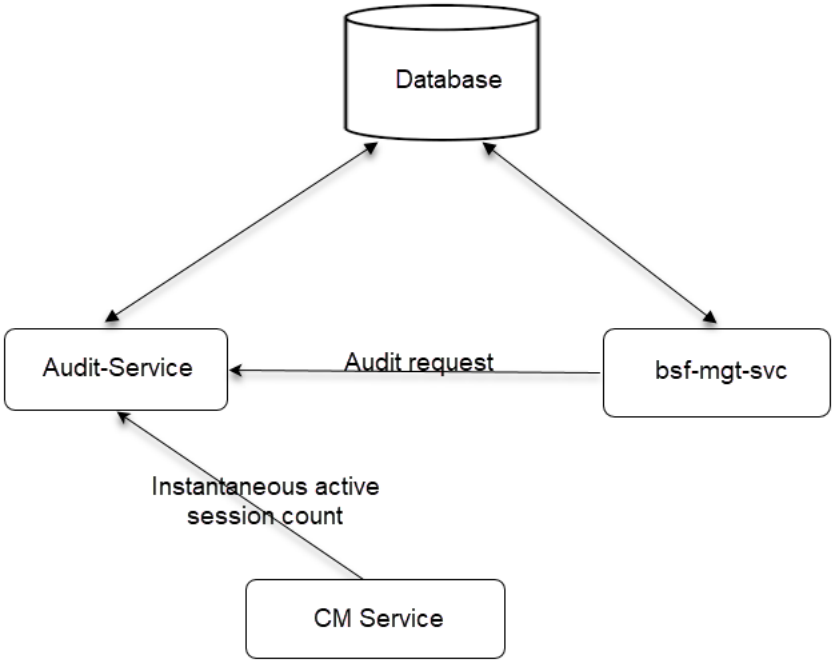
For more information, see User-Agent Header Metrics section.

3.33 Support for Active Sessions Counter

Active sessions are the unique PCF binding sessions in every BSF instance.

> **Note**
>
> The active sessions count also includes stale sessions until BSF removes it from its local database.
>
> For more details on how stale sessions are handled, see Handling Stale Session in BSF.

Figure 3-27 Retrieving Active Sessions Count

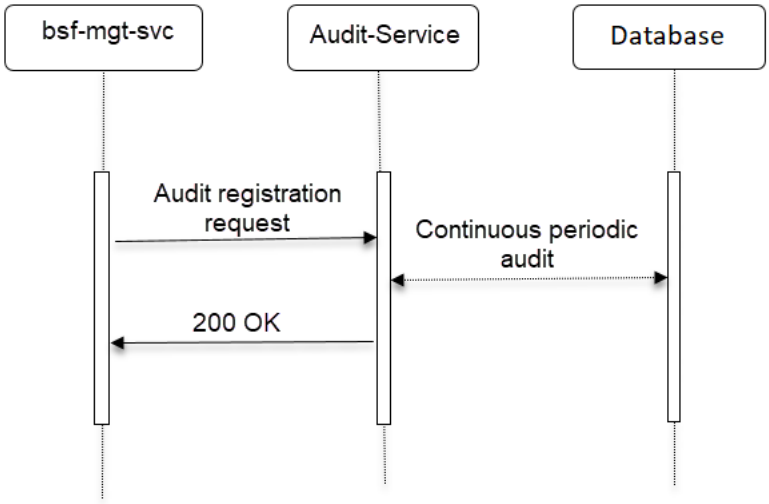


The Audit-Service periodically counts the simultaneous unique active sessions, over a configurable period of time. The default value of the time period is set to 15 mins. The time period can be configured to any value between 1 to 60 minutes.

The `bsf-mgt-svc` requests the Audit-Service to count active sessions for configurable time period. The Audit-Service periodically finds active sessions count and publishes the count as a metric.

To get the instantaneous value of active sessions count, you can query the CM service, which internally calls Audit-Service to fetch the value.

Figure 3-28 Active Sessions Count



> **Note**
>
> The audit registration process is used to register for audit registration as well as to enable active sessions counting.

The `bsf-mgt-svc` sends an audit registration request to the Audit-Service.

If the registration is successful, the Audit-Service responds with a 200 OK message.

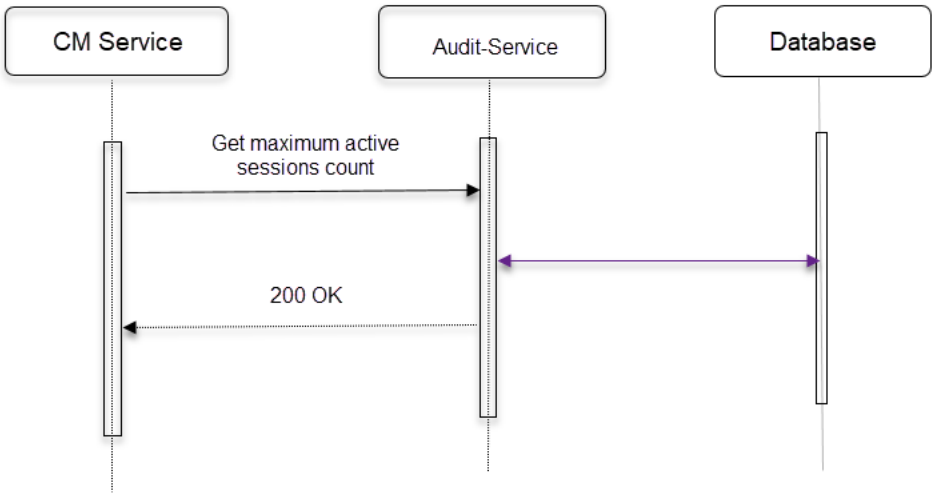
If the registration fails due to any issue with the request, the Audit-Service responds with a Bad Request - 400 message.

If the registration fails due to any other internal reason while processing the request, the Audit-Service responds with an Internal Server Error - 500 message.

> **Note**
>
> Audit registration is not required for CM Service to query the instantaneous active sessions count.

Once the registration is successful, the Audit-Service periodically finds active sessions count and publishes the count as a metric.

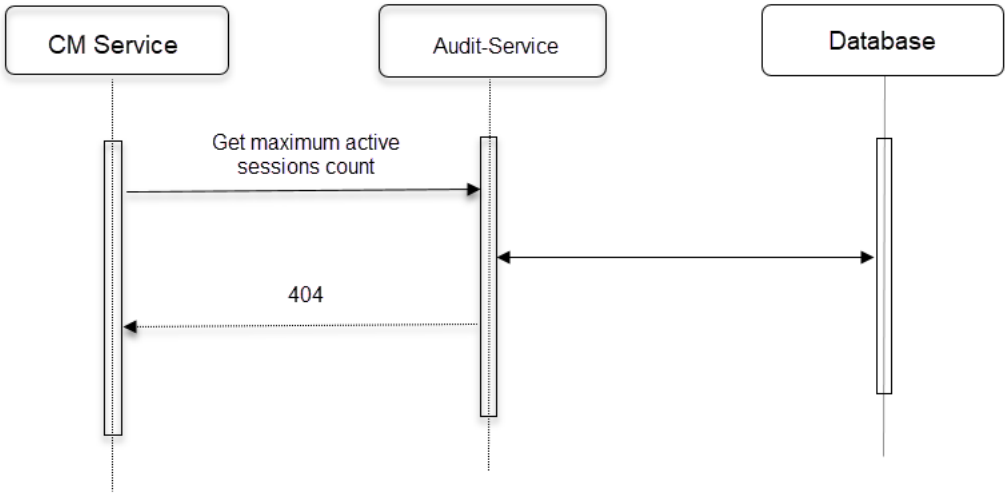
Figure 3-29 Get Instantaneous Active Sessions Count - Successful



The `CM Service` sends a Get maximum active sessions count request to Audit-Service.

If the CM Service call to Audit-Service is successful, it responds with a 200 OK message.

Figure 3-30 Get Instantaneous Active Sessions Count - Failure



If the CM Service call to Audit-Service fails, it responds with a 404 message.

ENABLE

You can enable the Active Sessions Counter feature using CNC Console or REST API.

- **Using CNC Console**: Set the value of **Count Active Sessions** parameter to `true` on **Active Sessions Counting** page. For more details, see *Active Sessions Count* under Service Configurations section.
- **Using REST API**: BSF provides the following REST API for Active Sessions Counter configuration:
  API: {apiRoot}/oc-bsf-configuration/v1/services/managementservice

  You can perform the GET and PUT operations to configure this feature.

  To enable the feature, set the value of `activeSessionCounting.countRecords` parameter to `true`.

  For more details, see *BSF REST Specifications* section in *Oracle Communications Cloud Native Core Binding Support Function REST Specification Guide*.

For more information, see Active Session Query.

Configure

You can configure the Active Sessions Counter feature using CNC Console or REST API.

- **Using CNC Console**: Set the value of **Session Count Interval (in minutes)** parameter on **Active Sessions Counting** page. You can set the time interval to any value between 1 to 60 minutes. For more details, see *Active Sessions Count* under Service Configurations section.

  For instantaneous query, use the **Active Session Query** tab under **Status and Query** in CNC Console.

  For more information, see Active Session Query.
- **Using REST API**: BSF provides the following REST API for Active Sessions Counter configuration:
  API: {apiRoot}/oc-bsf-configuration/v1/services/managementservice

  You can perform the GET and PUT operations to configure this feature.

  To configure the feature, set the value of `activeSessionCounting.countRecordsInterval` parameter.

  For instantaneous query, BSF provides the following REST API:

  API: {apiRoot}/oc-bsf-configuration/v1/activeSessionCount/pcfBindings

  You can perform the GET operation to retrieve the instantaneous active sessions count.

  For more details, see *BSF REST Specifications* section in *Oracle Communications Cloud Native Core Binding Support Function REST Specification Guide*.

Observe

BSF provides the following metric specific to Active Sessions Counter feature:

- oc_db_active_session_count
- inbound_requests_total

For more information, see Active Sessions Count Metrics.

3.34 Controlled Shutdown of an Instance

CNC BSF supports controlled shutdown feature to provide the partial or complete isolation of the site from the network so that the operator can perform necessary recovery procedures

when required. It helps the operator to perform the recovery procedures as per the requirement.

The site isolation is achieved by shutting down the load at gateways (Ingress Gateway, Egress Gateway, and Diameter Gateway) and updating the NF status as SUSPENDED at NRF.

Operational State

The site can be in one of the three possible operational states NORMAL, PARTIAL SHUTDOWN, or COMPLETE SHUTDOWN. The operational state can move to any of the states from the current state, there is no definitive order of state change. Currently, the operational state is stored in the common config server of the Ingress Gateway. It is read by Ingress Gateway, Egress Gateway, Diameter Gateway, and App-info periodically and action is triggered based on the current state.

> **Note**
>
> Since the operational state is stored in config server, the service instances will detect the state change after the config refresh is done. If the config refresh interval is set as 5 seconds, then the pods may recognize the operational state change after 5 seconds.

The operational state can be modified through CNC Console or REST API. Operation state configuration stored in the common config server will be read by the following services:

- Ingress Gateway
- Egress Gateway
- Diameter Gateway
- App-info

> **Note**
>
> If the Disaster Recovery procedure is performed when the config backup was taken when the system was in PARTIAL or COMPLETE SHUTDOWN state, then manual intervention may be required to change the operational state back to NORMAL state.

Load Control

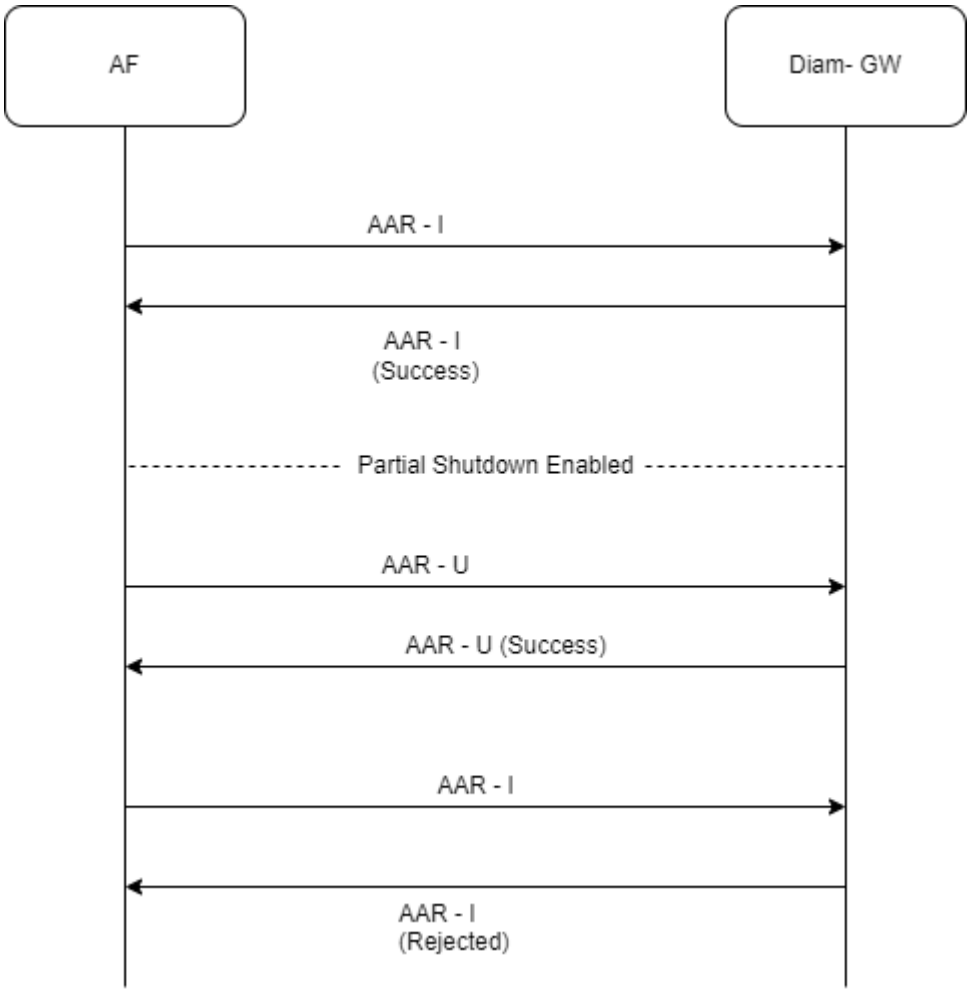
Gateways enforce load control when the system is in a PARTIAL or COMPLETE shutdown state. The level of load control varies based on the shutdown state. When in a PARTIAL shutdown state, no new session establishments are allowed so session creation messages will be rejected (with configured error code) in this state. When in complete shutdown, no messages are allowed.

> **Note**
>
> When the system is in COMPLETE SHUTDOWN state, audit service triggered notification or diameter messages will be rejected at respective gateways.

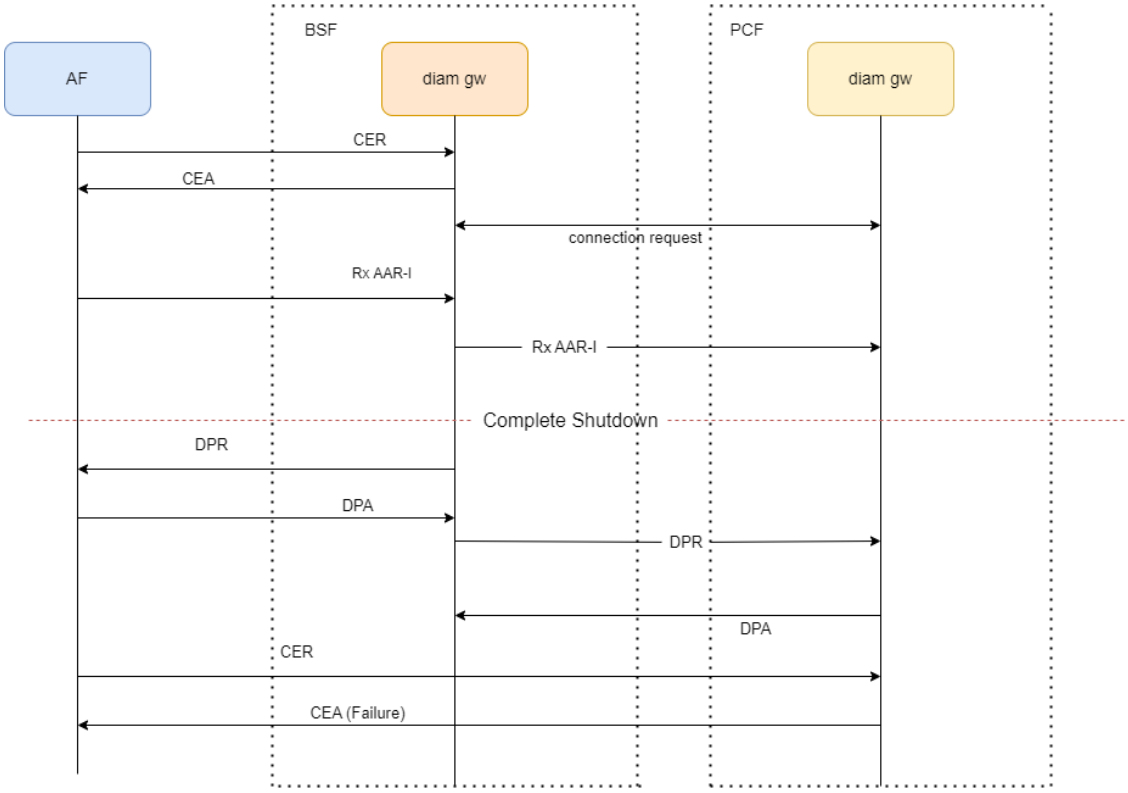
Call Flow for Daimeter Gateway

NORMAL State: If the Controlled shutdown operational state is NORMAL, then the Diameter Gateway processes the message as normal.

PARTIAL SHUTDOWN: If the controlled shutdown operational state is PARTIAL SHUTDOWN, then the Diameter Gateway accepts only in-session messages and rejects all CCR-I and AAR-I messages.



COMPLETE SHUTDOWN: If the controlled shutdown operational state is COMPLETE SHUTDOWN, then the Diameter Gateway accepts only in-session messages and rejects all messages.



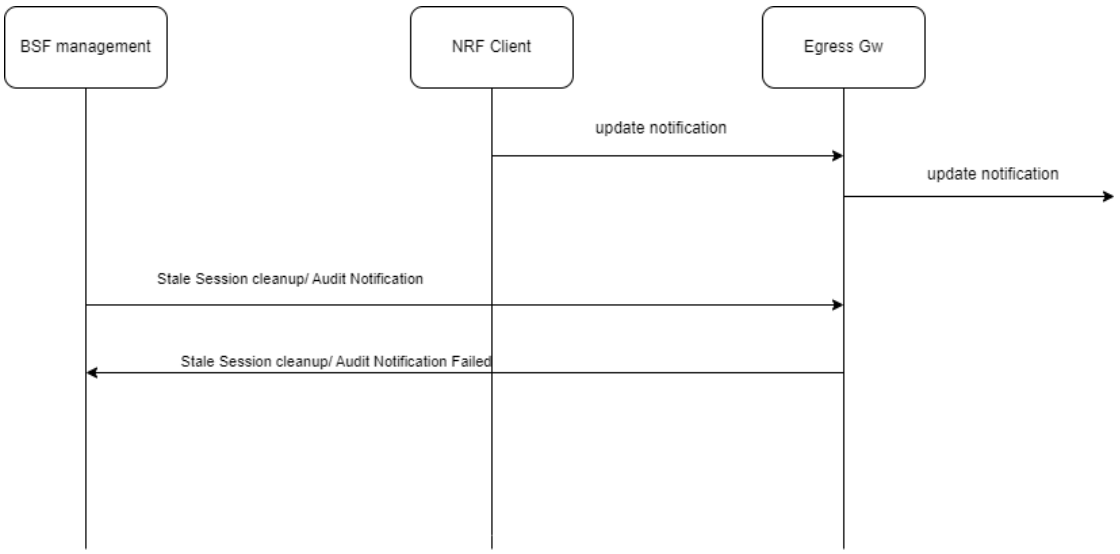
Call Flow for Egress Gateway

NORMAL State: If the Controlled shutdown operational state is NORMAL, then the Egress Gateway processes the message as normal.

PARTIAL SHUTDOWN: If the controlled shutdown operational state is PARTIAL SHUTDOWN, then the Egress Gateway processes the message as normal.

COMPLETE SHUTDOWN: If the controlled shutdown operational state is COMPLETE SHUTDOWN, then the Egress Gateway processes the request as follows:

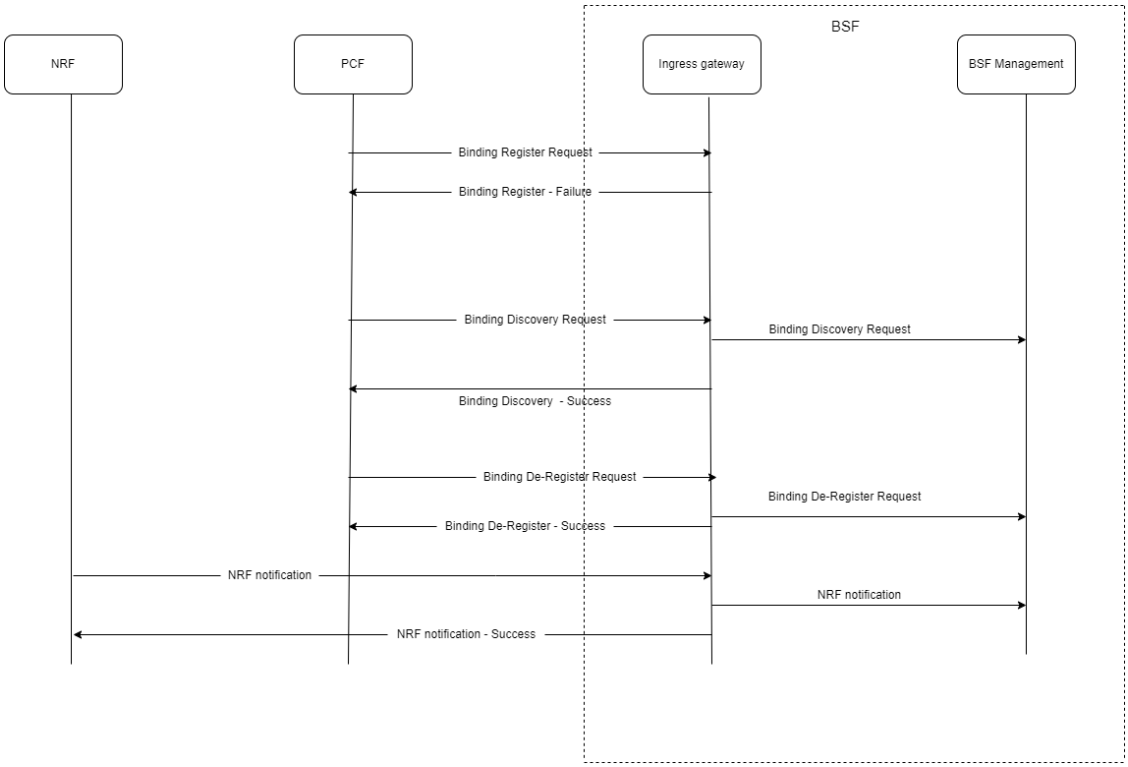
- Forward all requests received from NRF Client.
- Reject all requests received from any other services like UDR Connector, SM Service, AM Service, UE Service, and CHF Connector.



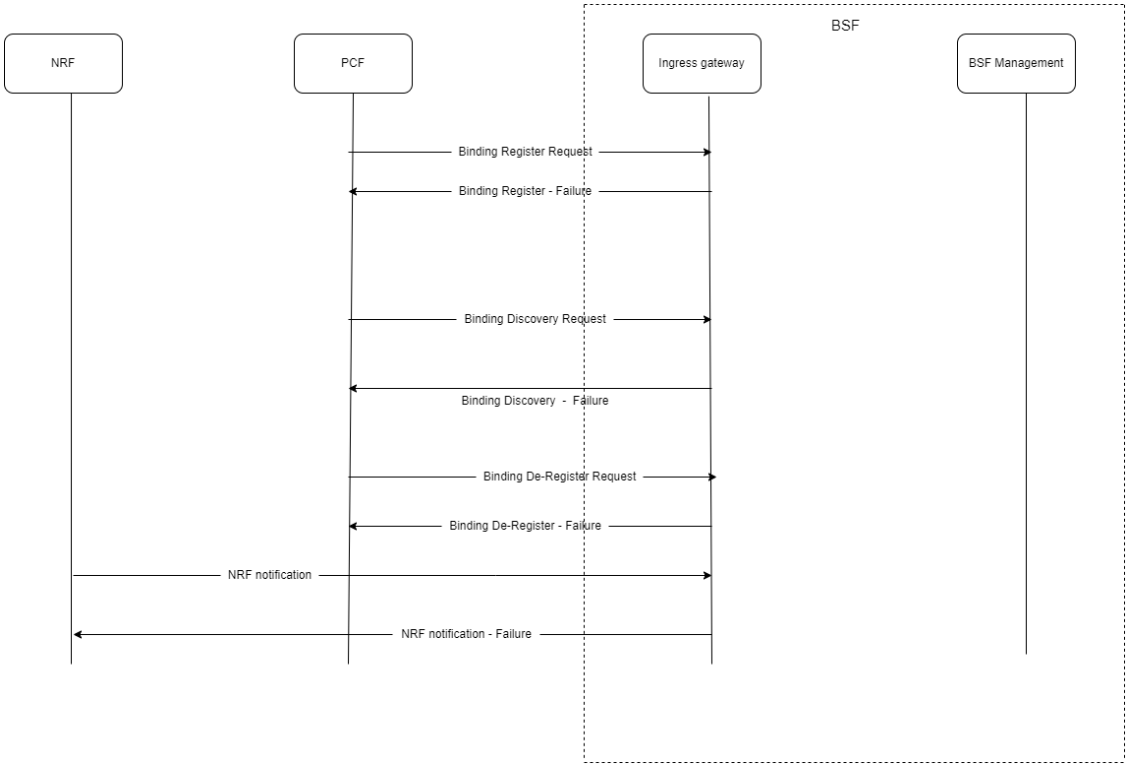
Call Flow for Ingress Gateway

NORMAL State: If the Controlled shutdown operational state is NORMAL, then the Ingress Gateway processes the message as normal.

PARTIAL SHUTDOWN: If the controlled shutdown operational state is PARTIAL SHUTDOWN, then the Ingress Gateway accepts only in-session messages and rejects all SM-Create requests.



COMPLETE SHUTDOWN: If the controlled shutdown operational state is COMPLETE SHUTDOWN, then the Ingress Gateway rejects all incoming requests.



Managing Controlled Shutdown of an instance

Enable

You can enable or disable the Controlled Shutdown feature by using the `enableControlledShutdown` parameter in the custom.yaml file. This parameter is set as `false` by default. You can enable it by setting its value as `true`. For more information, see *Controlled Shutdown Configurations* section in the *Oracle Communications Cloud Native Binding Support Function Installation and Upgrade Guide*.

Configure

Diameter Gateway and Ingress Gateway can be configured through CNC Console. For more information, see Controlled Shutdown Configurations.

Egress Gateway routes configuration for controlled shutdown is done through Helm. For more information, see the *Controlled Shutdown Configurations* section in the *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.

Observe

Metrics

CNC BSF provides the following metrics specific to controlled shutdown feature:

- system_operational_state
  For more information, see CM Service Metrics.
- diam_controlled_shutdown_message_reject_total
  For more information, see Diameter Gateway Metrics.

Alerts

CNC BSF provides the following alerts for controlled shutdown feature:

- SYSTEM_IMPAIRMENT_MAJOR
- SYSTEM_IMPAIRMENT_CRITICAL
- SYSTEM_OPERATIONAL_STATE_NORMAL
- SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN
- SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN

For more information, see BSF Alerts.

3.35 Graceful Termination of Kubernetes Pods

This feature is to support BSF NF's Kubernetes pods to terminate gracefully to reduce traffic loss.

In Kubernetes cluster, pods can get deleted due to various events. Few problems that can arise with abnormal termination:

1. A pod that is currently in the middle of processing a request is removed, leads to incomplete processing.
2. Kubernetes routes traffic to pods that have already been deleted, resulting in stale session at local or peer user.
3. The corruption of data in cache or database.

BSF services handles graceful termination of HTTP2 connections by

- accepting new request, but sends an immediate 503 service unavailable response to the clients.
- wait for ongoing response messages to complete the session.
- terminate the TCP connections and any DB transactions gracefully.

The applications performs all the above tasks before termination of the pod or before the grace period expires. If the grace period expires, and the process hasn't gracefully shutdown, the container runtime will force kill, stopping the pod immediately.

> **Note**
>
> Diameter gateway service handles graceful termination of "Disconnect-Peer-Request" and "Disconnect-Peer-Answer" along with HTTP2 connections.

The grace period is configurable in the custom-values.yaml file, the default value is set at 30 seconds. Here is a sample configuration for graceful shutdown parameters in custom-values.yaml file:

```
bsf-management-service:
    gracefulShutdown:
        gracePeriod: 30s
config-server:
    gracefulShutdown:
        gracePeriod: 30s
```

BSF Services that support Kubernetes graceful shutdown:

- BSF Management Services
- Config Server
- CM service
- Audit service
- Query service
- Diameter Gateway
- AppInfo service
- PerfInfo service
- Ingress Gateway
- Egress Gateway
- NRF client service

For more information on setting the gracePeriod value for different BSF services, see section "Customizing Binding Support Function" in *Oracle Communications Cloud Native Core Binding Support Function Installation and Upgrade Guide*.

3.36 NF Scoring for a Site

The NF Scoring feature calculates the score for a site based on Network Function (NF) specific factors such as metrics, alerts, etc. The NF Scoring feature helps the operator to determine the health of a site as compared to other sites. Comparing the NF scores within or across the sites helps the customers to choose the site.

One of the use cases is the Controlled Shutdown feature that allows the operator to partially or completely isolate the site. The NF Scoring feature helps the operators to choose which site to partially or completely isolate based on NF scoring.

App-Info service queries and calculates NF-Score as it has the site information.

App Info Scoring Mechanism:

App Info reads the configurations from the common config server to check if NF Scoring functionality is enabled or not. It works in the following ways:

- **Continuous NF Score Calculation:** When the NF Scoring feature is enabled, app info periodically reads the configurations to calculate the score.
- **On-Demand NF Score Calculation:** When the NF Scoring feature is enabled, app info fetches all the factors or criteria to calculate the NF Score. It is real-time fetching of factors and then the NF score is calculated on demand.

Table 3-19 NF Scoring Criteria

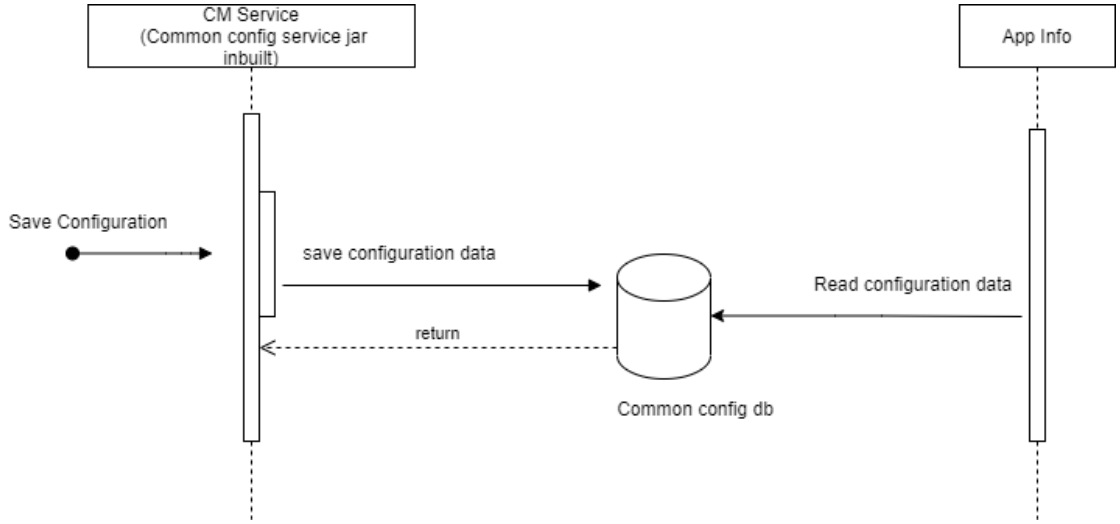
Factors	Default Score	Formula to calculate Factor Score	Details
TPS	20	min(Current-TPS / Max-TPS * Max- TPS-Score, Max- TPS-Score)	Current-TPS = IGW + EGW + Diameter Ingress + Diameter Egress Max-TPS specifies the maximum TPS. Max- TPS-Score Specifies the maximum score of the TPS.
Service	30	A / N * Max-SVC-Score	A = Number of available services N = Number of configured services Max-SVC-Score Specifies the maximum score of the Service Health.
Connection	20	min(Conn-Current / Conn-Total * Conn-Score, Conn-Score)	Conn-current specifies the number of connections from network to Policy. Conn-Total specifies the total number of connections expected from network to Policy. Conn-Score specifies the score for the connection.
Replication-health	30	min(Site-Current / Site-Total * Site-Score, Site-Score)	Site-Total specifies the total number of possible replication links. Site-Current specifies the available active healthy links. Replication-health Score specifies the score for the replication-health.
Locality-Preference	5	NA	The value of Locality-Preference is added for NF score calculation.
Critical-Alerts	2	CrN * Configured-Score	CrN is the Number of active critical alarms. Configured-Score-Critical-Alerts specifies the score configured by the user.
Major-Alerts	1	MaN * Configured-Score	MaN is the Number of active Major alarms. Configured-Score-Major-Alerts specifies the score configured by the user.
Minor-Alerts	0	MiN * Configured-Score	MiN is the Number of active Minor alarms. Configured-Score-Minor-Alerts specifies the score configured by the user.

Formula for NF scoring of a site: Sum of TPS-Score, SVC-Score, Conn-Score, Replication-health, and Locality-Preference score subtracted by Alerts scores.

Call Flows

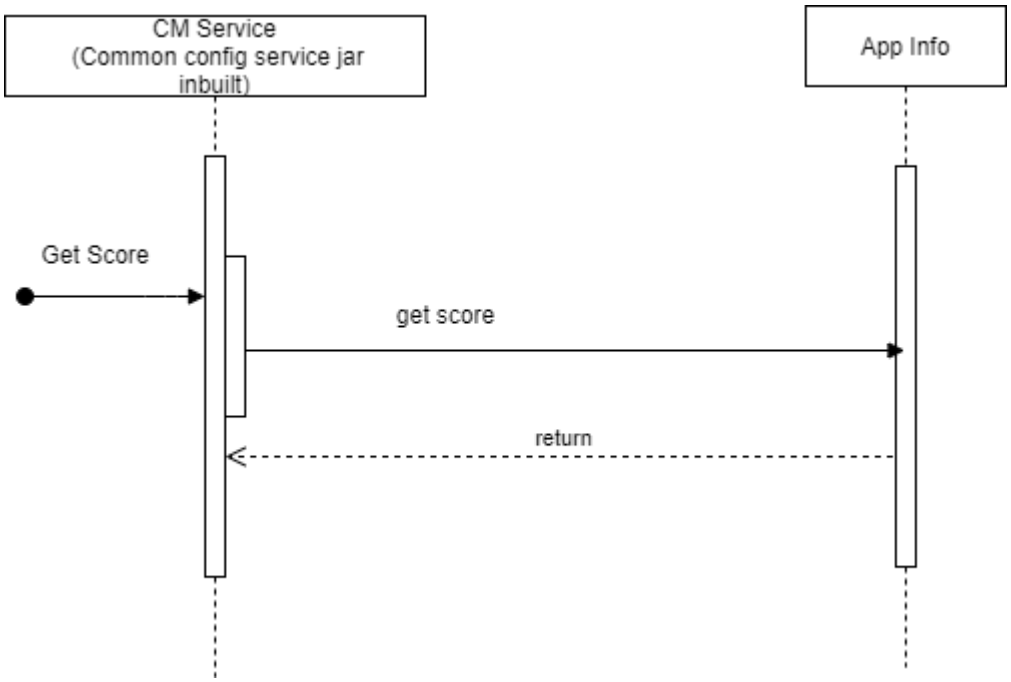
This section describes examples of the call flows for the NF Scoring feature:

Figure 3-31 Call flow to Save Configuration Data



The operator sends a request to save the configuration is sent to the CM service. It saves the configuration data to the common config database. App-Info reads the configuration data and returns the acknowledgment.

Figure 3-32 Call flow to Get the NF Score



The operator sends a request to CM service to get the score. CM service requests it to App-Info. App-Info queries and calculates NF-Score.

Managing Controlled Shutdown of an instance

Enable

You can enable this feature by selecting the **Enable NF Scoring** field in the **Settings** page of **NF Scoring**.

For more information about enabling the feature through CNC Console, see NF Scoring Configurations.

Configure

The NF Scoring feature can be configured through CNC Console. For more information, see NF Scoring Configurations.

> **Note**
>
> You can configure the env variable, NF_SCORING_INTERVAL, in deployment of app-info. Default value is 30 seconds (changing the env variable would result into restart of app-info pod).

Observe

Metrics

BSF provides the following metrics specific to NF Scoring feature:

- nfscore
- nfScoringFactorActualValue

For more information, see AppInfo Metrics .

3.37 NRF Client Retry and Health Check

With the alternate route retry feature, Policy can attempt service requests to an alternate secondary Network Repository Function (NRF) when the primary NRF throws errors. In addition, the health status check feature actively monitors the health of the NRFs and provides the list of the healthy NRFs for session requests only. The NRF client also provides the health information of NRFs to other services if requested, and notifies any change in the health status.

For a given service request, the NRF client initiates a request towards a healthy and the highest priority NRF. If the NRF client receives a failure response for the request or the request timed-out, it attempts to send the request to the same NRF for `NrfRetryConfig.primaryNrfRetryCount` number of times. If a success response is received before the retry count gets exhausted, NRF client accepts the response and does not send any further service requests. However, if NRF client fails to receive a success response, it attempts to send the service request to an alternate NRF. The alternate NRF is selected based on the assigned priority and health status.

If the NRF Client receives a `retryAfterTime` value in the response header from the NRF, the NRF Client halts any further attempts to the NRF and flags the NRF as unhealthy for the specified time period. The NRF client retries the service request to alternate NRFs until any one of the following conditions are met:

- NRF-client receives a success response.
- NrfRetryConfig.alternateNRFRetryCount is exhausted.
- All attempts to available healthy NRFs are exhausted.

Once any of the listed conditions are met, NRF-client accepts the response and proceed.

NRF Client marks NRF as unhealthy under the following conditions:

- If the NRF Client receives a *retryAfterTime* value in the response header from the NRF, then NRF will be unhealthy for a time period as defined in *retryAfterTime*.
- If the status code received is available in the default values for *errorCodeReasonsForFailure*, then NRF will be unhealthy for a period of time as defined in `ConfigMap.data: profile.retryAfterTime`.
- If the status code received is available in the default values for *errorCodeReasonsForFailure* and all the retry attempts are exhausted.
- If NRF Client receives an error from Gateway service and the error is configured in the *gatewayErrorCodes* with all the exhausted retry attempts.

> **Note**
>
> - If NRF Client receives an error from Gateway service and the error is not configured in the *gatewayErrorCodes*, then NRF remains marked as healthy.
> - *HealthCheckConfig* and *NRFRetryConfig* must be configured for the NRF Client functionality to work as expected.
> - NRF Client considers a response as failure only when it is configured in the `errorReasonsForFailure` parameter in the custom-values.yaml file. The primary and non-primary NRFs must be geo-redundant for the NRF Retry mechanism to work.
> - For autonomous procedures such as NfRegistration and NfHeartbeat, NRF-client continues to retry sending service requests till a success response is received. For details on NRF Client configuration parameters, see *NRF Client Configuration* section in *Oracle Communications Cloud Native Core, Converged Binding Support Function Installation, Upgrade and Fault Recovery Guide.*

3.38 BSF Message Feed for Monitoring

In order to enable correlation of the internal and external (request/response) messages for all the transactions initiated by the producer and consumer NFs, BSF supports copying the messages at Ingress and Egress Gateways.

This feature allows NFs using Ingress and Egress Gateways to report every incoming and outgoing message to Oracle Communications Network Analytics Data Director (OCNADD) monitoring system.

That is, OCNADD is a message store to keep a copy of each request and response processed through IGW & EGW.

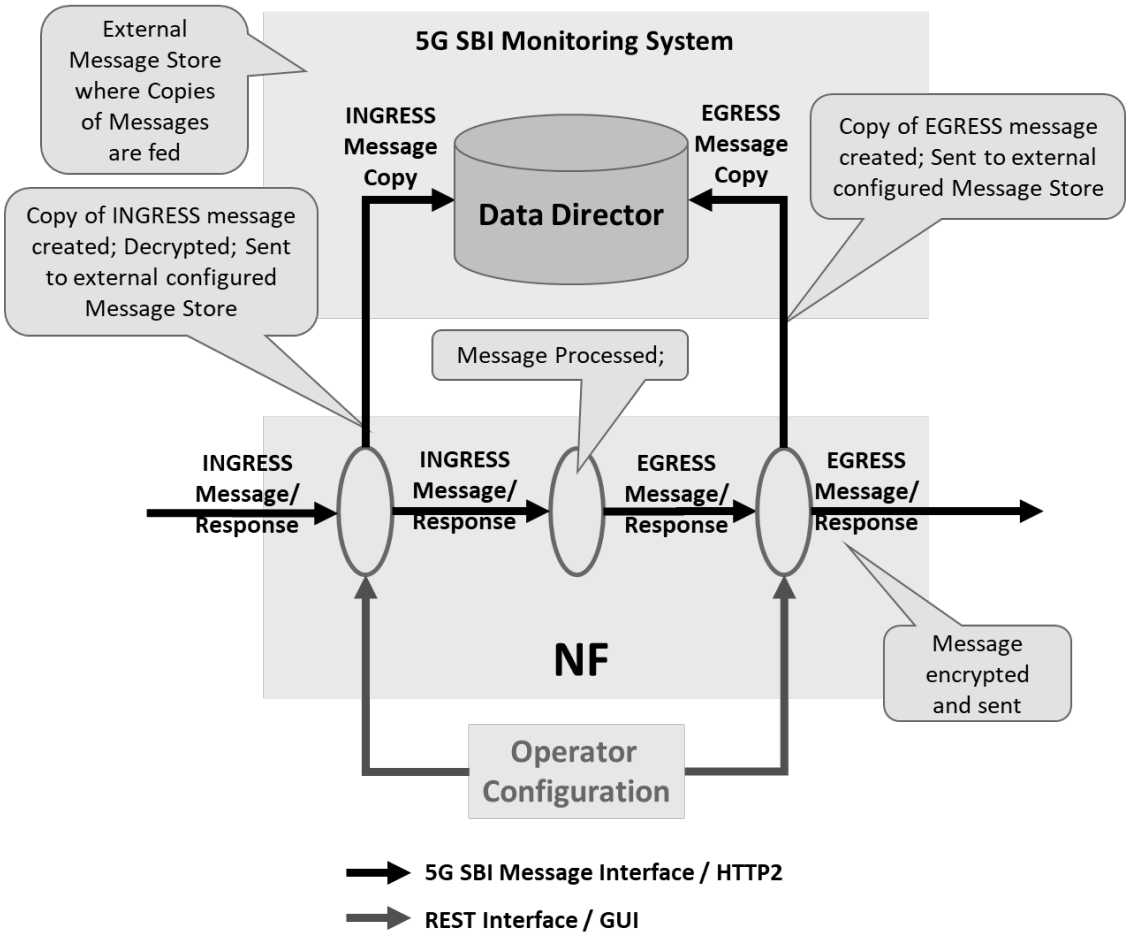
The insights on these messages enable NFs to integrate with external 5G SBI monitoring system for:

- Call Tracing / Tracking

- Live debugging

Architecture

Figure 3-33 BSF Message Feed Architeture



OCNADD is a Network Data Broker part of the Network Analytics suite of products. OCNADD receives network data traffic information from various sources such as 5G NFs and Non-5G Nodes and sends the data securely to subscribed consumer (3rd Party tools) after applying its powerful and configurable filtering, replication, and aggregation rule corresponding to subscribed consumers. For more information on OCNADD, see *Oracle Communications Network Analytics Data Director User Guide*.

5G NF Kafka Producer is used as the source to send the data stream towards OCNADD. The 5G NFs use integrated Kafka producer services to stream the 5G South Bound Interface (SBI) messages along with metadata added by NFs to OCNADD.

Managing BSF Message Feed

Enable

BSF Message Feed feature can be enabled using Helm parameters either at the time of BSF installation or during the software upgrade.

`ingress-gateway.message-copy.enabled` parameter is used to enable copying messages passing through Ingress Gateway.

`egress-gateway.message-copy.enabled` parameter is used to enable copying messages passing through Egress Gateway.

For more information, see *Configuring Ingress Gateway*, *Configuring Egress Gateway*, and *Configuring Kafka for NF Message Feed* sections in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

Configure

BSF Message Feed feature can be configured using Helm parameters either at the time of BSF installation or during the software upgrade.

For more information, see *Configuring Ingress Gateway*, *Configuring Egress Gateway*, and *Configuring Kafka for NF Message Feed* sections in *Oracle Communications Cloud Native Core, Binding Support Function Installation, Upgrade, and Fault Recovery Guide*.

SASL_SSL Configuration for BSF Message Copy

As there is no certificate-based client authentication required, a trustStore is created at BSF.

BSF contains placeholders to accept caroot certificates, which are then translated into trustStore using Gateway init-containers.

BSF uses native SSL functionality provided by Gateway services. SSL service block gets activated or used, when enableIncomingHttps is set to `true`. The same configuration is used for message copy SSL configuration too.

To configure only BSF-DD SSL communication without native SSL functionality, configure **caBundle** and **trustStorePassword** sections with appropriate secret configurations.

To use both native SSL functionality and BSF-DD SSL communication, add the caRoot certificate of Kafka broker to the existing caRoot certificate by appending Kafka broker ca certificate after the existing certificate.

1. Generate SSL certificates.

   > **Note**
   >
   > Creation process for private keys, certificates and passwords is based on discretion of user or operator.

2. Before copying the certificates to the secret, add the DD Root certificates contents into the CA certificate(**caroot.cer**) generated for NRF.

   > **Note**
   >
   > Make sure to add 8 hyphens "**-**" between 2 certificates.

```
-----BEGIN CERTIFICATE-----
<existing caroot-certificate content>
-----END CERTIFICATE-----
--------
-----BEGIN CERTIFICATE-----
```

```
<DD caroot-certificate content>
-----END CERTIFICATE-----
```

3. Create a secret for authentication with DD.
   To create a secret store the password in a text file and use the same file to create a new secret.

```
kubectl create secret generic ocingress-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=caroot.cer --from-file=ssl_rsa_certificate.crt --from-
file=ssl_ecdsa_certificate.crt --from-file=sasl.txt -n <namespace>

kubectl create secret generic ocegress-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=ssl_rsa_private_key.pem --from-
file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=ssl_cabundle.crt --from-file=ssl_rsa_certificate.crt --from-
file=ssl_ecdsa_certificate.crt --from-file=sasl.txt -n <namespace>
```

4. Provide appropriate values for the SSL section.
   SSL configuration:

```
service:
  ssl:

    privateKey:
      k8SecretName: ocegress-secret
      k8NameSpace: bsf
      rsa:
        fileName: rsa_private_key_pkcs1.pem
      ecdsa:
        fileName: ssl_ecdsa_private_key.pem

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

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

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

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

```
    initialAlgorithm: RS256
```

5. Configure the message copy feature.

```
messageCopy:
  enabled: true
  copyPayload: true
  topicName: BSF
  ackRequired: false
  retryOnFailure: 0
  security:
    enabled: true
    protocol: SASL_SSL
    tlsVersion: TLSv1.2
    saslConfiguration:
     userName: ocnadd
     password:
       k8SecretName: ocegress-secret
       k8NameSpace: bsf
       fileName: sasl.txt
```

6. Make sure to configure the correct SASL_SSL port in `kafka.bootstrapAddress` attribute. To get the correct value of this, refer to DD Kafka's Values.yaml file.

Observability

Metrics

The following metrics are used to count the ingress and egress messages at the gateways:

- oc_ingressgateway_msgcopy_requests_total
- oc_ingressgateway_msgcopy_responses_total
- oc_egressgateway_msgcopy_requests_total
- oc_egressgateway_msgcopy_responses_total

For more information, see:

- Ingress Gateway Metrics
- Egress Gateway Metrics

Alerts

The following alerts are raised when OCNADD is not reachable:

- INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
- EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

For more information, see

- INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR
- EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

4 Configuring BSF Using CNC Console

This chapter describes how to configure different global and service parameters in Oracle Communications Cloud Native Core Binding Service Function (BSF) using Oracle Communications Cloud Native Configuration Console (CNC Console).

Oracle Communications Cloud Native Configuration Console (CNC Console)

This section provides an overview of the CNC Console, which includes an interface to help in creating global and service parameters in BSF.

You can use BSF integration with CNC Console only after logging successfully in to the CNC Console application. To log in to the CNC Console, make the following updates to the hosts file available at the `C:\Windows\System32\drivers\etc` location.

1. In Windows system, open the **hosts** file in a notepad as an Administrator and append the following set of lines at the end:

   ```
   <IP Address> cncc-iam-ingress-gateway.cncc.svc.cluster.local
   ```

   ```
   <IP Address> cncc-core-ingress-gateway.cncc.svc.cluster.local
   ```

   where:

   <IP Address> is the host address of the deployment cluster. It depends on the deployment cluster.

   Example:

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

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

   > **Note**
   >
   > The IP Address can change when deployment cluster changes.

2. Save and close the hosts file.

> **Note**
>
> Before logging into CNC Console, create a CNC user and password. Using these user details, you can log in to the CNC Console application. For more information about creating a CNC Console user and password, see *Oracle Communications Cloud Native Configuration Console (CNC Console) Installation, Upgrade, and Fault Recovery Guide*.

To log in to CNC Console:

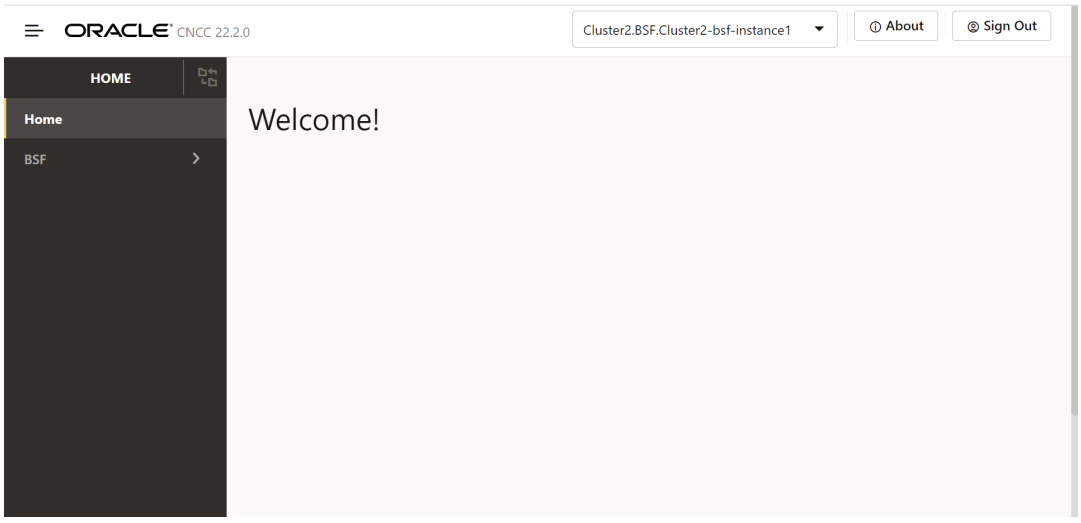
1. Open a web browser and enter the URL: http://cncc-core-ingress-gateway.cncc.svc.cluster.local:*port number*/ and press Enter.

> **Note**
>
> *port number* is cncc-iam-ingress-port number.

The login page opens.

2. Enter the **Username** and **Password**.
3. Click **Log In**.
4. On the Welcome page, select the required NF instance from the **Please Select Instance** drop-down field.
   This opens the CNC Console home page for the selected NF instance:

Figure 4-1 CNC Console for BSF



5. To use BSF services integrated with CNC Console, click **BSF** in the left navigation pane.

4.1 General Configurations

This section describes the general configurations for Oracle Communications Cloud Native Core Binding Support Function (BSF).

To access the General Configurations page from the CNC Console home page, click **BSF**, and then click **General Configurations**.

It consists of the following two sections:

- General Settings
- SBI Error Codes

4.1.1 General Settings

This section describes the general settings, which can be configured using Cloud Native Core Console for Binding Support Function (BSF).

To access the General Settings page from the CNC Console home page, click **BSF**, select **General Configurations**, and click **General Settings**.

To edit the existing general settings, perform the following steps:

1. Click Edit .
   This opens the **Edit General Settings** page.
2. Enter the values for the following fields:

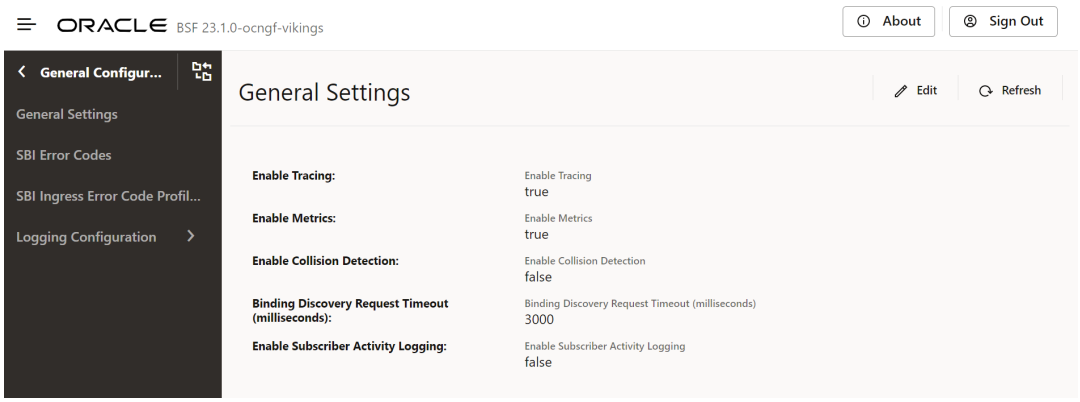
Table 4-1 General Settings

Field Name	Description
Enable Tracing	Specifies whether to enable or disable tracing for the BSF deployment. By default, this configuration is enabled.
Enable Metrics	Specifies whether to enable or disable system metrics for the BSF deployment. By default, this configuration is enabled.
Enable Collision Detection	Specifies whether to enable or disable collision detection for the BSF deployment. By default, this configuration is disabled.
Binding Discovery Request Timeout	Specifies the request timeout value for the discovery request sent by the BSF Diameter Gateway towards the BSF Management Service.
Enable Subscriber Activity Logging	Specifies whether to enable or disable subscriber activity logging. The default value is `false`.
Enable SBI Correlation	Specifies whether to enable or disable correlation-info header in BSF. The dafault value is `false`.

Table 4-2 General Settings - Enhanced Logging Configuration

Field Name	Description
Enable Enhanced Logging	Specifies whether to enable or disable enhanced logging for the BSF deployment. By default, this configuration is disabled.
Enable UE Identifier Information	Specifies whether to enable or disable UE Identifier information for the BSF deployment. By default, this configuration is disabled.

Figure 4-2 General Setting Console Page



3. Click **Save** to save the chosen general settings.

4.1.2 SBI Error Codes Configurations

This section describes how to customize the SBI error codes according to the network requirements using the SBI Error Codes page.

The **SBI Error Codes** page on CNC Console allows users to view and edit conditions defined by default for the Binding Support Function (BSF) network function. This page also provides the options to import and export SBI error codes.

The following table describes the errors supported by BSF:

Table 4-3 Error Codes and Responses

Condition ID and Name	Error Description	HTTP Status Code	Application Error Code
ERROR_CODE_RESOURCE_URI_STRUCTURE_NOT_FOUND Binding resource URI is invalid	This error is returned when bindingId is missing in the request URI or when the request URI is invalid.	404	RESOURCE_URI_STRUCTURE_NOT_FOUND
ERROR_CODE_BINDING_NOT_FOUND Binding key not found	This error is returned when binding data is not found in the database.	404	NOT_FOUND
ERROR_CODE_INVALID_QUERY_PARAM Parameters in binding key are not acceptable	This error is returned when parameters such as multiple UE addresses are sent in the request.	400	INVALID_QUERY_PARAM
ERROR_CODE_MANDATORY_QUERY_PARAM_INCORRECT Required parameter in binding key is not acceptable	This error is returned when the mandatory query parameter is invalid.	400	MANDATORY_QUERY_PARAM_INCORRECT
ERROR_CODE_OPTIONAL_QUERY_PARAM_INCORRECT Optional parameter in binding key is invalid	This error is returned when the optional query parameter is invalid.	400	OPTIONAL_QUERY_PARAM_INCORRECT
ERROR_CODE_MANDATORY_QUERY_PARAM_MISSING Required parameter in binding key is missing	This error is returned when the mandatory query parameter is missing in the URI request.	400	MANDATORY_QUERY_PARAM_MISSING

Table 4-3 (Cont.) Error Codes and Responses

Condition ID and Name	Error Description	HTTP Status Code	Application Error Code
`ERROR_CODE_INVALID_MSG_FORMAT` Parameter(s) in binding data is not supported	This error is returned in case of invalid binding data is sent as payload. For instance, when an IP domain is present without an IPv4 address, this error is reported.	400	INVALID_MSG_FORMAT
`ERROR_CODE_MANDATORY_IE_INCORRECT` Required parameter in binding data is invalid	This error is returned when the mandatory parameter such as SNSSAI is assigned a semantically incorrect value.	400	MANDATORY_IE_INCORRECT
`ERROR_CODE_MANDATORY_IE_MISSING` Required parameter in binding data is missing	This error is returned when the mandatory parameter such as SNSSAI is missing.	400	MANDATORY_IE_MISSING
`ERROR_CODE_OPTIONAL_IE_INCORRECT` Optional parameter in binding data is invalid	This error is returned when the Information Element (IE) in the request is invalid.	400	OPTIONAL_IE_INCORRECT
`ERROR_CODE_INTERNAL_SERVER_ERROR` Unexpected server error	This error is returned in the following situations: • Issue in saving data successfully to the database. • URI pattern for `nbsf-management/v1/pcfBindings` throws `IllegalArgumentException`.	500	INTERNAL_SERVER_ERROR
`ERROR_CODE_METHOD_NOT_ALLOWED` Request method not supported	This error is returned when the requested method is not supported. For instance, if the user sends a PUT request instead of a POST request to register PCFBinding, BSF returns error 405 in response to the request.	405	METHOD_NOT_ALLOWED

Editing SBI Error Codes

To edit any of the defined conditions, perform the following steps:

1. From the navigation menu, click **BSF**, then select **General Configurations**, and click **SBI Error Codes**.

This opens the SBI Error Codes page that lists the condition names along with their **HTTP Status code** and **Application Error Code**.

2. Click Edit against the condition that you need to customize.
   This opens the Edit SBI Error Codes page.
3. Update the required values for the fields as described in the following table:

Table 4-4 Parameters for Edit SBI Error Codes

Parameter	Description
Error Description	Specifies the description for a defined condition. It is recommended to use descriptions that clearly explain the condition.
HTTP Status Code	Specifies the HTTP Status code for a defined condition. This is a mandatory field and cannot be left blank. **Note:** Currently, the value for HTTP status code can be selected only from the supported set of values. To view the values, see Table 4-3.
Application Error Code	Specifies the application error code for a defined condition. Users can customize application error codes as per their requirements. This is a mandatory field and cannot be left blank.

4. Click **Save**.

Supported HTTP Status Codes

The following table describes the HTTP status codes that can be used as an input for the **HTTP Status Code** field while configuring the SBI Error codes feature:

Table 4-5 1xx Informational Series

Status Code	Description
100	CONTINUE
101	SWITCHING_PROTOCOLS
102	PROCESSING
103	CHECKPOINT

Table 4-6 2xx Success Series

Status Code	Description
200	OK
201	CREATED
202	ACCEPTED
203	NON_AUTHORITATIVE_INFORMATION
204	NO_CONTENT
205	RESET_CONTENT
206	PARTIAL_CONTENT
207	MULTI_STATUS
208	ALREADY_REPORTED
226	IM_USED

Table 4-7 3xx Redirection Series

Status Code	Description
300	MULTIPLE_CHOICES
301	MOVED_PERMANENTLY
302	FOUND
302	MOVED_TEMPORARILY
303	SEE_OTHER
304	NOT_MODIFIED
305	USE_PROXY
307	TEMPORARY_REDIRECT
308	PERMANENT_REDIRECT

Table 4-8 4xx Client Error Series

Status Code	Description
400	BAD_REQUEST
401	UNAUTHORIZED
402	PAYMENT_REQUIRED
403	FORBIDDEN
404	NOT_FOUND
405	METHOD_NOT_ALLOWED
406	NOT_ACCEPTABLE
407	PROXY_AUTHENTICATION_REQUIRED
408	REQUEST_TIMEOUT
409	CONFLICT
410	GONE
411	LENGTH_REQUIRED
412	PRECONDITION_FAILED
413	PAYLOAD_TOO_LARGE
413	REQUEST_ENTITY_TOO_LARGE
414	URI_TOO_LONG
414	REQUEST_URI_TOO_LONG
415	UNSUPPORTED_MEDIA_TYPE
416	REQUESTED_RANGE_NOT_SATISFIABLE
417	EXPECTATION_FAILED
418	I_AM_A_TEAPOT
419	INSUFFICIENT_SPACE_ON_RESOURCE
420	METHOD_FAILURE
421	DESTINATION_LOCKED
422	UNPROCESSABLE_ENTITY
423	LOCKED
424	FAILED_DEPENDENCY
425	TOO_EARLY
426	UPGRADE_REQUIRED
428	PRECONDITION_REQUIRED

Table 4-8 (Cont.) 4xx Client Error Series

Status Code	Description
429	TOO_MANY_REQUESTS
431	REQUEST_HEADER_FIELDS_TOO_LARGE
451	UNAVAILABLE_FOR_LEGAL_REASONS

Table 4-9 5xx Server Error Series

Status Code	Description
500	INTERNAL_SERVER_ERROR
501	NOT_IMPLEMENTED
502	BAD_GATEWAY
503	SERVICE_UNAVAILABLE
504	GATEWAY_TIMEOUT
505	HTTP_VERSION_NOT_SUPPORTED
506	VARIANT_ALSO_NEGOTIATES
507	INSUFFICIENT_STORAGE
508	LOOP_DETECTED
509	BANDWIDTH_LIMIT_EXCEEDED
510	NOT_EXTENDED
511	NETWORK_AUTHENTICATION_REQUIRED

4.1.3 SBI Ingress Error Code Profiles Collection

This procedure provides information about how to use the SBI Ingress Error Code Profiles Collection page to create and manage SBI Ingress error code profiles collection in General Configurations.

To configure Error Code profiles, perform the following steps:

1. From the navigation menu, under **BSF**, click **General Configurations**, and then select **SBI Ingress Error Code Profiles Collection**.
   This opens the SBI Ingress Error Code Profiles Collection page.
2. Click Edit.
   This opens the Edit SBI Ingress Error Code Profiles Collection page.
3. Click 

   .
   This opens the Add SBI Ingress Error Code Profiles Collection page.
4. Enter values for the available input fields as described in the following table:

Table 4-10 Error Code Profiles Collection Configurations

Field Name	Description
Name	Specifies a unique name to identify the error profile.

Table 4-10 (Cont.) Error Code Profiles Collection Configurations

Field Name	Description
Error Code	Specifies the HTTP Code that is populated in the error response when a message request is rejected due to overload control.
Error Cause	Specifies the error cause that is populated in the error response when a message request is rejected due to overload control.
Error Title	Specifies the error title that is populated in the error response when a message request is rejected due to overload control.
Error Description	Specifies the error description that is populated in the error response when a message request is rejected due to overload control.

5. Click **Save** to save the error code profile.
   To discard the changes, click **Cancel**

   The value gets listed on the SBI Ingress Error Code Profiles Collection page. Use or available under the **Actions** column to update or delete the profile.

4.2 Error Handling

This section describes how to manage and view the error configurations in BSF, using the **Error Handling** Configurations page

4.2.1 Error Configurations

The error handling framework allows the users to configure an error state and an action for it. The action contains two parts, an error rule and an error context. On the Console UI, the operator configures the error state specific to the BSF services and the list of actions for it.

The **Error Configurations** page displays the error configurations related to different BSF services.

To add error handler template for a BSF service:

Error Configurations for Diameter Gateway Service

1. From the navigation menu, under **BSF**, click **Error Handling**, and select **Error Configurations** page. This opens the **Error Handling Configurations** page.
2. From the `Select Service Name` drop-down list select the value `diam-gateway`. This page displays diameter message retry configurations for AAR messages.. On the page **Error Handler Templates of diam-gateway** and **Error Configurations of diam-gateway** subsections are displayed.
3. The **Error Handler Templates of diam-gateway** provides two options:
   - **Error Code Configuration**
   - **Timeout Error Configuration**
4. The **Error Configurations of diam-gateway** provides default error handling configurations to retry on all error codes (except diameter result code 2xxx) and timeout for Rx AAR failed diameter messages.

5. To configure the **Error Code Configuration** in **Error Handler Templates of diam-gateway** , Click 

.
This opens the **Error Handler Template** editing page.
6. Enter values for the available input fields. The following table describes the fields:

Table 4-11 Create Error Code Configuration - Edit

Field Name	Description
On Rx	Specifies the list of diameter interfaces. The values are: • AAR
Status	Specifies the error status to be provided by the user.

Table 4-12 Error Cause Configure

Field Name	Description
Error Cause Field	Species to search for which error causing filed in the diameter answer message. Default value: ALL
Match Operator	Species the match operator to search error section in the diameter answer message. Default value: ANY
Error Response Originator	The peer from which the error origination occurs. User can choose from the following options: • ANY • INTERMEDIATE_PEER • DESTINATION PEER
Message	Specifies the error message to search in the error section of diameter answer message. Default value: ANY
Status	Specifies the error status code to search in the error section in the diameter answer message. Default value: ANY
Cause	Specifies the field that matches the cause during error ends with 'not found'. User can choose from the following options: • ANY • RESPONSE_TIMEOUT

Table 4-13 Action

Field Name	Description
Action	The action to be performed in the event of failed diameter message on Rx interface. User can choose from the following options: • RETRY TO ALTERNATE PEER • ONE RETRY TO ALTERNATE PEER

7. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

8. To configure **Timeout Error Configuration** in **Error Handler Templates of diam-gateway** , Click 

.
This opens the **Error Handler Template** editing page.
9. Enter values for the available input fields. The following table describes the fields:

Table 4-14 Create Timeout Error Configuration

Field	Description
On Rx	Specifies the list of diameter interfaces. Default value: AAR
Status	Specifies the error status to be provided by the user. Default value: ANY

Table 4-15 Error Cause Configure

Field	Description
Error Cause Field	Species to search for which error causing filed in the diameter answer message. Default value: MESSAGE
Match Operator	Species the match operator to search error section in the diameter answer message. Default value: EQUALS
Message	Specifies the error message to search in the error section of diameter answer message. Default value: TIMEOUT_EXCEPTION
Status	Specifies the error status code to search in the error section in the diameter answer message. Default value: ANY
Cause	Specifies the field that matches the cause during error ends with 'not found'. Default value: ANY
Instance	Specifies the field that matches the instance during error contains the term 'Illegal'. Default value: ANY
resource	Specifies the resource to search in the error section of diameter answer message. Default value: ANY

Table 4-16 Action

Field	Description
Action	The action to be performed in the event of response timeout on Rx interface. User can choose from the following options: • RETRY TO ALTERNATE PEER • ONE RETRY TO ALTERNATE PEER
Error Originator	The peer from which the error origination occurs. User can choose from the following options: • ANY • INTERMEDIATE_PEER • DESTINATION PEER

10. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

11. Perform the following steps to configure **Advanced Settings**:

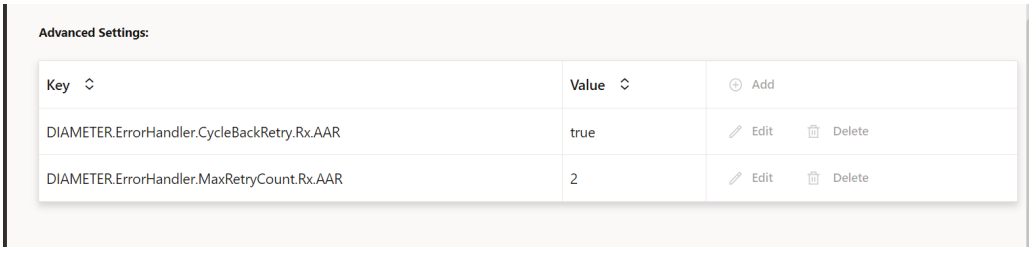
    a. Click the Add
    The page opens the **Add Advanced Settings** dialog box.

    b. In the dialog box, enter the following **key** and respective **value**:

Table 4-17 Parameters for Advanced Settings

Keys	Value
DIAMETER.ErrorHandler.MaxRetryCount.Rx.AAR	It is used to set the maximum retries that can be performed for failed AAR messages. **Default Value**: 1
DIAMETER.ErrorHandler.CycleBackRetry.Rx.AAR	It is used to set if peers can be cycled back for retries or not. **Default Value**: false

Figure 4-3 Advance Setting Configurations Screen



    c. Click **Save**.
    The page saves the Error Handling configurations.

Error Configurations for BSF Management Service

1. From the navigation menu, under **BSF**, click **Error Handling**, and select **Error Configurations** page. This opens the **Error Handling Configurations** page.

2. From the `Select Service Name` drop-down list select the value `BSF Management Sevice`. This page displays BSF Management Sevice.
3. Enable the error handler configurations using the **Enable Error Handler Configurations** toggle button.
4. The error handler template provides *Error Enhancement Configurations*.
5. To configure the *Error Enhancement Configurations* in Error Handler Templates of the required service, Click 

. This opens the **Error Handler Template** editing page.
6. Enter values for the available input fields. The following table describes the fields:

Table 4-18 Error Handler Template

Field	Description
On	Specifies the Application Error. Default value: Application Error

Table 4-19 Action

Field	Description
Action	Specifies the action to be performed in the event of failed message. Default value: Reject with Enhanced Detail
Exclude from error message	Specifies exclusion of the provided components from detail error message. By default, "Error State and "Probelm Cause" are excluded.

7. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

Importing **Error Handling Configurations**:

1. Click the **Import** icon.
   The **File Upload** dialog box opens.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

4.3 Logging Configurations

This section describes how to customize the log level and subscriber logging activity settings in BSF using the Logging Configurations pages.

4.3.1 Logging Level

This procedure describes how to configure the log level for different services through CNC Console.

> **Note**
>
> The default log level for each service is **Warn**.

The Logging Level page displays the log level configured for different services. The page allows you to edit the log level configurations.

To configure the log level:

1. From the navigation menu, under **BSF**, click **Logging Level**.
   This opens the **Logging Level Configuration** page. You can add or edit the log level and package log level for each service type from this page.
2. Click Edit .
   This opens the **Edit Log Level** page.
3. From the **Service Type** drop-down list, select the service for which you need to view, edit, or delete the logs.
4. From the **Application Log Level** drop-down list, select the root log level of the application for the selected service type. Possible values are:
   - **TRACE**
   - **DEBUG**
   - **INFO**
   - **WARN**
   - **ERROR**

   > **Note**
   >
   > The value for the **Application Log Level** field is the mandatory value, and the **Package Log Level** is the optional value.

5. Expand the **Package Log Level** group to enter the package log level information:

   > **Note**
   >
   > This step is only applicable when Oracle Engineering is trying to isolate an issue and requests one or more package names be added and logs collected after the reproduction of an issue.

   a. Click Add .
      The page opens the **Add Package log Level** dialog box.
   b. Enter the value in the **Package** field. The value of **Package** field is dependent on the package's name in each application. Before you set the value of **Package** field, you need to know what package is existed in that application.
   c. From the **Log Level** drop-down menu, select the log level for the package. Possible values are:
      - **TRACE**

- **DEBUG**
- **INFO**
- **WARN**
- **ERROR**

d. Click **Save**.
The Package log level information for the selected service is saved.

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

6. Click **Save**.
The log level information for the selected service type is saved.

4.3.2 Subscriber Activity Logging

Subscriber Activity Logging allows you to define a list of the subscribers (identifier) that you may require to troubleshoot the NFs and trace all the logs related to the subscribers separately to view. This functionality can be used to troubleshoot problematic subscribers without enabling logs or traces that can impact all subscribers. You can capture and monitor subscriber logs for Binding Register and Deregister call flow between Ingress Gateway and BSF Management Service and Binding Discovery call flow between Diameter Gateway and BSF Management Service.

To enable the subscriber activity logging functionality, set value of the **Enable Subscriber Activity Logging** parameter to **true** on the **General Configurations** page. By default, this functionality remains disabled. For more information about enabling the functionality, see General Settings

This procedure provides information about how to configure and manage subscriber logging.

The **Subscriber Activity Logging** page allows you to create new and manage existing subscribers. The page displays the list of defined subscribers and provides the options to import, export, or add lists.

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

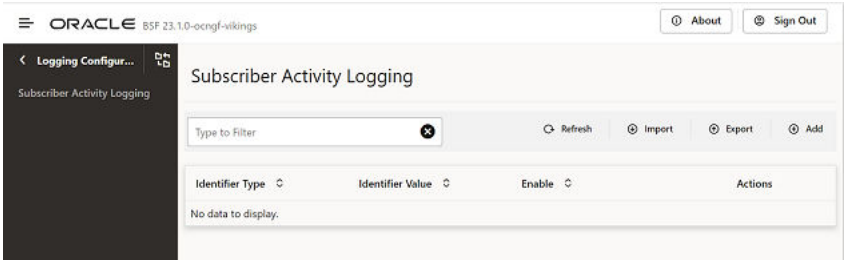
To configure a list of subscribers for logging:

To configure Subscriber Activity Logging:

1. From the navigation menu under **BSF**, navigate to **General Configurations**, click **Logging Configurations**, and then select **Subscriber Activity Logging**.
This opens the **Subscriber Activity Logging** page. The page lists the existing configurations. You can add or import new subscriber activity logging configurations using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

Figure 4-4 Adding Subscriber Activity Logging

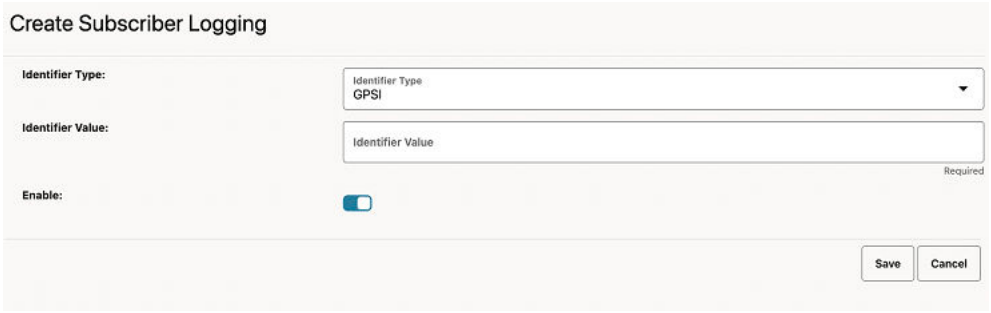


2. Click Add .
This opens the **Create Subscriber Activity Logging** page.
3. On the **Create Subscriber Activity Logging** page, enter the following information:

Table 4-20 Create Subscriber Activity Logging Field Description

Field Name	Description
Identifier Type	Select the subscriber identifier type. Supported subscriber identifier type are: • GPSI • SUPI • IPV4 • IPV6
Identifier Value	The identifier value for the selected identifier type.
Enable	Use this switch to enable or disable the subscriber logging functionality for the selected subscriber.

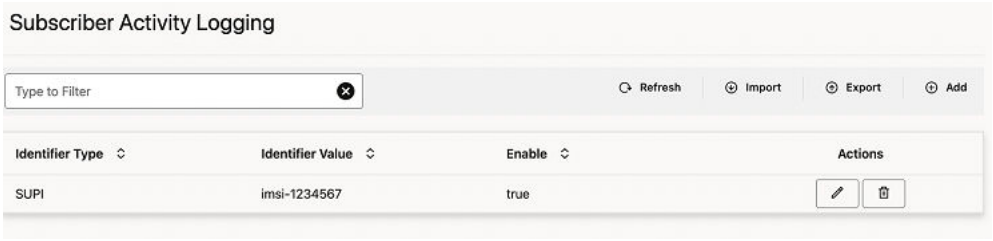
Figure 4-5 Creation of Subscriber for Logging with Identifier Console



4. Click **Save**.
The configuration gets listed on the **Subscriber Activity Logging** page. The page defines the Subscriber Activity Logging configuration in the BSF database.

> **Note**
>
> Use or available under the **Actions** column to update or delete the configuration.

Figure 4-6 Added List of Subscribers



To import Subscriber Activity Logging configuration:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Subscriber Identifiers

SUPI

In the 5G system, a globally unique Subscription Permanent Identifier (SUPI), known as IMSI (International Mobile Subscriber Identity) till 4G, is assigned for each subscription. The SUPIs are assigned in such a manner that it helps in identifying subscriptions and is independent of the user equipment.

For 4G systems, the value of IMSI is structured as:

imsi: <value>

For 5G systems, the value of SUPI is structured as:

supi: imsi-<value>

GPSI

General Public Subscription Identifier (GPSI), known as MSISDN (Mobile Station International Subscriber Directory Number) till 4G, is a 3GPP defined subscriber public identifier that can be used both inside and outside of the 3GPP system. The association between GPSI and its related SUPI are stored in the subscription data in a 5G system.

For 4G systems, the value of MSISDN is structured as:

msisdn/e164:<value>

For 5G systems, the value of GPSI is structured as:

gpsi: msisdn-<value>

4.4 Service Configurations

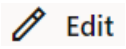
This section describes how to customize the BSF Management Service and Audit Service according to the network requirements using the Service Configuration page.

4.4.1 Management Service

You can view and edit configurations for BSF Management Service on the **Management Service** page using the CNC Console.

To access this screen from the Home screen of CNC Console, under **BSF**, click **Service Configurations** and then **Management Service**.

To edit management service configurations, perform the following steps:

1. From the navigation menu, under **BSF**. click **Service Configurations**, and select **Management Service**.
   This opens the **Management Service** page.
2. Click 

   .
   This opens the **Edit Management Service** page.
3. Update the required values for the parameters as described in the following table:

Table 4-21 Parameters for Edit Management Service Configurations

Parameter	Description
Server Root URL	Specifies the callback URI for notifications to be received by the user.

Table 4-22 NF Bindings Settings

Parameter	Description
Send Binding Header	Indicates if BSF includes the 3gpp-sbi-binding header in SBI messages for the registration creation, modification, or notification responses, as applicable. By default, the switch remains disabled.
Binding Level	Indicates the binding level to be included in the 3gpp-sbi-binding header when BSF adds this header in a message to another NF. Select any of the following values from the drop-down menu: • NF Set • NF Instance (**Default**)

Table 4-23 NF Server Settings

Parameter	Description
Send Server Header	Indicates if BSF management service includes server header while sending an error response.
Server Header Error Codes	Indicates the error codes for which service header is generated. The error codes can be from 100 to 999. Note: If you do not specify an error code in this field, BSF management service sends server headers for all error codes.

Table 4-24 Audit

Parameter	Description
Enabled	Use this flag to enable or disable stale session handling feature. By default, the feature is disabled.

Table 4-24 (Cont.) Audit

Parameter	Description
Notification Rate (per second)	Specifies the number of notifications that Audit service sends to the BSF Management service in one second. The recommended value is 50. **Default and Recommended Value**: 50 **Note**: To configure higher number than the recommended value, contact My Oracle Support (https://support.oracle.com)
Binding Age (in minutes)	Specifies the binding age for binding records. Once the binding age for a record exceeds the configured value, audit service marks the record as suspected stale. The recommended value is 3600.
Maximum Binding Age (in minutes)	Specifies the maximum binding age for binding records. Once the binding age for a record exceeds the configured value, audit service marks the record as stale and BSF removes the record from its local database. The recommended value is 7200.
Minimum Audit Attempts	Specifies the minimum number of consecutive failed audit attempts until maxTTL / forceTTL is reached. If maxTTL is reached and audit_attempts + 1 >= Minimum Audit Attempts for maxTTL, Audit service sends notification to Management Service with maxTTL flag set to *true*. Management Service deletes the record. **Range**: 0-255 **Default Value**: 0 **Note**: If maxTTL is not reached and if audit attempts are reached, the number of audit attempts are incremented until maxTTL is reached.
Minimum Audit Passes Interval (in minutes)	Specifies the minimum interval between two consecutive audits. The recommended value is 10.
Answer with Result Code Configuration	Choose the value that BSF compares with the result code in the AAA-I answer. If both the values match, BSF Management service initiates stale record notification. To add the result code, perform the following steps: a. Click **Add**. The **Add Answer with Result Code Configuration** dialog box opens. b. For the **Answer with Result Code**, select any of the following valid values from the drop-down list: • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE **Note**: If you select `EXPERIMENTAL_RESULT_CODE`, enter the required values for **Result Code** and **Vendor ID**. c. Click **Save** on the dialog box.

Table 4-24 (Cont.) Audit

Parameter	Description
Query to PCF	Indicates whether BSF management service queries PCF to confirm the status of a PcfBinding record, which is suspected as stale by the audit service. **Default value**: false **Note**: When Query to PCF parameter is set to false, the value of "Minimum Audit Attempts" parameter in Service Configurations of Management Service, and "Forced Deletion - Minimum Audit Attempts" parameter in Service configurations of Audit Service should be set to 0.
Vendor ID	Specifies the vendor ID that BSF retrieves from the Vendor Specific Attribute to send query requests towards PCF. The vendor ID should be 6-digit long. **Note**: PCF sends the Vendor Specific Attribute in the request body at the time of binding registration.

Table 4-25 Active Bindings Counting

Parameter	Description
Count Active Binding	Enables or disables the active sessions counting. By default, the active sessions counting is disabled. To enable the feature, set the value of this parameter to `true`.
Bindings Count Interval (in minutes)	Specifies the time interval (in minutes) for which maximum active sessions are reported as a metric. Default value is 15 minutes. You can set the time interval to any value between 1 to 60 minutes.
Root Log Level	Specifies the log level of BSF Management service. The available values for this field are as follows: • Trace • Debug • Information • Warn (**Default**) • Error • Always
Log Levels	To add the log levels, perform the following steps: a. You can add log levels using the **Log Levels** group on this page. b. To add log level: i. Click ⊕ Add . This opens the **Add Log Levels** dialog box. ii. On the dialog box, enter the values shown in Table 4-26. iii. Click **Save** on the dialog box. The log level information for the selected service type is saved.

Table 4-26 Parameters for Add Log Levels Configurations

Parameter	Description
Logger Name	Specifies the name of the logger.

Table 4-26 (Cont.) Parameters for Add Log Levels Configurations

Parameter	Description
Level	Specifies the log level of BSF Management service. Select any of the following valid values: • Trace • Debug • Information • Warn (**Default**) • Error • Always

Table 4-27 NF Correlation Settings

Parameter	Description
Send Correlation-Info Header	Specifies an option to forward the received or generated headers to the Produce NFs. By default the switch remains disabled.
Allowed Correlation-info Header Generation Type(s)	Specifies that if correlation header is not received from consumer NFs, BSF should generate the header. The Correlation-Type supported • SUPI • GPSI • (Select either both or none)
Enable Binding Revalidation	When this field is enabled, BSF checks if the binding information for the PDU session is present in BSF. Existence of the binding association for the PDU session in BSF confirms the binding association being valid in BSF. If the binding association is missing in BSF, it is restored by creating the association in BSF. **Default value**: false

4. Click **Save** on the **Edit Management Service** page to save your changes.

4.4.2 Audit Service

This section provides information about configuring the Audit Service.

4.4.2.1 Audit

The **Audit Service** page displays the Audit Service configurations. The page allows you to edit the configurations.

To configure Audit service:

1. From the navigation menu under **BSF**, navigate to **Service Configurations**, and select **Audit Service** and browse to **Audit** page.
   This opens the **Audit** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit Audit** page.
3. Make sure that the value of the **Audit Enabled** switch is enabled.
   This field determines if auditing is enabled for BSF Management Service. By default, this switch is enabled.

4. Expand the **Forced Deletion** group and configure the **Minimum Audit Attempts** parameter.

   Minimum Audit Attempts specifies the minimum number of audit attempts until ForceTTL is reached.

   If ForceTTL is reached and audit_attempts + 1 >= Minimum Audit Attempts of ForceTTL, then Audit service deletes the identified stale records from its respective database.

   The default value of this parameter is 0 and the value can range between 0 to 255.

5. Click **Save**.
   The page saves the Audit service configurations.

> **Note**
>
> **Important considerations during Audit configurations**:
>
> In situations where the number of stale records (records that are eligible to be audited) at any given point of time in the system (for a given microservice database) is expected to be high (for example, > 1M), then the **Session Age** and/or the **Notification Rate** parameters should be set appropriately such that at least 2 audit cycles can be finished before the records that were assessed by the first cycle fall stale again. The Audit procedure having a **Session Age** less than this recommendation, may not be able to assess all stale records as the already assessed ones will be stale again too soon. It is recommended to keep a minimum of 24 hours for the **Session Age** and a minimum of 48 hours for **Max Binding Age**.
>
> The time taken to complete an Audit Cycle and begin the next one can be calculated as below:
>
> Audit Cycle Time = S / (N*60) + I minutes, where,
>
> S = expected number of stale sessions at any given time,
>
> N = notification rate (per second),
>
> I = minimum Audit Interval

4.4.2.2 Audit Schedule Data

Audit service supports multiple pod, using the Audit Schedule and Audit TaskScheduler. Audit schedule has list of registerd services that needs audit service with all the scheduled details. Audit TaskScheduler polls for all those audit jobs in the QUEUED status.

Figure 4-7 Audit Scheduled Service List Data

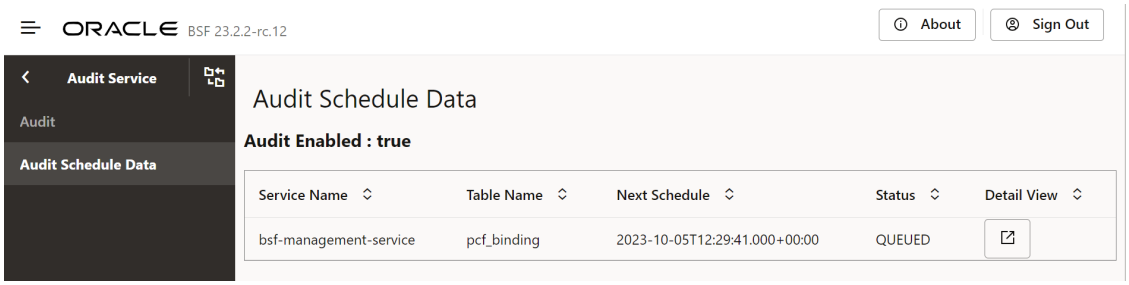


Table 4-28 Audit Schedule Data Fields

Field Name	Description
Service Name	Name of the service that had registerd for audit service.
Table Name	Name of the database table that has requested for the audit service
Next Schedule	Next schedule availability time
Status	Scheduler job status
Start Time	Audit start time of pod.
End Time	Audit end time of pod.
Last Polled Time	Pod and associated scheduler details.
Schedular Details	Last time at which pod updated this table.
Is Service Dependent	If this is true, notification will be triggered for one table in the service, for all table's in the service, notifications will be sent parallelly based on the notificationRate set for each table.

Audit Schedule task can be in one of the state described below:

Figure 4-8 Audit Schedule Job Work Flow

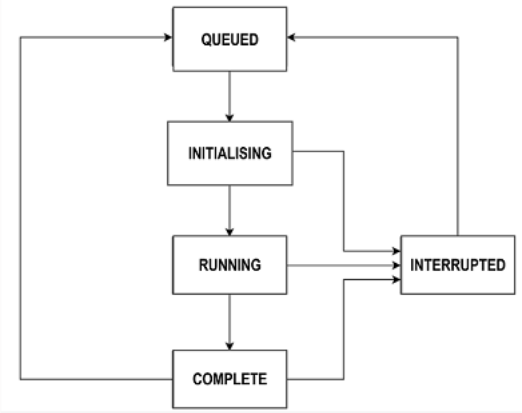


Table 4-29 Audit Schedule Job Status

Status	Description
QUEUED	When a registered request is received it is added to the schedule table, the job status is set to Queued.
INITIALISING	When polling task is complete and is initialising for AuditTaskManager to audit, the job status is set to Initialising.
RUNNING	When Audit task manager starts the task, the job status is set to Running.
COMPLETE	When Audit TaskManager completes the Audit, the status is set to Complete.

Table 4-29 (Cont.) Audit Schedule Job Status

Status	Description
INTERRUPTED	When the audit process is paused from GUI, then the job status is set to Interrupted. When resumed from GUI, job status is set to Queued When deregistered, the job data will be removed from the table. when a service is register, it is set to Queued.
DEREGISTERED	When deregistered, the job status is set to Deregistered for Initialising or Running and the entry will be deleted for any other status(except Initialising or Running). In case the a service register request is received before AuditTaskManager deletes the table entry for deregistered job statuses, the status would be moved to Queued.

For more information on Audit Service and Audit Schedule REST API details, see the section *Audit Service* in *Oracle Communications Cloud Native Core, Binding Support Function REST Specification Guide*.

4.5 Diameter Configurations

This section describes how to manage and view the Diameter Configurations in BSF using the Diameter Configurations pages.

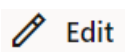
The Diameter configuration includes:

- Settings
- Peer Nodes
- Diameter Routing Table

4.5.1 Settings

The **Settings** page displays the general configurations related to the Diameter Gateway. The page allows you to edit the configurations.

To edit settings:

1. From the navigation menu, under **BSF**, click **Diameter Configurations** and select **Settings**.
   This opens the **Settings** page. The page displays the existing configurations.
2. Click 

   .
   This opens the **Edit Settings** page.
3. Enter the following information under the respective groups:

Table 4-30 Timer

Field Name	Description
Reconnect Delay (sec)	Enter the time frame to delay before attempting to reconnect after a connection failure in seconds. The default value is 3 seconds.
Response Timeout (sec)	The amount of time Diameter Gateway waits for the answer to come from the sent request. It is a global value applicable for all the interfaces messages. Enter the response timeout interval in seconds. **Note:** To enable Application or Command code Response timeout value, see Enhanced Timer Configuration. The default value is 5 seconds.
Connection Timeout (sec)	Enter the connection timeout interval in seconds. The default value is 3 seconds.
WatchDog Interval (sec)	Enter the watchdog interval in seconds. The default value is 6 seconds.

Table 4-31 Transport

Field Name	Description
Protocol	The protocol supported is TCP.

Table 4-32 Congestion Control

Field Name	Description
Load Shedding Profile	Select any one of the configured load shedding profiles for congestion control on Diameter interface from the drop-down list.
Message Priority Profile	Select any one of the configured message priority profiles for congestion control on Diameter interface from the drop-down list.

Table 4-33 Overload Control

Field Name	Description
Load Shedding Profile	Select any one of the configured load shedding profiles for overload control on Diameter interface from the drop-down list.

Table 4-33 (Cont.) Overload Control

Field Name	Description
Message Priority Profile	Select any one of the configured message priority profiles for overload control on Diameter interface from the drop-down list. **Note**: The following message priority data that was exported prior to BSF 23.2.0 cannot be imported as the data may be corrupt: • message containing Sd as interface • Sy-SLR as condition message The data with Sd interface or Sy-SLR condition messages that are exported only with BSF 23.2.0 or later versions can be imported.

Table 4-34 Enhanced Timer Configuration

Field Name	Description
Application Name	Request Timer configuration for applications name like Rx, Gx, Sy, Sd.
Application Response Timeout (milliseconds)	Enter the application response timeout in milliseconds. The range of this value is between between 3 seconds to 2147483647.

Table 4-35 Command Code Response TimeOut

Field Name	Description
AAR (milliseconds)	The command code response timeout value for AAR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000
STR (milliseconds)	The command code response timeout value for STR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000
RAR (milliseconds)	The command code response timeout value for RAR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000
ASR (milliseconds)	The command code response timeout value for ASR. The allowed value ranges from 3 to 2147483647. **Default Value**: 5000

The order of precedence (from highest to lowest) of response timeout configurations is:

a. Command Code Response Timeout (ms) - Message level configurations i.e at AAR, STR etc.

b. Application Response Timeout (ms) - Interface level configurattion i.e at Gx, Rx etc.

c. Response Timeout (ms) - General level configutation

4. Perform the following steps to configure **Advanced Settings**:

   a. Click the Add
   The page opens the **Add Advanced Settings** dialog box.

   b. In the dialog box, enter the following **keys** and respective **values**:

   The following table describes the keys and values:

Table 4-36 Add Advanced Settings Configurations

Key	Value
DIAMETER.Enable.Validate.Realm	Used to validate the destination-realm received in the AAR-I message against the destination-realm in BSF's Diameter Gateway host realm. **Default value**: false
DIAMETER.BSF.Enable.Validate.Binding.Realm	Used to validate the destination-realm of AAR-I against the discovered pcfBinding's realm. **Default value**: false
DIAMETER.BSF.Enable.Overwrite.Realm	Used to configure whether to overwrite the pcfBinding's realm and identity information in AAR-I destination-realm AVP. **Default value**: false
DIAMETER.ErrorHandler.Enable.UpdateDestinationHost	By default, BSF Diameter Gateway keeps the Destination-Host AVP to the retry message same as originally recieved request message. There is an option to change the Destination-Host for retry message with respective destination peer (Retry Peer) found using the error handling configuration. If *DIAMETER.ErrorHandler.Enable.UpdateDestinationHost* value is set to true, then change the Destination-Host with respective destination peer (retry peer). **Default value**: false

5. Click **Save** to save the settings.

4.5.2 Peer Nodes

This procedure provides information about how to define and manage Peer Nodes in Diameter Configurations.

The **Peer Nodes** page allows you to create new peer nodes and manage existing peer nodes. The page displays the list of defined configurations and provides the options to import, export, or add data.

To configure Peer Nodes:

1. From the navigation menu, under **BSF**, click **Diameter Configurations**, and select **Peer Nodes**.
   This opens the **Peer Nodes** page. The page lists the existing Peer Nodes. You can add or import new nodes using this page.

> **Note**
>
> Click Export to download the available listings in the JSON file format on your system.

2. Click Add .

   This opens the **Create Peer Node** page.

3. On the **Create Peer Node** page, enter values for the available input fields.
   The following table describes the various field names:

Table 4-37 Create Peer Node Configurations

Field Name	Description
Name	Unique name of the peer node. Example value: `ocs`
Type	Defines which type of diameter service must be selected. The values can be • PCF • Application function (AF) • backend • diameter routing agent (dra) • online charging system (ocs) • tdf • udr
Reconnect Limit (sec)	Defines the reconnect limit. Configure this value as the Diameter peer configuration. Example value: `10`
Initiate Connection	Set to **true** to initiate the connection with peer node.
Transport	Defines the type of transport ways for configuring a peer. The values can be: • TCP • TLSv1.2 • TLSv1.3 • TLSv1.2_OR_TLSv1.3
Port	Enter the port number. Enter a number from 0 to 65535. Example value: `8007`
Host	Enter the host name. Enter an FQDN, ipv4, or ipv6 address available for establishing diameter transport connections to the peer node.
Realm	Enter the realm name, that is, FQDNs to all of the computers that transact diameter traffic. For example, to add the realm detail of the OCS peer, enter `xxx.com`.
Identity	Enter an identity to define a node in a realm. For example, to add the identity detail of the OCS peer, provide value enter `ocs`.

4. Click **Save** to save the changes.

> **Note**
>
> Click **Cancel** to discard the changes.

The value gets listed on the **Peer Node** page. Use or available in the next column to update or delete the listing.

Importing Peer Nodes

To import peer node:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

4.5.3 Diameter Routing Table

Configuration allows routing Diameter request messages to next hop peer based on `Diameter application-id`, `Destination-Realm`, and `Destination-Host`.

When using routing table, there are two ways of configure next hop route:

1. Host-Based Routing: The destination-host of incoming message is checked in the routing table, and then the message is routed to the top priority matching route's peer.
2. Realm-Based Routing: The destination-realm of incoming message is checked in the routing table, and then the message is routed to the top priority matching route's peer.

Routing decision at Diameter-Gateway

Diameter gateway follows below steps in order:

1. If the incoming request message has destination-host and the specified peer is directly connected with gateway pod, then the message is routed to the peer specified in destination-host.
2. If the incoming request message has destination-host and is not directly connected via any other diameter-gateway pods in the cluster, then the message will be inter-pod routed.
3. The routing table is scanned for a matching route by:
   - If the host is reachable, message is sent.
   - If the host is not reachable directly, find if it can be reached by another diameter gateway pod, message is sent using inter-pod route
   - If the host is not reachable directly or indirectly, lookup the routing table again for the next matching route.

The **Diameter Routing Table Configurations** page displays the Diameter routing configurations. This page allows you to edit the configurations.

To configure the Diameter routing table:

1. From the navigation menu, under **BSF**, click **Diameter Configurations**, and select **Routing Table**.

This opens the **Diameter Routing Table Configurations** page. The page displays the existing configurations.

2. Click Edit .
   This opens the **Edit Diameter Routing Table Configurations** page.
3. Expand the **Diameter Route Table** Table group.
   The expanded group allows you to add route table entries.
4. To add routing table:
   a. Click Add .
      The page opens the **Add Diameter Route Table** dialog box.
   b. Enter the values for the following input fields:

Table 4-38 Add Diameter Route Table Configuration

Field Name	Description
Priority	Defines the order of use when one or more routes have overlapping criteria. It can be a number in the range of 0 to 65535. The lowest priority value indicates the highest priority. **Note:** If there are more than one routing table entry with same priority, it will consider only first row from multiple rows with same priority.
Name	Specifies the unique name of the diameter routing table.
Type	Specifies whether the diameter route table is Host or Realm based.
Realms/Hosts	Specifies the value of the Realms or Hosts depending on the Type selected by the user. For Realms, you can add multiple FQDNs to this field.
Application ID	Specifies the type of application or interface. The available values are • Rx • Gx • Sh • Sy • All Users can select multiple values for this parameter.
Server Identifier	Specifies the server to which the message is to be routed. This identity must also be present in the Identity field of the peer node. **Note:** If multiple server identifiers are configured one after the other separated by (,) comma, it considers the first value and ignores the rest of the values which were added with the comma separator.

An example of adding the diameter routing details is shown below:

Figure 4-9 Adding first Diameter Routing Element

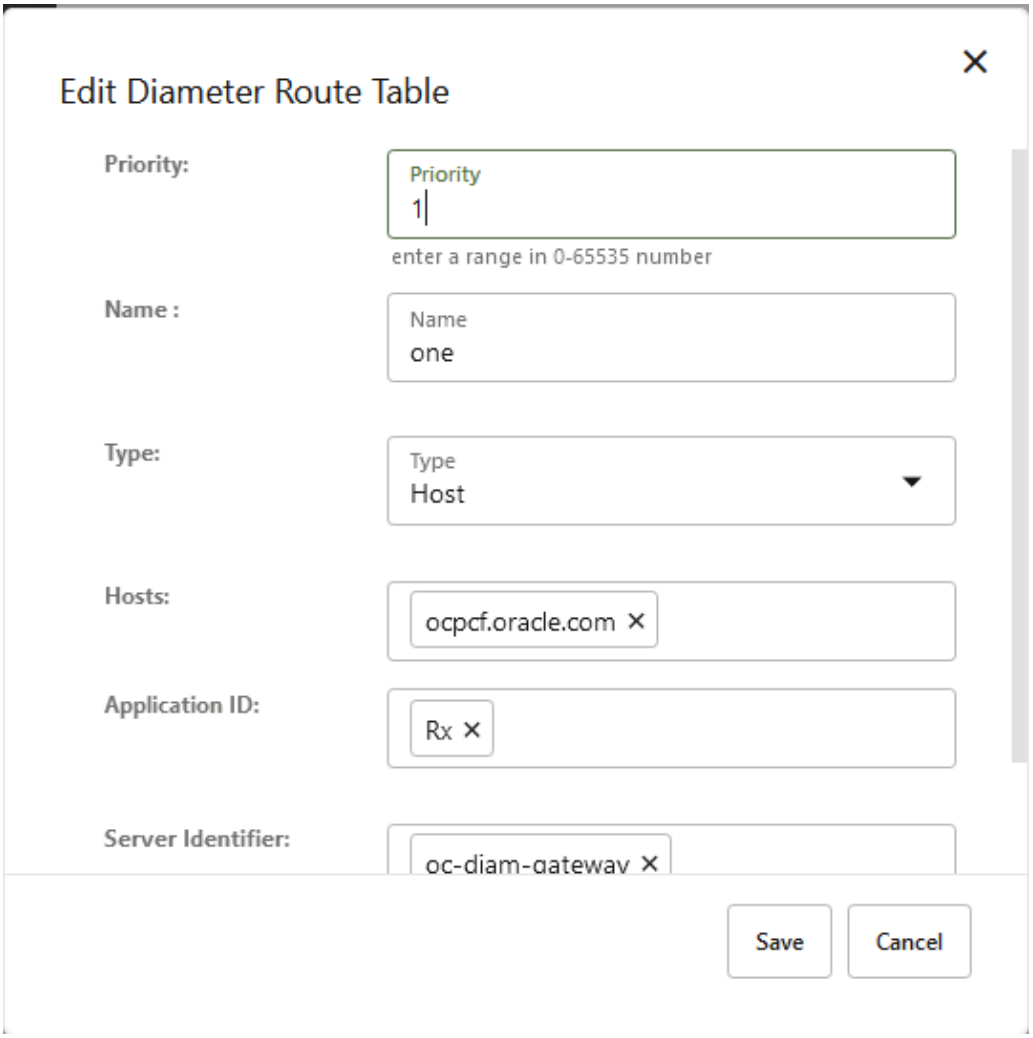
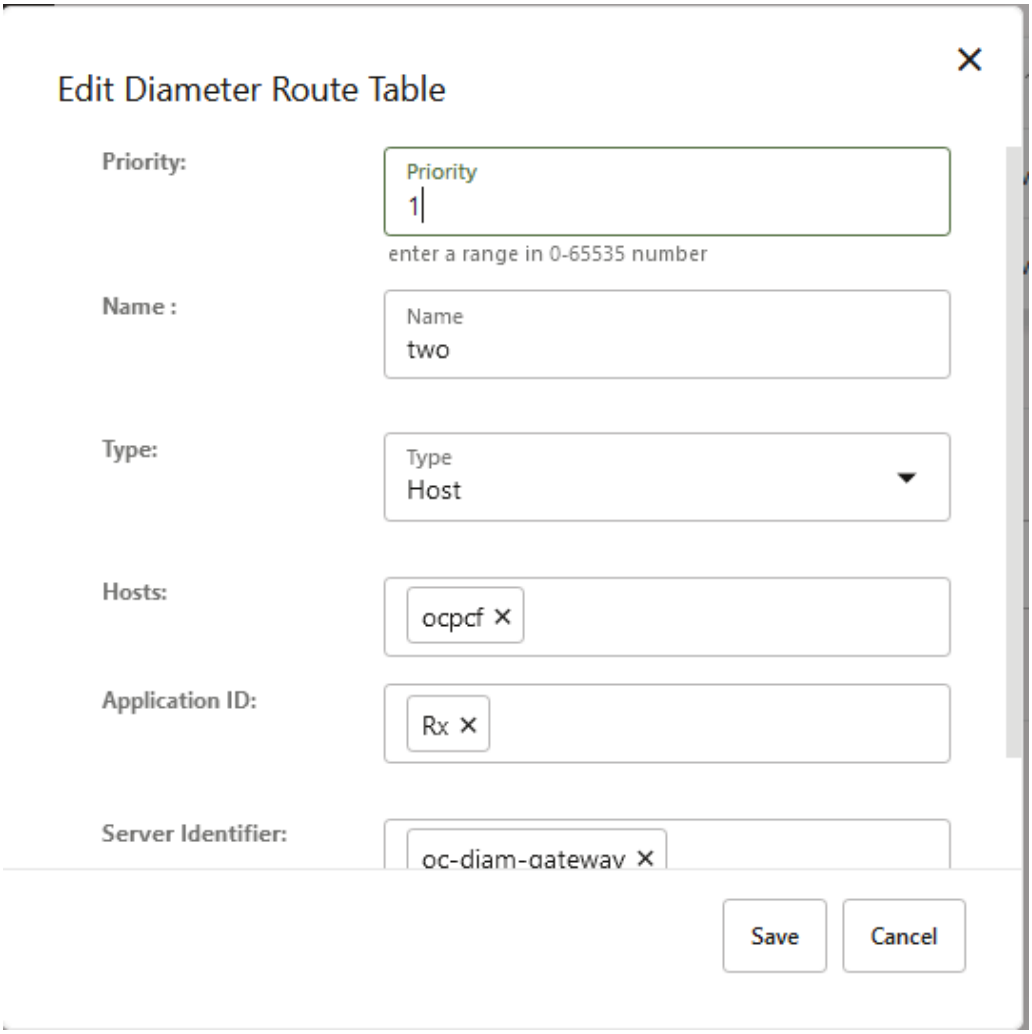


Figure 4-10 Adding Second Diameter Routing Element



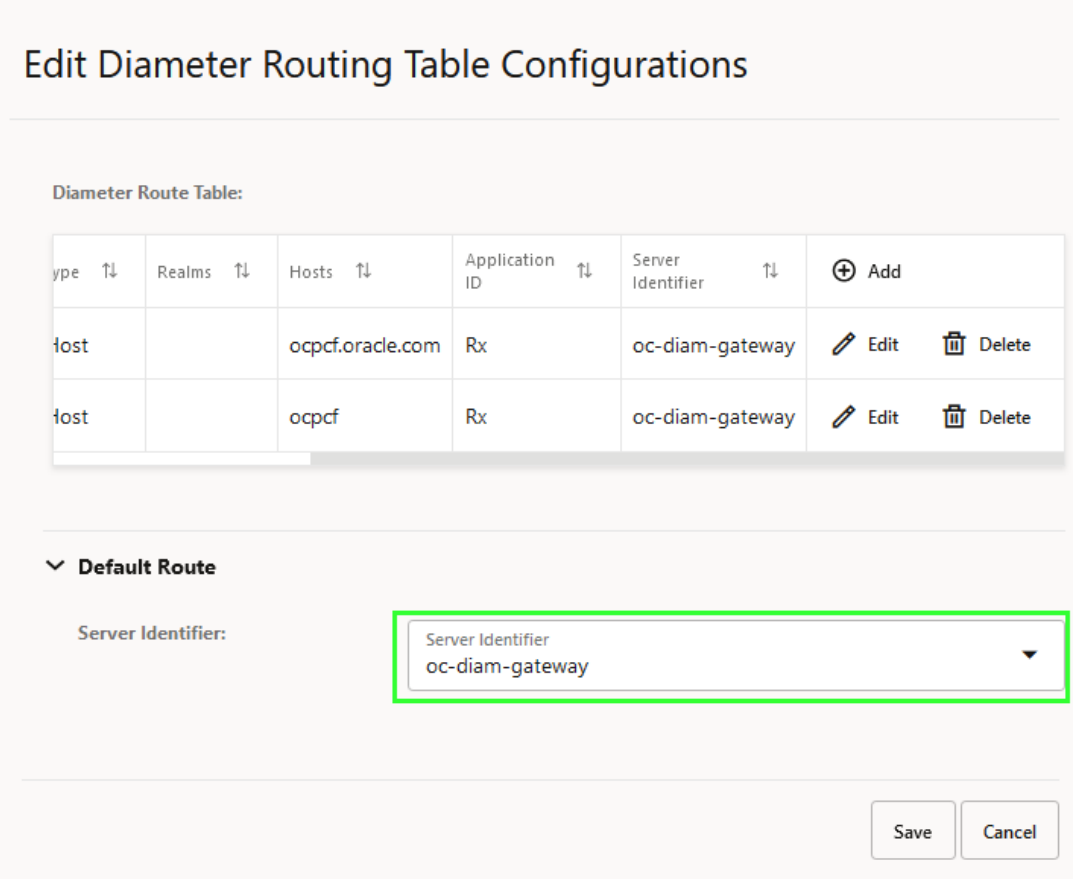
c. Click **Save** on the **Add Diameter Routing Table** dialog box.

5. On the **Edit Diameter Routing Table Configurations** page, expand the **Default Route** group.
6. Enter a value for the **Server Identifier** drop-down list.
   The server identifier drop-down list shows the list of the configured peer nodes on the **Peer Nodes** configuration page. For more information on configuring Peer Nodes, see Peer Nodes.

   On selecting any of the values, make sure that the name is the same as the value of server identifier.

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

Figure 4-11 Diamter Routing Table Configurations



7. Click **Save**.
   The configuration gets listed on the **Diameter Routing Table Configurations** page.

> **Note**
>
> Use or available under the **Actions** column to update or delete the Diameter Routing Table configurations.

4.5.4 Diameter Error Codes Configurations

This section describes how to customize the Diameter error codes according to the network requirements using the Diameter Error Codes page.

The **Diameter Error Codes** page on CNC Console allows users to view and edit conditions, which are defined by default for the Binding Support Function (BSF) network function. This page also provides the options to import and export diameter error codes.

The following table describes the diameter errors supported by BSF:

Table 4-39 Error Codes and Responses

Condition Name	Error Message	Diameter Result Code
Unable to Route Diameter Message	BSF cannot route a diameter message to the selected destination.	3002 DIAMETER_UNABLE_TO_DELIVER
Diameter Request Message Timeout	BSF sent a diameter request message to the selected destination but did not receive a response in the specified time.	3002 DIAMETER_UNABLE_TO_DELIVER
Unsupported Diameter Interface Received	A diameter message was received for a diameter interface that is not supported by BSF.	3007 DIAMETER_APPLICATION_UNSUPPORTED
AVP Value Invalid	A diameter message was received containing an AVP with a value that is invalid (indicated in FailedAVP)	5004 DIAMETER_INVALID_AVP_VALUE
Required AVP Not Present	A diameter message was received that did not have a required AVP (indicated in FailedAVP)	5005 DIAMETER_MISSING_AVP
Binding Not Found	A binding record was not found for the subscriber key(s) present in the Diameter AAR Initial message	5065 IP-CAN_SESSION_NOT_AVAILABLE
Internal Error	An internal failure occurred	5012 DIAMETER_UNABLE_TO_COMPLY

Table 4-40 Error Codes and Responses

Condition Name	Error Message	Diameter Result Code
Unable to Route Diameter Message	BSF cannot route a diameter message to the selected destination.	3002 DIAMETER_UNABLE_TO_DELIVER
Diameter Request Message Timeout	BSF sent a diameter request message to the selected destination but did not receive a response in the specified time.	3002 DIAMETER_UNABLE_TO_DELIVER
Unsupported Diameter Interface Received	A diameter message was received for a diameter interface that is not supported by BSF.	3007 DIAMETER_APPLICATION_UNSUPPORTED
AVP Value Invalid	A diameter message was received containing an AVP with a value that is invalid (indicated in FailedAVP)	5004 DIAMETER_INVALID_AVP_VALUE
Required AVP Not Present	A diameter message was received that did not have a required AVP (indicated in FailedAVP)	5005 DIAMETER_MISSING_AVP
Binding Not Found	A binding record was not found for the subscriber key(s) present in the Diameter AAR Initial message	5065 IP-CAN_SESSION_NOT_AVAILABLE

Table 4-40 (Cont.) Error Codes and Responses

Condition Name	Error Message	Diameter Result Code
Internal Error	An internal failure occurred	5012 DIAMETER_UNABLE_TO_COMPLY

Table 4-41 Error Codes and Responses

Condition Name	Error Message	Diameter Result Code
Unable to Route Diameter Message	BSF cannot route a diameter message to the selected destination.	3002 DIAMETER_UNABLE_TO_DELIVER
Diameter Request Message Timeout	BSF sent a diameter request message to the selected destination but did not receive a response in the specified time.	3002 DIAMETER_UNABLE_TO_DELIVER
Unsupported Diameter Interface Received	A diameter message was received for a diameter interface that is not supported by BSF.	3007 DIAMETER_APPLICATION_UNSUPPORTED
AVP Value Invalid	A diameter message was received containing an AVP with a value that is invalid (indicated in FailedAVP)	5004 DIAMETER_INVALID_AVP_VALUE
Required AVP Not Present	A diameter message was received that did not have a required AVP (indicated in FailedAVP)	5005 DIAMETER_MISSING_AVP
Binding Not Found	A binding record was not found for the subscriber key(s) present in the Diameter AAR Initial message	5065 IP-CAN_SESSION_NOT_AVAILABLE
Internal Error	An internal failure occurred	5012 DIAMETER_UNABLE_TO_COMPLY

Editing Diameter Error Codes

To edit any of the defined conditions, perform the following steps:

1. From the navigation menu, click **BSF**, then select **Diameter Configurations**, and click **Diameter Error Codes**.
   This opens the Diameter Error Codes page that lists the condition names along with their **Result code**, **Vendor Id**, and **Application Error Code**.
2. Click **Edit** against the condition that you need to customize.
   This opens the Edit Diameter Error Codes page.
3. Update the required values for the fields, described in the following table:

Table 4-42 Parameters for Edit Diameter Error Codes

Parameter	Description
Use Experimental Result	Indicates whether to use the Result Code AVP (268) or Experimental Result AVP (297) when an error result is generated by BSF.
Result Code	Specifes the Diameter result code for a defined condition. When **Use Experimental Result** switch is disabled, this field cannot be left blank. **Note**: The value must be a standard diameter result code as defined in the RFC 6733.
Experimental Result Code	Specifies the custom Diameter result code for a defined condition. When **Use Experimental Result** switch is enabled, this field cannot be left blank. **Note**: The value must be a standard diameter result code, from 3000 to 9999, as defined in the *3GPP Technical Specification 29.230*
Vendor Id	Specifies the Vendor ID of the operator or governing body that manages the code entered by the user in the **Experimental Result Code** field. When **Use Experimental Result** switch is enabled, this field cannot be left blank.
Error Message	A message that explains the nature of the error. This error message is only for user understanding and must not be parsed by network entities.

4. Click **Save**.

Importing Diameter Error Codes

To import Diameter error codes, perform the following steps:

1. Click **Import**.
   The **File Upload** dialog box opens.
2. Using the **Drag and Drop** button, upload the file in JSON format.
3. Click **Import**.

Exporting Diameter Error Codes

To export Diameter error codes, click **Export**. A file named `bsf.diameter.errorcodes.json` is saved to your device.

4.6 Status and Query

This section describes how to retrieve status of BSF profile registration and query sessions using the Session Viewer page.

4.6.1 Session Viewer

You can use the Session Viewer page to query and view PCF binding information for a UE by using any of the following parameters:

- SUPI

- GPSI
- UE Address

To access this screen from the Home screen of CNC Console, click **BSF** and then **Session Viewer**.

To view PCF bindings of a specific UE, perform the following steps:

1. On the **Session Viewer** page, enter the value of SUPI, GPSI, or UE Address.
Query Parameters Session Viewer

Table 4-43 Address

Parameter	Description
IPv4 Address	Specifies the IP addresses in IPv4 format
IPv6 Prefix	Specifies the IPv6 Address Prefix. Note: When you use IPv6 prefix to query a session, ensure that you provide the full notation value. **Example**: `2011:db8:3c4d:0:0:0:0:0/48`
IP Domain	Specifies the IPv4 address domain identifier
MAC Address	Specifies the MAC address, which is formatted as six groups of two hexadecimal digits separated by colons (:) or hyphens (-). For example, in the format hh:hh:hh:hh:hh:hh.

Table 4-44 User

Parameter	Description
SUPI	Specifies the Subscription Permanent Identifier. For example - `imsi-450081100100001`.
GPSI	Specifies the Generic Public Subscription Identifier. For example - `msisdn-9192503899`.

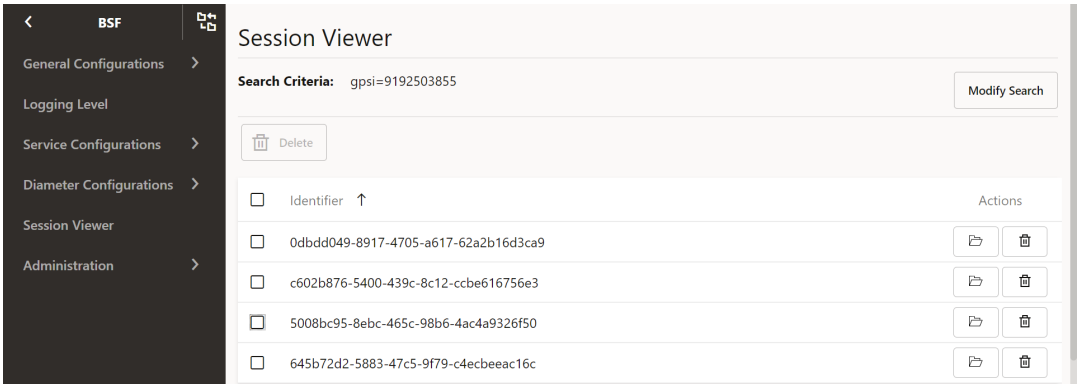
Table 4-45 Slice Information/DNN

Parameter	Description
DNN	Specifies the Data Network Name (DNN).
S-NSSAI_SST	Specifies the Slice or Service type for a given S-NSSAI (Single Network Slice Selection Assistance Information).
S-NSSAI_SD	Specifies the Slice Differentiator (SD) for a given S-NSSAI (Single Network Slice Selection Assistance Information). This optional information is used to difference slice or service type across multiple network slices.

2. Click **Query**.
The page displays all the PCF binding records of the UE. For georedundant BSF deployments, the query results include PCF binding data across all sites.

   The following screenshot shows the binding IDs when the user searches with GPSI as 9192503855:

Figure 4-12 Query Results using Session Viewer



If binding data is not available, the page displays **No bindings found** message.

> **Note**
>
> As SUPI and GPSI are optional parameters, PCF may not add these values when sending a query request. In such cases, BSF returns a **No session found** message despite binding data being available in the database.

Delete Bindings in Session Viewer

Upon receiving the search results for a query, user may want to delete one or multiple PCF binding IDs on the Session Viewer page.

To delete PCF binding IDs individually, click delete under **Actions** against the required binding ID.

To delete multiple or all the binding records for a subscriber, select binding IDs, then click **Delete** button, and select **YES** on the dialog box.

For georedundant BSF deployments, user can delete PCF binding data across all sites by selecting the binding records from the query results.

4.6.2 BSF NF Data

This section provides information on NF status.

4.6.2.1 BSF Registration Profile

This page lists the BSF profile registered with NRF.

To make updates to any of the parameters of the BSF registration profile, perform the following steps:

1. Click **Edit** button.
2. Update the values of the required parameters.
3. Click **Save**.

To dowload the BSF profile, click **Download** button. A file named `bsfRegistrationProfile.json` is saved on your system.

4.6.2.2 BSF NRF Status

This page provides the consolidated status of BSF instances registered with NRF.

On the **BSF NRF Status** page, you can view the status of BSF and the NRFs deployed in the cluster.

To view the page:

1. From the navigation menu under **BSF** navigate to **Status and Query**. Click **BSF NRF Data** and select **BSF NRF Status**.
   This opens the **BSF NRF Status** page.
2. The page displays the registered BSF instances and current NRF health status.

Figure 4-13 BSF Registration Status at NRF

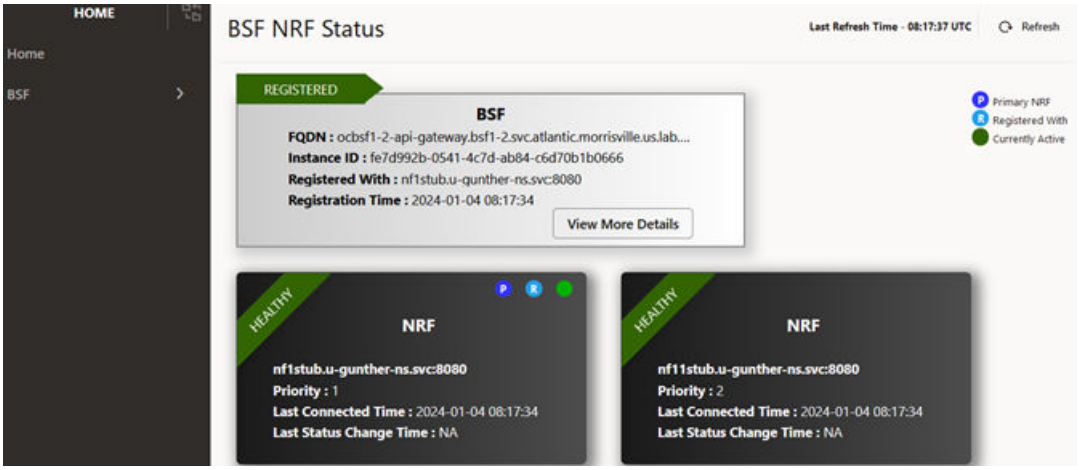
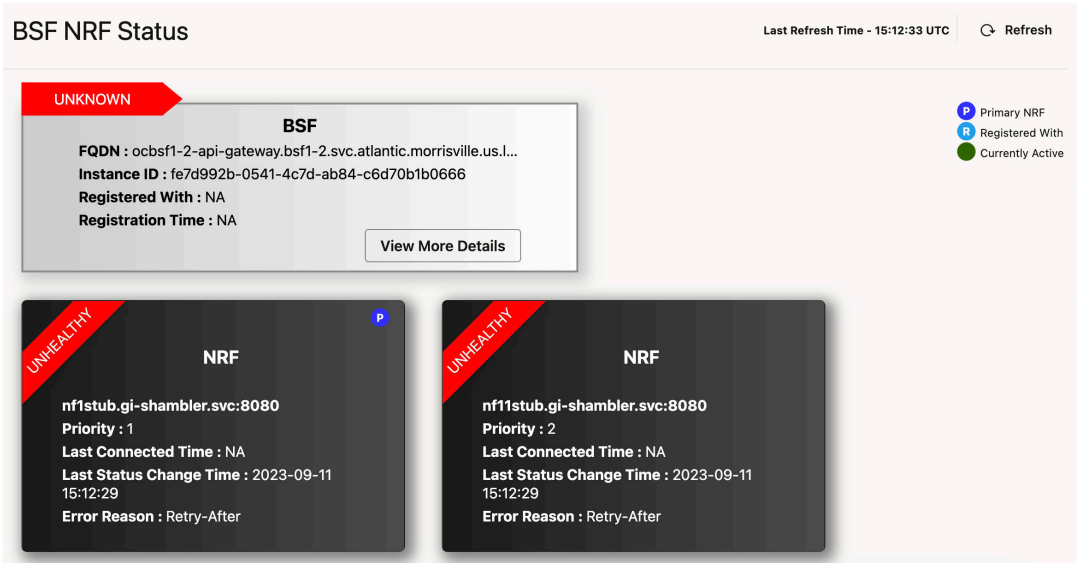


Figure 4-14 BSF NRF Health Status



3. **For BSF**

   You can view the following details for BSF:

- **BSF status with NRF** - It shows whether the BSF instance is **REGISTERED**, **SUSPENDED**, or **DEREGISTERED** with NRF.
- **FQDN** - It shows the FQDN of the BSF registered with NRF.
- **Instance ID** - It shows the unique Instance ID of BSF was registered with NRF.
- **Registration Time** - It shows the time at which BSF was registered with NRF.

If you want to view more details of the BSF instance such as its registration profile, click **View More Details**. It opens the **NF Registration Profile** page.

4. **For NRF**

   You can view the following details for NRF:

   - **Health Status** - This ribbon-styled badge shows the health status of the NRF instance. It could be in either healthy or unhealthy state.
   - **Primary NRF** - The circular icon with the label P indicates that the NRF is primary.
   - **Active Status** - The pulsating green circular icon shows that the NRF is currently active.
   - **FQDN** - It shows the FQDN of the NRF.
   - **Priority** - It shows the priority of the NRF instances. An NRF instance with priority 1 is treated as primary NRF.
   - **Last Connected Time** - It shows the time when BSF last connected with primary NRF.
   - **Last Status Change Time** - It shows the time when the NRF status changed.

   When the status of an NRF instance changes from healthy to unhealthy, the error reason is also displayed on the page.

   The number of NRF's displayed on the page are dynamic and get updated according to the NRF's configured in the network.

5. Based on when the data refreshes, the **Last Refresh Time** on the page is also updated.

In case of any network error, the page displays **Unable to load NRF data** error.

4.6.3 Active Session Query

This section describes the **Active Session Query** tab under **Status and Query** in CNC Console.

This page allows you to query active sessions count instantly.

To get the active sessions count, click **Query Active Sessions**.

Sample output is as follows:

```
Count: 7032
DateTime: 07-07-2022 11:42:28
```

4.7 Administration

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

4.7.1 Import and Export

This section describes how to perform the bulk export or bulk import of the managed objects (MOs) configured on BSF.

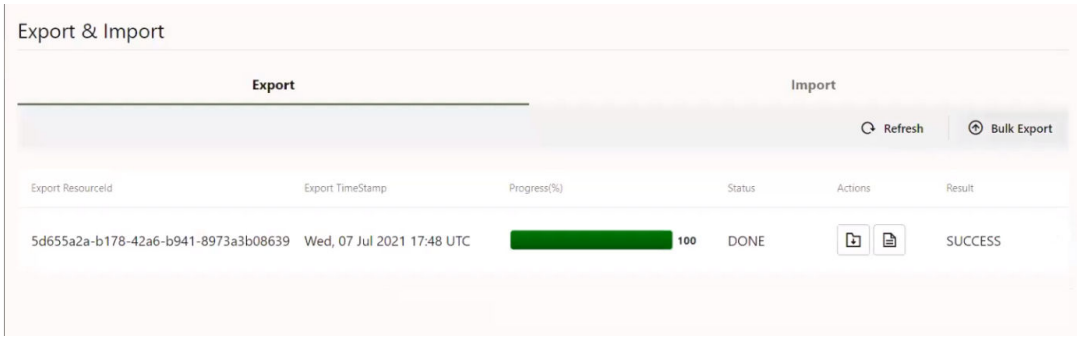
You can perform the bulk export and import of BSF data using the following methods:

- **Using CNC Console for BSF**:
  BSF provides the GUI to perform bulk export and import of BSF data.

  To access the export and import functionality from the CNC Console home page, expand **BSF**, navigate to **Administration**, and select **Import & Export**.

  The page displays the **Export** and **Import** tabs. By default, the **Export** tab remains selected. The following screen capture illustrates an example of the **Import & Export** page:

Figure 4-15 Import & Export



You can perform the following operations using the **Import & Export** page:

- Exporting BSF Configurations
- Importing BSF Configurations

> **Note**
>
> - Importing the Overload Threshold Profile will be rejected if the CPU validation mentioned under `Configure Threshold Values` section in Overload Control Threshold fails for any of the three threshold levels.
> - The service names mentioned in the json file used to import the Overload Threshold Profile must be same as mentioned in the exported json file.
> - The default Overload Threshold Profile cannot be exported or imported. The default Overload Threshold Profile must be customized with a different profile name before exporting.

- **Using REST API for BSF**:
  BSF provides REST APIs to bulk export and import BSF data. For more information about REST API configuration, see Using REST API for BSF Import & Export.

> **Note**
>
> The following message priority data that was exported prior to BSF 23.2.0 cannot be imported as the data may be corrupt:
>
> - message containing Sd as interface
> - Sy-SLR as condition message
>
> The data with Sd interface or Sy-SLR condition messages that are exported only with BSF 23.2.0 or later versions can be imported.

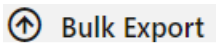
4.7.1.1 Exporting BSF Configurations

The export functionality allows you to export BSF configurations with the respective data.

The BSF data export is aligned with the left navigation menu options under BSF on the CNC Console. You can export either all the configurations or the configurations of the selected menu options.

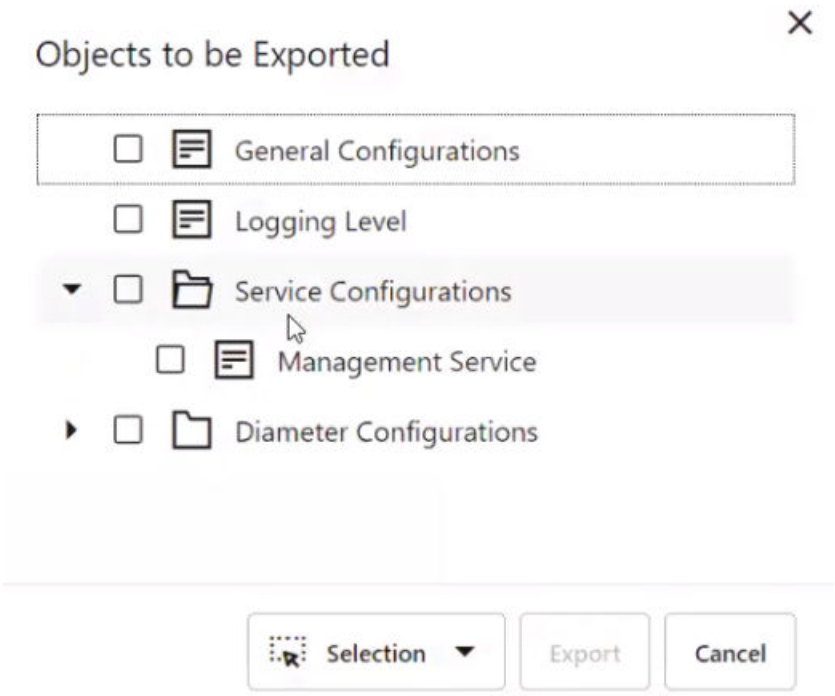
To export BSF configuration data::

1. From **BSF**, navigate to **Administration**, and select **Import & Export**.
   This opens the **Import & Export** page, displaying the **Export** and **Import** tabs. By default, the **Export** tab remains selected.
2. Click



.
This opens the **Objects to be Exported** dialog box, displaying the list of BSF configurations in a menu tree structure. The dialog box allows you to select the configurations to be exported. The following screen capture displays an illustration of the Objects to be Exported dialog box:

Figure 4-16 Objects to be Exported dialog box



3. In the dialog box, select the configurations according to the export requirement. Selecting or deselecting a parent folder automatically selects or deselects all the child nodes respectively.

> **Note**
>
> To select or deselect all the configurations, click Selection and perform the required operation.

4. Click **Export**.

> **Note**
>
> Click Cancel to discard the export operation.

This starts the export of all the selected configurations. A row is created in the export status table on the **Import & Export** page, displaying the export status with the following details:

- **Export ResourceId**: A new export resource ID is generated for each export operation. You can use this ID to get the export status.
- **Creation TimeStamp**: The timestamp of generation of **Export ResourceId**.
- **Progress (%)**: Shows the export progress in form of a percentage bar. The page auto refreshes the status until the progress reaches 100 percent.
- **Status**: The status of the export operation. It can be any of the following:

  - **INIT**: The validation of policies is in progress, and the export of the configurations has not yet started.
  - **IN_PROGRESS**: The export is running.
  - **DONE**: The export is complete.
- **Actions**: Provides the buttons to download the following:
  - **Export configuration files in ZIP file format**: The exported configurations in ZIP file format. The ZIP file contains the configuration data in JSON file format. You can download the exported data by clicking  under the **Action** column.
  - **Export report in TEXT file format**: The export report provides results for each JSON file present in the exported ZIP file. It also provides the reason for failure in case the export of any of the configurations fails.

    You can download the export report by clicking  under the **Action** column.

    > **Note**
    >
    > The buttons remain enabled only for the export operation with **DONE** status.
- **Result**: Provides the result of an export operation. This result is available only for the export operations with **DONE** status. Following are the possible values:
  - **SUCCESS**: The export is successful
  - **FAILED**: The export fails
  - **PARTIAL_SUCCESS**: The export is partially successful

4.7.1.2 Importing BSF Configurations

The import functionality allows you to import BSF data configurations. Using this functionality, you can import the same set of BSF data to different BSF systems.
To import BSF data in JSON or ZIP file format:

1. From **BSF**, navigate to **Administration**, and select **Import & Export**.

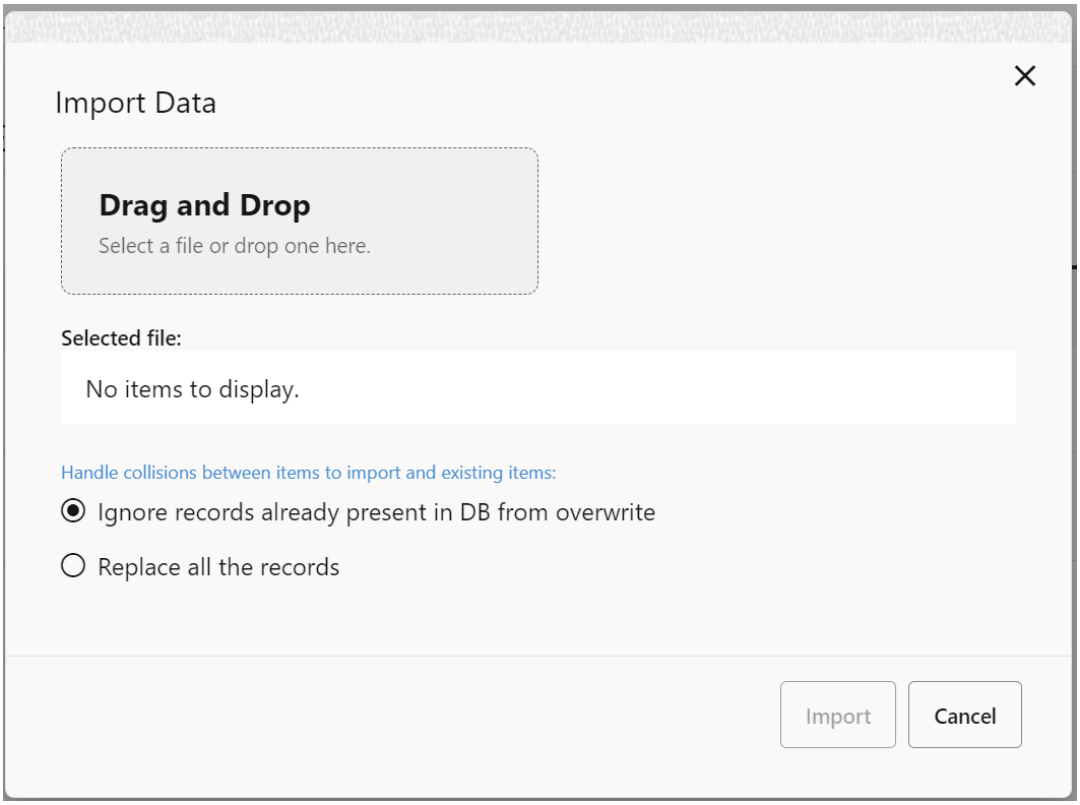
   This opens the **Import & Export** page, displaying the **Export** and **Import** tabs. By default, the **Export** tab remains selected.

2. Select the **Import** tab and click 

.

   This opens the **Import Data** dialog box.

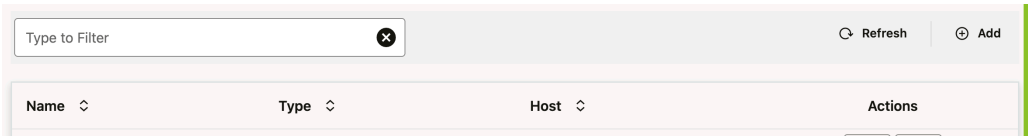
Figure 4-17 Import Data



3. Upload the file in JSON or ZIP format by using the **Drag and Drop** button.
4. Select any of the following options from **Handle collisions between items to import the existing item**.
   - **Attribute Configurations Screens**:

> **Note**
>
> This option is applicable to all the atttribute configuration screens such as **Data Sources** under **Data Source Configurations** or **Subscriber Activity Logging** under **Loggging Configurations** which have ⊕ Add button at the top right corner along with a table. In such screens each row is considered as managed object.

Figure 4-18 Sample Attribute Configurations Screen



Conflict Resolution Strategy

– **Ignore records already present in DB from overwrite** : Ignores records already present in the database and does not overwrite. For each object in the import file,

if the object already exists in the system, the import does not update the object with the configurations provided in the import file. If an object does not exists, then it is added to the system.

- **Replace all the records** : For each object in the import file, if the object already exists in the system, the import replaces the object with the configuration provided in the import file. If an object does not exist, then it is added to the system.
  If an object existing in the system and is not present in the imported file, it is retained in the system.

- **Service Configuration Screens**:

> **Note**
>
> This option is applicable to all the service configuration screens such as **Management Service** under **Service Configurations** or **Settings** under **Diameter Configurations**, which have Edit button at the top right corner along with a table.

Figure 4-19 Sample Service Configurations Screen

Conflict Resolution Strategy

- **Ignore records already present in DB from overwrite** : Ignores the records and data which are getting imported. For each object in the import file, the imported record will be ignored.
- **Replace all the records**: For each object in the import file, data to be imported will overwrites the existing data in the database, irrespective of whether the object is already present in the database or not.

5. Click **Import**.

> **Note**
>
> Click **Cancel** to discard the import operation.

This starts the import of configuration objects and their settings to the database. A row is created in the Import status table, displaying the import status with the following additional details:

- **Import ResourceId**: A new import resource ID is generated for each import operation. You can use this ID to get the import status.
- **Creation TimeStamp**: The timestamp of generation of **Import ResourceId**.
- **Progress (%)**: Shows the import progress in form of the percentage bar. The page auto refreshes the status until the progress reaches 100 percent.

- **Status**: The status of the import operation. It can be any of the following:
  - **IN_PROGRESS**: The import is running.
  - **DONE**: The import is complete.
- **Actions**: Provides a button to download the import report in text format. This button gets enabled once the status is **DONE**. The report provides results for each JSON file present in the imported ZIP file. You can download the import report by clicking  under the **Action** column.
- **Result**: Provides the result of an import operation. This result is available only for operations with **DONE** status. Following are the possible values:
  - **SUCCESS**: The import is successful
  - **FAILED**: The import has failed
  - **PARTIAL_SUCCESS**: The import is partially successful

4.7.1.3 Using REST API for BSF Import & Export

This section describes how to perform the bulk export or import of BSF configurations and BSF Data using REST APIs. BSF provides cURL commands for export and import.

cURL Commands for Bulk Import

Import:

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

where,

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

<ipAddress>:<port> is the host and port where CNC BSF is running.

Import Report:

```
curl -X GET "http://<ipAddress>:<port>/oc-bsfconfiguration/v1/administration/import/
{importResourceId}/report" -H "accept: application/octet-stream"
```

where, *<importResourceId>* is the resource id generated in response to the POST request for import. The `ResourceId` is the background task id for the POST operations. This id can be used to track the import requests, and download the data.

Import Status:

```
curl -X GET "http://<ipAddress>:<port>/oc-bsfconfiguration/v1/administration/import/
{importResourceId}/status/<importResourceId>/status" -H "accept: application/json"
```

For more information about Bulk Import REST APIs, see "Bulk Import Export Controller" in *Oracle Communications Cloud Native Core BSF REST Specification Guide*.

cURL Commands for Bulk Export

Export All:

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

where, *<ipAddress>:<port>* is the host and port where CNC BSF is running.

Export with Managed Objects:

```
curl -X POST "http://<ipAddress>:<port>/oc-bsf-configuration/v1/administration/export/?
managedObjects=PCF%20Session%20Management" -H "accept: */*" -d""
```

Download:

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

where, *<exportResourceId>* is the resource id generated in response to the POST request for export. The `ResourceId` is the background task id for the POST operations. This id can be used to track the export requests, and download the data.

Export Report:

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

Export Status:

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

For more information about Bulk Export REST APIs, see "Bulk Import Export Controller" in *Cloud Native Binding Support Function REST Specification Guide*.

4.8 Controlled Shutdown Configurations

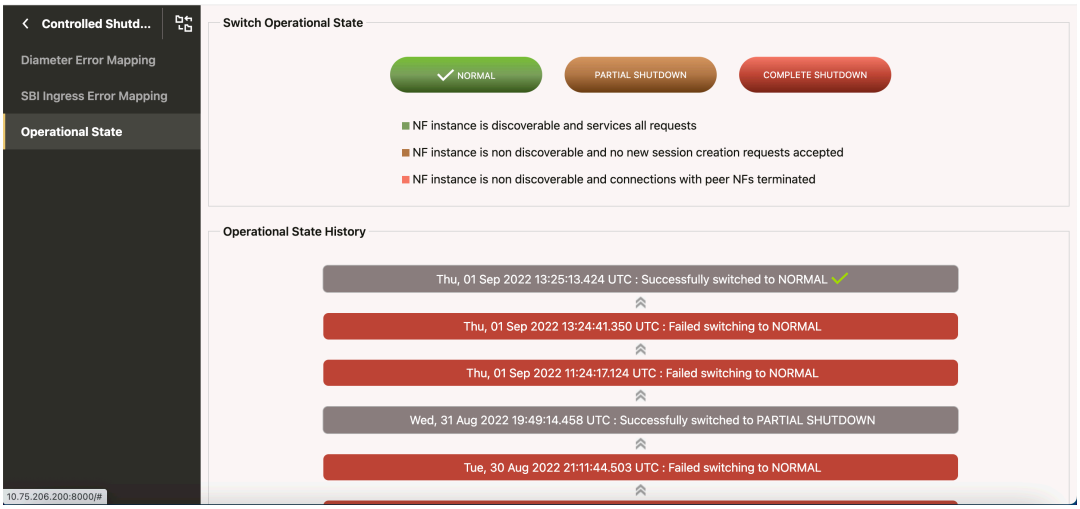
This section describes how to perform Controlled Shutdown configurations for Diameter and Ingress interface.

4.8.1 Operational State

To change Operational State of a site:

- From the navigation menu, under **BSF**, click **Controlled Shutdown**, and then select **Operational State**.
  This opens the page displaying the two groups, **Switch Operational State** and **Operational State History**:

  Figure 4-20 Operational State



- Switch Operational State It displays the following operational states:
  - NORMAL: NF instance is discoverable and services all requests.
  - PARTIAL SHUTDOWN: NF instance is non discoverable and no new session creation requests accepted.
  - COMPLETE SHUTDOWN: NF instance is non discoverable and no new session creation requests accepted.

> **Note**
>
> By default, NORMAL state is assigned to a site. The current state of any site can be identified with a tick mark.

You can switch to a different operational state by clicking the NORMAL, PARTIAL SHUTDOWN, or COMPLETE SHUTDOWN button.

- Operational State History: It displays the history of the operational states along with the timestamp.

> **Note**
>
> It displays maximim of ten records at a time. On scrolling further, another set of ten records is displayed. The maximum number of record maintained is hundred.

4.8.2 Diameter Error Mapping

To configure Diameter Error Mapping, perform the following steps:

1. From the navigation menu under **BSF**, click **Controlled Shutdown** and then select **Diameter Error Mapping**.
   This opens the **Diameter Error Mapping** page. The page lists the existing configurations. You can add or import new diameter error mapping configurations using this page.

   > **Note**
   >
   > Click Export to download the available listings in the JSON file format on your system.

2. Click Add .
   This opens the Create Diameter Error Mapping page.
3. On the **Create Diameter Error Mapping** page, enter the following information:

Table 4-46 Create Diameter Error Mapping

Field Name	Description
Message Type	Type of the request

Table 4-46 (Cont.) Create Diameter Error Mapping

Field Name	Description
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of congestion control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • CUSTOM_RESULT_CODE **Note**: When the CUSTOM_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Use Experimental Result Code**: This is disabled by default. You can enable it by clicking the icon against it. When it is enabled, Vendor ID field is poplulated on the page: – **Vendor ID**: Enter a valid value to specify vendor ID.

4. Click **Save**.
   The configuration gets listed on the **Diameter Error Mapping** page. The page defines the Diameter Error Mapping configuration in the BSF database and it is available to be used in a BSF.

> **Note**
>
> Use  or  available under the **Actions** column to update or delete the configuration.

Importing Diameter Error Mapping

To import Diameter Error Mapping configuration:

1. Click  .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

4.8.3 SBI Ingress Error Mapping

To configure SBI Ingress Error Mapping, perform the following steps:

1. From the navigation menu, under **BSF**, click **Controlled Shutdown**, and then select **SBI Ingress Error Mapping**.
   This opens the SBI Ingress Error Mapping page.
2. Click Edit.
   This opens the Edit SBI Ingress Error Mapping page.

3. Click Add .

   This opens the Add SBI Ingress Error Mapping page.

4. Enter values for the available input fields as described in the following table:

Table 4-47 Ingress Error Mapping Configurations

Field Name	Description
Id	Specifies the list of IDs available for BSF.
Error Code Profile	Select an error code profile from the dropdown list. It displays the list of error profiles configured using the SBI Ingress Error Code Profiles Collection.

5. Click **Save** to save the Ingress error mapping.
   To discard the changes, click **Cancel**.

   The value gets listed on the SBI Ingress Error Mapping page. Use or available under the **Actions** column to update or delete the profile.

4.9 Overload and Congestion Control Configurations

This section describes how to perform overload and congestion control configurations.

To use the Error Code Profiles page to create and manage error code profiles in Overload Control Configurations for Diameter Gateway and SBI interface, see *SBI Ingress Error Code Profiles Collection* section.

> **Note**
>
> When overload control feature is enabled, it should be enabled for both Diameter gateway and SBI interface. The overload control manager needs data from both Ingress Gateway and Diameter Gateway to determine the overall load on BSF management. It is not possible to enable overload control for Diameter Gateway and disable the same in Ingress Gateway.

4.9.1.1 Load Shedding Profiles

This procedure provides information about how to create and manage load shedding profiles in Diameter Configurations.

The Load Shedding Profiles page allows you to create new and manage existing load shedding profiles. The page displays the list of defined profiles and provides the options to import and export data as well.

To configure Load shedding profiles, perform the following steps:

1. From the navigation menu, under **BSF**, click **Diameter Configurations**, and select **Load Shedding Profiles**.
   This opens the Load Shedding Profiles page.

2. Click Add .

This opens the Create Load Shedding Profiles page.

3. Enter values for the available input fields described in the following table:

Table 4-48 Load Shedding Profiles Configurations

Field Name	Description
Name	Unique name of the load shedding profile.
Scheme	Allows to configure the discard policy based on • Priority: to discard messages based on priority range • Priority and Percentage: to discard messages based on priority range and percentage for each range
Type	Defines the type of load shedding profile. You can select any of the following values from the drop-down list: • Congestion Control • Overload Control

To add load shedding rules for the profile type congestion control, perform the following steps:

a. Under **Load Shedding Rules**, click ⊕ Add.
This opens the **Add Load Shedding Rules** dialog box.

b. Enter values for the available input fields, described in the following table:

Table 4-49 Load Shedding Rules Configurations When the Selected Scheme is "Priority"

Field Name	Description
State	This field appears when the **Type** of load shedding profile is `Congestion Control`. Specifies the type of state for which the rule is being defined. Select any of the following values using the drop-down: • Danger of Congestion • Congested
Discard Priority	This field appears when the **Scheme** of load shedding profiles is `Priority`. Specifies the discard priority for the load shedding rule. The discard priority value can be a number from 0 to 15. Any request message with equal or greater priority is rejected.

Table 4-49 (Cont.) Load Shedding Rules Configurations When the Selected Scheme is "Priority"

Field Name	Description
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of congestion control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE **Note**: When the EXPERIMENTAL_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Vendor ID**: Enter a valid value to specify vendor ID.

Table 4-50 Load Shedding Rules Configurations When the Selected Scheme is "Priority and Percentage"

Field Name	Description
State	This field appears when the **Type** of load shedding profile is `Congestion Control`. Specifies the type of state for which the rule is being defined. Select any of the following values using the drop-down: • Danger of Congestion • Congested
Discard Priority Percentage	Allows to configure the Discard Priority Percentage as explained in the following step.

c. To configure discard Priority Percentage, perform the following steps:

i. Under **Discard Priority Percentage**, click 

.
This opens the **Add Discard Priority Percentage** dialog box.

Enter values for the available input fields, described in the following table:

Table 4-51 Adding Discard Priority Percentage

Field Name	Description
Priority Range	Specifies the discard priority range for the load shedding rule. The discard priority value can be a number from 0 to 15. Any request message with equal or greater priority will be rejected based on the percentage discard configured.
Discard Percentage	Specifies the discard percentage for the specified priority range.

Table 4-51 (Cont.) Adding Discard Priority Percentage

Field Name	Description
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of congestion control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE **Note**: When the EXPERIMENTAL_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Vendor ID**: Enter a valid value to specify vendor ID.

ii. Click **Save** to save the discard priority percentage.

d. Click **Save** to save the load shedding rule.

OR

To add load shedding rules for the profile type overload control, perform the following steps:

a. Under **Load Shedding Rules**, click ⊕ Add .
This opens the **Add Load Shedding Rules** dialog box.

b. Enter values for the available input fields, described in the following table:

Table 4-52 Load Shedding Rules Configurations When the Selected Scheme is "Priority"

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies. Select any of the following values using the drop-down list: • L1 • L2 • L3 **Note**: If the load levels are not configured, then level transitions will not happen and it will stay at the same level. Also, any existing L4 level data will be removed, as L4 is not supported.
Discard Priority	Specifies the discard priority for the load shedding rule. The discard priority value can be a number from 0 to 15. Any request message with equal or greater priority is rejected.

Table 4-52 (Cont.) Load Shedding Rules Configurations When the Selected Scheme is "Priority"

Field Name	Description
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of overload control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE **Note**: When the EXPERIMENTAL_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Vendor ID**: Enter a valid value to specify vendor ID.

Table 4-53 Load Shedding Rules Configurations When the Selected Scheme is "Priority and Percentage"

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies. Select any of the following values using the drop-down list: • L1 • L2 • L3 **Note**: If the load levels are not configured, then level transitions will not happen and it will stay at the same level. Also, any existing L4 level data will be removed, as L4 is not supported.
Discard Priority Percentage	Configure the discard priority percentage as explained in the following step.

c. To configure Discard Priority Percentage, perform the following steps:

i. Under **Discard Priority Percentage**, click ⊕ Add .
This opens the **Add Discard Priority Percentage** dialog box.

Enter values for the available input fields, described in the following table:

Table 4-54 Adding Discard Priority Percentage

Field Name	Description
Priority Range	Specifies the discard priority range for the load shedding rule. The discard priority value can be a number from 0 to 15. Any request message with equal or greater priority will be rejected based on the percentage discard configured.
Discard Percentage	Specifies the discard percentage for the specified priority range.
Answer with Result Code	Specifies the result code, returned in the answer response, when request message is rejected as part of congestion control. Users can select any of the following values from the drop-down menu: • DIAMETER_TOO_BUSY • DIAMETER_UNABLE_TO_COMPLY • DIAMETER_UNABLE_TO_DELIVER • EXPERIMENTAL_RESULT_CODE **Note**: When the EXPERIMENTAL_RESULT_CODE value is selected, the following two fields are populated on the page: • **Result Code**: Enter a custom result code. • **Vendor ID**: Enter a valid value to specify vendor ID.

ii. Click **Save** to save the discard priority percentage.

d. Click **Save** to save the load shedding rule.

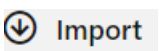
> **Note**
>
> You can not edit or delete the load shedding rule for an existing load shedding profile. As a workaround, you must create a new load shedding profile with the updated load shedding rule and delete the old load shedding profile.

4. Click **Save** to save the load shedding profile.
   To discard the changes, click **Cancel**

   The value gets listed on the Load Shedding Profiles page. Use  or  available under the **Actions** column to update or delete the profile.

Importing Load Shedding Profiles

To import load shedding profiles, perform the following steps:

1. Click 

   .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Exporting Load Shedding Profiles

To export load shedding profiles, click **Export**. A `json` file is saved to your device.

4.9.1.2 Message Priority Profiles

This procedure provides information about creating and managing message priority profiles in Diameter Configurations.

The Message Priority Profiles page allows you to create new and manage existing message priority profiles. The page displays the list of defined profiles and provides the options to import and export data.

To configure Message Priority profiles, perform the following steps:

1. From the navigation menu, under **BSF**, click **Overload Control Configurations**, select **Diameter**, and then select **Message Priority Profiles**.
   This opens the Message Priority Profiles page.
2. Click ⊕ Add .
   This opens the Create Message Priority Profiles page.
3. Enter values for the available input fields, described in the following table:

Table 4-55 Message Priority Profiles Configurations

Field Name	Description
Name	Unique name of the message priority profile.

To add message priority rules for the profile, perform the following steps:

a. Under **Message Priority Rules**, click ⊕ Add .
   This opens the **Add Message Priority Rules** dialog box.
b. Enter values for the available input fields, described in the following table:

Table 4-56 Message Priority Rules Configurations

Field Name	Description
Name	Specifies the unique name of the message priority rule.
Message Priority	Specifies the priority assigned to the message. It can be a number from 0 to 15.
Rule Priority	Specifies the priority assigned to the message priority rule.
Use DRMP Priority	When this switch is enabled, the priority for the message rule is assigned from DRMP AVP.

Table 4-57 Message Priority Rules Configurations - Conditions

Field Name	Description
Application	Specifies the type of application. Users can select the following value from the drop-down: • Rx
Message	Specifies the type of message for the selected application. The supported message values for each application type are as follow: • For Rx application, choose a value from AAR, STR, RAR, and ASR.

c. To add pre-defined AVP conditions, click ⊕ Add under **Add Pre Defined AVP Conditions**. On the **Add Pre Defined AVP Conditions** dialog box, select Name and enter values as described in the following table:

Table 4-58 Pre Defined AVP Conditions Configurations

Name	Values
`Called-Station-Id`	This AVP can be used only when the application type is specified a Rx. Users can enter multiple comma-separated values. **Note**: BSF supports wildcard format for this AVP.
`Rx-Request-Type`	This AVP can be used for Rx application with message specified as AAR. You can select any of the following valid values from the drop-down list: • INITIAL_REQUEST • UPDATE_REQUEST • PCSCF_RESTORATION_REQUEST
`Service-URN`	This AVP indicates that an AF session is used for emergency traffic. It is of type OctetString. Examples: "sos", "sos.fire", "sos.police" and "sos.ambulance". **Note**: BSF supports wildcard format for this AVP.
`MPS-Identifier`	This AVP indicates that an AF session relates to an MPS session and contains the national variant for MPS service name. It is of type OctetString. Example: NGN GETS
`MCPTT-Identifier`	This AVP includes either one of the namespace values used for MCPTT and may include the name of the MCPTT service provider. It is of type OctetString.
`MCVideo-Identifier`	This AVP includes the name of the MCVideo service provider. It is of type OctetString.
`Reservation-Priority`	This AVP is of type Enumerated and is specified in an AA-Request as the main AVP to associate a priority with a resource reservation or modification request. You can specify a value from 0 to 7 for this AVP.

Click **Save** to save the pre-defined AVP conditions for the message priority rule.

d. Click **Save** to save the message priority rule.

4. Click **Save** to save the message priority profile.
   To discard the changes, click **Cancel**

   The value gets listed on the Message Priority Profiles page. Use or available under the **Actions** column to update or delete the profile.

Importing Load Shedding Profiles

To import message priority profiles, perform the following steps:

1. Click Import .
   The page opens the **File Upload** dialog box.
2. Upload the file in JSON format by using the **Drag and Drop** button.
3. Click **Import**.

Exporting Message Priority Profiles

To export load shedding profiles, click **Export**. A `json` file is saved to your device.

4.9.2.1.1 Rate Limiting Policy

This procedure provides information about how to use the Rate Limiting Policy page to manage rate limiting policies for overload control on SBI interface.

To configure rate limiting policy, perform the following steps:

1. From the navigation menu, under **BSF**, click **Overload Control Configurations**, select **SBI**, then select **Rate Limiting**, and then select **Rate Limiting Policy**.
   This opens the Rate Limiting Policy page.
2. Click Edit.
   This opens the Edit Rate Limiting Policy page.
3. Enter values for the available input fields as described in the following table:

Table 4-59 Rate Limiting Policy Configurations

Field Name	Description
Enable Rate Limiting	Specifies whether to enable or disable rate limiting.
Sampling Period (in milliseconds)	Specifies the time frame for each cycle of rate limiting per service. Its default value is 200 ms.

4. Under **Rate Limit Policy**, click Add .

   This opens the Add Rate Limit Policy dialog box.
5. Enter values for the available input fields as described in the following table:

Table 4-60 Rate Limit Policy Configurations

Field Name	Description
Name	Specifies the name of the rate limit policy that is further used to determine a mapping between route and discard policy name per route.
Discard Priority	Specifies the discard priority for the rate limiting policy. Any request with message priority higher in value than the discard priority is rejected.
Action	Specifies the action taken when when requests are discarded. Currently, the only supported value is RejectWithErrorCode.
Scheme	Specifies the scheme for applying rate limiting. Currently, the only supported value is PriorityBased.
Error Code Profile	Specifies the list of error code profiles configured on the **Error Code Profiles** page.

6. Click **Save** to save the rate limit policy. The value gets listed under the **Rate Limit Policy** group.
   To discard the changes, click **Cancel**.

   Use or available under the **Actions** column to update or delete any given policy.
7. Click **Save** to save the rate limiting policy.
   To discard the changes, click **Cancel**.

4.9.2.1.2 Route Level Mapping

This procedure provides information about how to use the Route Level Mapping page to manage route level mapping for overload control on SBI interface.

To configure route level mapping, perform the following steps:

1. From the navigation menu, under **BSF**, click **Overload Control Configurations**, select **SBI**, then select **Rate Limiting**, and then select **Route Level Mapping**.
   This opens the Route Level Mapping page.
2. Click Edit.
   This opens the Edit Route Level Mapping page.
3. Under **Route Configuration**, click Add .

   This opens the Add Route Configuration dialog box.
4. Enter values for the available input fields as described in the following table:

Table 4-61 Rate Limiting Policy Configurations

Field Name	Description
Id	Specifies the list of route IDs available for BSF. Choose any value from the drop-down list: • BSF Management Register • BSF Management Deregister • BSF Management Discovery

5. Under **Rate Limiting**, click Add .

This opens the Add Method dialog box.

6. Enter values for the available input fields as described in the following table:

Table 4-62 Method Configurations

Field Name	Description
Http Method	Specifies the HTTP method. Depending on the value select for **Id**, you can select any of the following values from the drop-down list: • POST • PUT • GET • DELETE • PATCH
Message Rate (per sampling period)	Specifies the message rate per sampling period for a given method.
Rate Limit Policy	Select a rate limit policy from the drop-down list. It displays the list of rate limit policies configured using the Rate Limiting Policy page.

7. Click **Save** to save the method. The value gets listed under the **Rate Limiting** group.
   To discard the changes, click **Cancel**.

   Use  or  available under the **Actions** column to update or delete any given policy.
8. Click **Save** to save the route configuration.
   To discard the changes, click **Cancel**.
9. Click **Save** to save the route level mapping.
   To discard the changes, click **Cancel**.

4.9.2.2.1 Discard Policy Mapping

This procedure provides information about how to use the Discard Policy Mapping page to manage discard policy mapping in Overload Control Configurations for SBI interface.

To configure Discard Policy Mapping, perform the following steps:

1. From the navigation menu, under **BSF**, click **Overload Control Configurations**, select **SBI**, then select **Overload Control**, and then select **Discard Policy Mapping**.
   This opens the Discard Policy Mapping page.
2. Click Edit.
   This opens the Edit Discard Policy Mapping page.
3. Enter values for the available input fields as described in the following table:

Table 4-63 Discard Policy Mapping Configurations

Field Name	Description
Enable Overload Control	Specifies whether to enable or disable overload control.
Sampling Period (in milliseconds)	Specifies the time frame for each cycle of overload control per service. Its default value is 200 ms.

4. Under **Mappings**, click Add .

   This opens the Add Mappings dialog box.

5. Enter values for the available input fields as described in the following table:

Table 4-64 Mappings Configurations

Field Name	Description
Service Name	Specifies the name of the microservice that is further used to determine a mapping between service and discard policy name per service. **BSF Management** is the only supported value for this field.
Policy Name	Specifies the name of the discard policy that is used to determine a mapping between service and discard policy name per service. The drop-down list shows the policies configured using the Discard Policy page.

6. Click **Save** to save the mappings.
   To discard the changes, click **Cancel**

   The value gets listed under the **Mappings** group on the Discard Policy Mapping page. Use or available under the **Actions** column to update or delete the mappings.

7. Click **Save** to save the discard policy mapping.
   To discard the changes, click **Cancel**.

4.9.2.2.2 Discard Policy

This procedure provides information about how to use the Discard Policy page to manage discard policies for overload control for SBI interface.

To configure discard policy, perform the following steps:

1. From the navigation menu, under **BSF**, click **Overload Control Configurations**, select **SBI**, then select **Overload Control**, and then select **Discard Policy**.
   This opens the Overload Control Discard Policy page.
2. Click Edit.
   This opens the Edit Overload Control Discard Policy page.
3. Click Add .

   This opens the Add Discard Policies page.

4. Enter values for the available input fields as described in the following table:

Table 4-65 Discard Policy Configurations

Field Name	Description
Name	Specifies the unique name of the discard policy.

Table 4-65 (Cont.) Discard Policy Configurations

Field Name	Description
Scheme	Specifies the criteria of dropping requests for a microservice. It could be either priority based or percentage based. If you select the value as Priority Based, configure the values of the parameters under Priority Based Policies. For Percentage Based scheme, configure the parameters under Percentage Based Policies.

To add priority based policies, perform the following steps:

a. Under **Priority Based Policies**, click Add.
This opens the **Add Priority Based Policies** dialog box.

b. Enter values for the available input fields as described in the following table:

Table 4-66 Priority Based Policies Configurations

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies. Select any of the following values using the drop-down list: • L1 (Load Level 1) • L2 (Load Level 2) • L3 (Load Level 3)
Discard Priority	Specify the discard priority for the discard policy rule. Any request message with equal or lower message priority is rejected. **Note**: 1 is considered as the highest message priority.
Error Code Profile	Select an error code profile from the drop-down list. It displays the list of error profiles configured using the Error Code Profile page.
Action	Specifies the action taken when selected requests are rejected. Currently, it only supports the action to reject requests based on error code.

OR

Table 4-67 Percentage Based Policies Configurations

Field Name	Description
Level	Specifies the name of the level. The name specified in this parameter must match the level name in Ingress Gateway's ocdiscardpolicies. Select any of the following values using the drop-down list: • L1 (Load Level 1) • L2 (Load Level 2) • L3 (Load Level 3)

Table 4-67 (Cont.) Percentage Based Policies Configurations

Field Name	Description
Discard Percentage	Specify the discard percentage for the policy rule. The specified percentage of the calculated rate for service in previous sampling period is discarded in current sampling period.
Error Code Profile	Select an error code profile from the drop-down list. It displays the list of error profiles configured using the Error Code Profile page.
Action	Specifies the action taken when selected requests are rejected. Currently, it only supports the action to reject requests based on error code.

c. Click **Save** to save the discard policy.
To discard the changes, click **Cancel**.

5. Click **Save** to save the overload control discard policy.
To discard the changes, click **Cancel**

The value gets listed on the Overload Control Discard Policy page. Use or available under the **Actions** column to update or delete any given policy.

4.9.3 Overload Control Threshold

To open Overload Control Threshold page:

1. From the navigation menu under **BSF**, navigate to **Overload Control Configurations**, and select **Overload Control Threshold**.

Overload Control Threshold page is displayed. The page shows the existing configurations.

2. BSF allows you to configure the threshold values using a profile. You can either use a default or custom profile or create a new profile. You must activate one of the profiles to use the values. At a time, you can activate only one profile.

> **Note**
>
> If there are no profiles activated, Policy calculates the load level based on `overloadLevelThreshold` configured in `custom-values.yaml` file.

If you are upgrading from an older version of BSF to 23.1.0 or later, the following message appears at the top of the page:

```
System looks to be using old configuration (Not profile based). Request you to
please migrate the data or activate one of the profile
```

a. Click **Migrate**.
Migrate Data window opens.

b. Enter the name of the profile.

c. Either click **Migrate** to migrate the data from the previous version of BSF or click **Migrate and Activate** to migrate the data and activate the profile.

> **Note**
>
> Migrate button will only migrate the existing threshold data to profile. It does not activate the profile. Until one of the profile is not active , the UI will continue to show the above message to migrate the data.
>
> In case of fault recovery, the active profile details are recovered and used from the database. No need to migrate again.

Table 4-68 Create and Manage Threshold Profiles

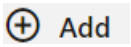
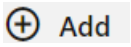
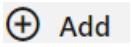
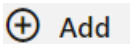
Button/icon	Action
	Opens the **Create Profile** window and allows you to create a new profile. By default, the values of the default profile are associated with the new profile. Click  next to each of the services to edit the values.
	Deletes the selected threshold profile. **Note**: You cannot delete the default system provided profile.
	Opens the **Copy Profile** window to copy an existing profile. While using the copy profile option, whichever profile is selected in the **Threshold Profile** dropdown, the values are copied from that profile.
Threshold Profile	Lists all the threshold profiles. You can select any of the profiles from the list to activate. If the selected profile is already active, you can see **(ACTIVE)** button in green color next to the profile name.
Activate	Activates the profile selected from **Threshold Profile** list. At a time, you can have only one active profile.
Go To Active	**Go To Active** button selects the current active profile from the **Threshold Profile** drop down list. **Note**: If none of the profiles are active, the **Go To Active** button does not appear.

Table 4-69 Configure Threshold Values

Configuration	Description
Service Name	You can configure the threshold values for BSF Management Services:

Table 4-69 (Cont.) Configure Threshold Values

Configuration	Description
CPU	Click  to view the abatement and onset values for each of the three levels (L1, L2, and L3). The onset and abatement values for CPU are calucalted in percentage (%) and the range is from 1 to 100. Click  to edit the abatement and onset values for each of the levels. **Note** Make sure that the onset value of L1 is less than the abatement value of L2 and the onset value of L2 is less than the abatement value of L3. You can click  to delete the CPU values for a service. The application prompts you to confirm before deleting the values.
Pending Message Count	Click  to add the pending message count for each of the services. Pending message count accepts an integer value between 1 to 1000000.
Failure Count	Click  to add the failure count for each of the services. The failure count accepts an integer value between 1 to 1000000.
Memory	Click  to add the abatement and onset memory values for each of the three levels (L1, L2, and L3). Memory details are calculated in Percentage (%) and ranges between 1 to 100.

4.10 NF Scoring Configurations

You can configure the NF Scoring feature using the CNC Console. To navigate to NF Scoring, click NF Scoring, under BSF. It shows Settings and Calculated Score, which are described as follows:

Table 4-70 NF Scoring

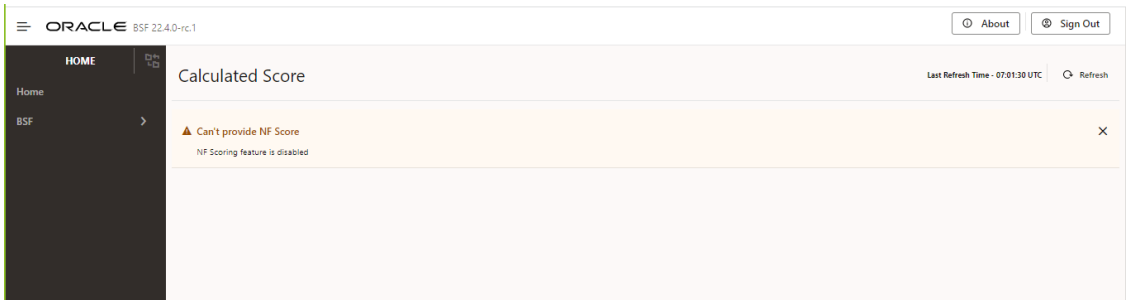
Field Name	Description
Enable NF Scoring	Specifies whether to enable or disable the NF Scoring
TPS	Traffic
Enable	Enables the TPS.
Max Score	Specifies the maximum score of the TPS.
Max TPS	Specifies the maximum TPS.
Service Health	Specifies the service health of a site.
Enable	Enables the Service Health.
Max Score	Specifies the maximum score of the Service Health.
Signaling Connections	Specifies the Signaling Connections of a site.
Enable	Enables the Signaling Connections.
Max Score	Specifies the maximum score of the Signaling Connections.
Max Connections	Specifies the maximum connections.
Replication Health	Specifies the Replication Health of a site.
Enable	Enables the Replication Health.
Max Score	Specifies the maximum score of the Replication Health.
Locality/Site Preference	Specifies the Locality or Site Preference.
Enable	Enables the Locality or Site Preference.
Score	Specifies the score of the Locality or Site Preference.
Active Alert	Specifies the Active Alerts of a site.
Enable	Enables the Active Alert.
Critical Alert Weightage	The site with more critical alerts is unhealthy.
Major Alert Weightage	The site with more major alerts is unhealthy.
Minor Alert Weightage	The site with more minor alerts is unhealthy.

Calculated Score:

To check the calculated Score of a site:

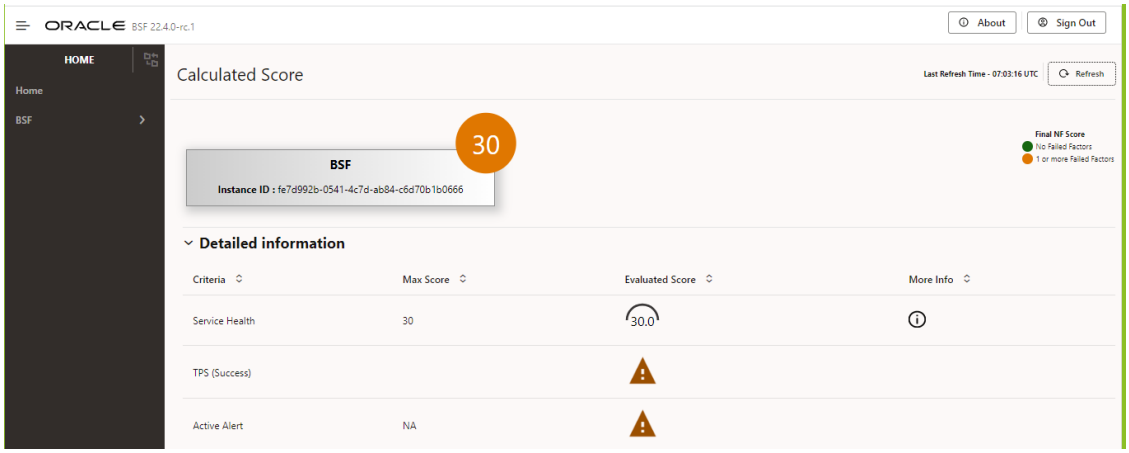
From the navigation menu, under BSF, click NF Scoring and then select Calculated Score. This opens the page displaying the Calculated Score.

Figure 4-21 NF Scoring Disabled



If the NF Scoring feature is enabled. The calculated Screen page displays as:

Figure 4-22 NF Scoring Enabled



> **Note**
>
> If app-info pod is down, you will not be getting the NF Score. You will get an error message that "Data can't be fetched due to internal server error".

Calculated Score shows the total score along with the Instance ID. The total score is shown in either Green or Orange color. If the NF Score is shown in green color there are no failed factors. And, if the NF Score is shown in Orange color there are one or more failed factors. You can click on **Detailed information** to view different criteria and their Max Score, Evaluated Score, and More Info. The criteria in the detailed information tab show the evaluated score. The failed factors are shown with a warning symbol under the evaluated score.

On the top-right of the screen, the *Last Refresh Time* information is available. Moreover, a *Refresh* button is given to refresh the NF Score of a site.

4.11 Viewing cnDBTier functionalities in CNC Console

Perform the following procedure to view the cnDBTier version, status of cnDBTier clusters, and georeplication status on the CNC Console.

> **Note**
>
> The following cnDBTier functionalities are read only and is available only through CNC Console.

4.11.1 Backup List

Perform the following procedure to view the list of completed backups:

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.
2. Click the **Backup List** to view the list of completed backups along with Backup ID, Backup size, and Creation Timestamp.

The **Backup List** screen is displayed.

Table 4-71 Backup List

Fields	Description
Backup Details	This field displays information such as backup Id, backup size, and backup creation timestamp.
Site Name	This field displays the name of the current site to which BSF is connected.
Backup Id	This field displays the ID of the stored backup.
Backup Size (bytes)	This field displays the size of the stored backup.
Creation TimeStamp	This field displays the time recorded when the backup was stored.

4.11.2 Database Statistics Report

Perform the following procedure to view the available database:

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.
2. Click the **Database Statistics Report** to view the available database.

Table 4-72 Database Statistics Report

Fields	Description
Database Count	This field displays the number of available database.
Database Tables Count	This field displays the available database names and their table count.
Database Name	This field displays the database name.
Table Count	This field displays the table count for each database.
Database Table Rows Count	This field displays the table rows present in each table.

a. Click the **View** icon available next to the database name to view the **View Database Table Rows Count** screen.

Table 4-73 View Database Table Rows Count

Fields	Description
Database Name	This field displays the database name.
Tables	This field displays the table names and the corresponding rows in each table.
Table Name	This field displays the table name.
Row Count	This field displays the table rows present in each table.

4.11.3 Georeplication Status

Perform the following procedure to view the local site and remote site name to which BSF is connected.

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.

2. Click the **Georeplication Status** to view the local site and remote site name to which BSF is connected.

Table 4-74 GeoReplication Status

Fields	Description
Local Site Name	This field displays the local site name to which BSF is connected.
Remote Site Name	This field displays the remote site name.
Replication Status	This field displays the replication status with corresponding sites.
Seconds Behind Remote Site	This field displays the number of seconds that the last record read by the local site is behind the latest record written by the remote site for all the replication groups.

a. Click the **View** icon in the **Actions** menu to view the **View Georeplication Status** screen.

Table 4-75 Georeplication Status

Fields	Description
Replication Group Delay	This field displays the number of seconds that the last record read by the local site is behind the latest record written by the remote site for individual replication groups.
Replication Channel Group Id	This field displays the ID of the replication channel group.

b. Click the **View** icon to view the **Replication Group Delay** attributes.

Table 4-76 View Replication Group Delay

Fields	Description
Channel Details	This field displays the channel details such as Remote Replication IP and Role.
Remote Replication IP	This field displays the IP of the remote replication channel.
Role	This field displays the role of the replication channel IP.

4.11.4 Heartbeat Status

Perform the following procedure to view the connectivity between local site and remote site name to which BSF is connected.

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.
2. Click the **HeartBeat Status** to view the connectivity between local site and remote site to which BSF is connected.

Table 4-77 HeartBeat Status Details

Fields	Description
Site Name	This field displays the name of the current site to which BSF is connected.

Table 4-77 (Cont.) HeartBeat Status Details

Fields	Description
HeartBeat Details	This field displays information such as the remote site name, heartbeat status, heartbeat lag, and replication channel group id.
Remote Site Name	This field displays the remote site name.
Heartbeat Status	This field displays the connectivity status with corresponding sites.
Heartbeat Lag	This field displays the lag or latency in seconds it took to syncronize between sites.
Replication Channel Group Id	This field displays the ID of the replication channel group.

4.11.5 Georeplication Recovery

Perform the following procedure to mark cnDBTier cluster as failed, execute georeplication recovery, and monitor their status:

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.
2. Click **Georeplication Recovery** to access the Georeplication Recovery Status of the cnDBTier cluster. This includes options such as Update Cluster As Failed, Start Georeplication Recovery, and Georeplication Recovery Status.
   - Click the **Update Cluster As Failed** to mark the cluster as FAILED.
     The **Update Cluster As Failed** page is displayed.

Table 4-78 Update Cluster As Failed

Fields	Description
Cluster Names	This attribute lists the names of cnDBTier clusters. It allows you to select a cluster from the available list to mark as failed.
Failed Cluster Names	This attribute displays the list of names of cnDBTier clusters that are marked as failed.
Update Cluster	Click the **Update Cluster** to mark the cluster as FAILED.
Cancel	Click the **Cancel** to cancel the process.

   - Click the **Start Georeplication Recovery** to start the georeplication recovery process for a failed site.
     The **Start Georeplication Recovery** page is displayed.

Table 4-79 Start Georeplication Recovery

Attribute	Description
Failed Cluster Name	This attribute displays a list of cnDBTier clusters that have been marked as failed.
Backup Cluster Name (Optional)	This attribute displays the list of active cnDBTier clusters designated for georeplication recovery.
Start Georeplication Recovery	Click the **Start Georeplication Recovery** to start the georeplication recovery process for a failed site.
Cancel	Click the **Cancel** to cancel the process.

- Click the **Georeplication Recovery Status** to view the status of georeplication recovery for cnDBTier clusters.
  The **Georeplication Recovery Status** page is displayed.

Table 4-80 Georeplication Recovery Status

Attribute	Description
Local Cluster Name	This attribute displays the name of the local cluster.
Georeplication Recover Status Details	This attribute displays the details of the georeplication recovery status for cnDBTier clusters.
Cluster Name	This attribute displays the names of all the clusters.
Georeplication Recovery Status	This attribute displays the current status of georeplication recovery for a cluster.
Refresh	Click **Refresh** to view the most current data.

The following are the states of Georeplication Recovery:

Table 4-81 Georeplication Recovery States

Georeplication Recovery State	Description
ACTIVE	The cluster is in a healthy state, and replication is up and running with its respective mate cluster.
REINSTALLED	The cluster enters this state during fatal error recovery when the end user reinstalls the cluster.
STARTDRRESTORE	When Georeplication recovery is started, the cluster will transition into this state.
INITIATEBACKUP	Once Georeplication recovery is started, the cluster will identify a healthy cluster for backup initiation and transition into this state.
CHECKBACKUP	Once the backup is initiated, the georeplication recovery cluster will monitor the progress of the backup until its completion. If the backup fails, the cluster will restart the backup.
COPY_BACKUP	Upon completion of the backup, the georeplication recovery cluster will request the transfer of the backup from the healthy cluster to the georeplication recovery cluster.
CHECK_BACKUP_COPY	Once backup copy is started georeplication recovery cluster will monitor for the backup transfer progress till it's completion and if it's fails the cluster will re-initiates the backup transfer.
BACKUPCOPIED	Once the backup copy is started, the georeplication recovery cluster will monitor the progress of the backup transfer until its completion. If the transfer fails, the cluster will restart the backup transfer.
BACKUPEXTRACTED	This state indicates that the backup has been successfully extracted at the georeplication recovery cluster, allowing the restoration of the backup to start.
FAILED	This state is used by end user to mark specific cluster as failed and hence georeplication recovery is essential to recover the cluster.This state can also indicates that georeplication recovery started and the database is restored using the healthy cluster backup.

Table 4-81 (Cont.) Georeplication Recovery States

Georeplication Recovery State	Description
UNKNOWN	This state is used by the end user to mark a specific cluster as failed, necessitating georeplication recovery for cluster recovery. Additionally, this state can indicate that georeplication recovery has started and the database has been restored using the backup from the healthy cluster.
RECONNECTSQLNODES	This state is used to instruct SQL nodes to be offline during backup restoration to prevent any records from entering the binlog of the georeplication recovery cluster.
BACKUPRESTORE	This state indicates that the backup, successfully copied from the healthy cluster, is currently being used to restore the georeplication recovery cluster.
RESTORED	Once the backup is successfully restored in the georeplication recovery cluster, the cluster will enter this state to start the reestablishment of replication channels.
BINLOGINITIALIZED	This state indicates the start of binlogs for the restoration of replication channels, necessary to start the restore process
RECONFIGURE	Once the binlog is restarted, the georeplication recovery cluster will reestablish the replication channels with respect to all its mate clusters.

4.11.6 Local Cluster Status

Perform the following procedure to view the local cluster status for the current site.

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.
2. Click the **Local Cluster Status** to view the local cluster status for the current site:

Table 4-82 Local Cluster Status

Fields	Description
Site Name	This field displays the name of the current site to which BSF is connected.
Cluster Status	This field displays the local cluster status for the current site.

4.11.7 On Demand Backup

Perform the following procedure to backup the database on demand.

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.
2. Click the **On Demand Backup** to create a new backup and view the status of initiated on-demand backups.

> **Note**
>
> On Demand Backup can be initiated on both single site and multi-site cnDBTier cluster and can be used to restore the first standalone site. DB Backup will not be initiated if sites are not properly configured.

Table 4-83 On Demand Backup Details

Fields	Description
Site Name	This field displays the name of the current site to which BSF is connected.
DR Status	This field displays the status of DR.
Backup Id	This field displays the ID of the stored backup.
Backup Status	This field displays the status of backup.
Remote Transfer Status	The field displays the status of remote transfer.
Initiate Backup	The field displays whether the backup is initiated or not.

a. Click the **Edit** icon.
The **Edit** On Demand Backup screen appears.

> **Note**
>
> The **Edit** mode is available only for Initiate Backup.

b. To enable the Initiate Backup option, click **Save**.
A confirmation message "Save successfully" appears.

c. Click **Cancel** to navigate back to the On Demand Backup screen.

d. Click **Refresh** to reload the On Demand Backup screen.

4.11.8 Version

Perform the following procedure to view the cnDBTier version:

1. From the left navigation pane, click the **BSF** tab, and then click the **DB Tier** tab.
2. Click the **cnDBTier Version** to view the version.

Table 4-84 cnDBTier Version Attributes

Fields	Description
cnDBTier Version	This field displays the cnDBTier version.
NDB Version	This field displays the network database (NDB) version.

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.

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

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

Table 5-1 Alerts Levels or Severity Types

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

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

   0utput: 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.

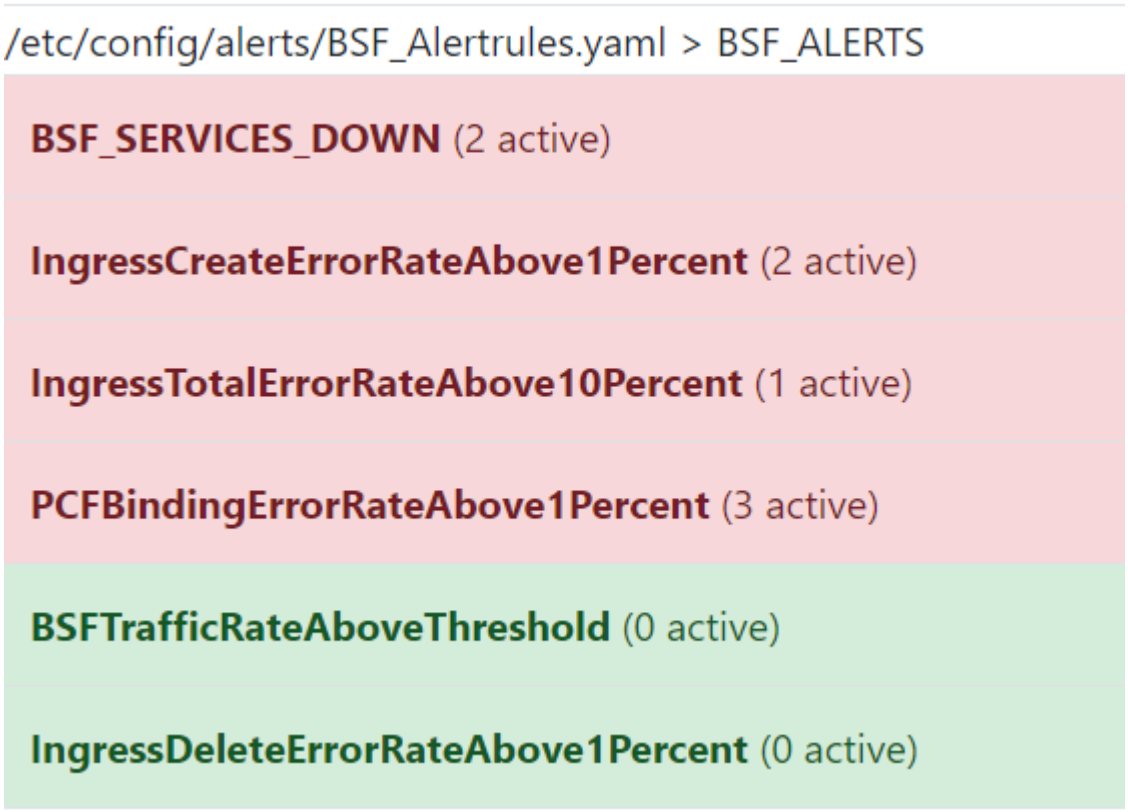
5. Add **BSF_Alertrules.yaml** file into Prometheus server configmap by running the following command :

   ```
   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:



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/occne/cluster/<cluster-name>/artifacts/alerts` directory on the OCCNE Bastion Host.

   ```
   $ pwd /var/occne/cluster/stark/artifacts/alerts
   $ ls
   occne_alerts.yaml
   $ vi BSF_Alertrules.yaml
   $ ls BSF_Alertrules.yaml occne_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 occne-prometheus-alerts configmap, run the following command:

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

4. 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>
   ```

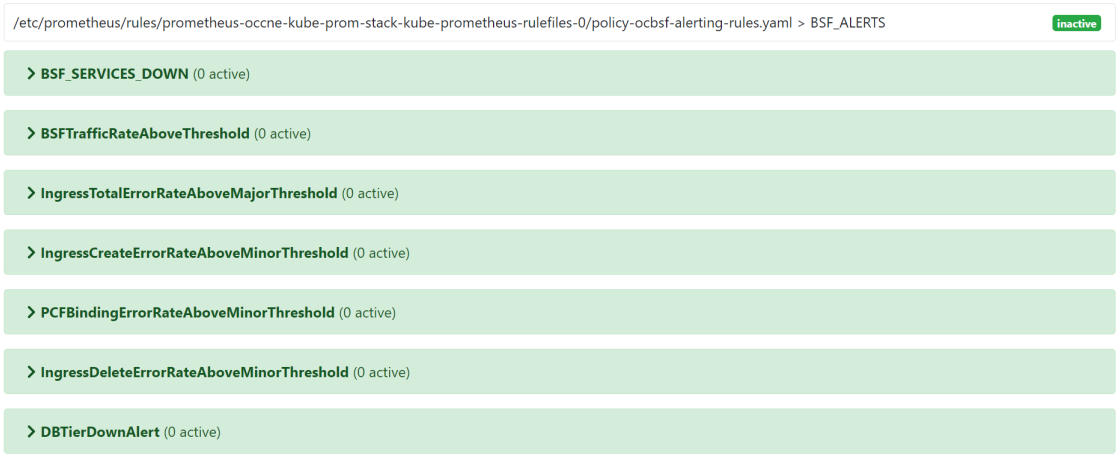
   To verify if the CRD is created, run the following command:

   ```
   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 5-2 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) (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
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

Table 5-3 AAA_RX_FAIL_COUNT_EXCEEDS_MAJOR_THRESHOLD

Field	Details
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

Table 5-4 AAA_RX_FAIL_COUNT_EXCEEDS_MINOR_THRESHOLD

Field	Details
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", appId="16777236", responseCode!~"2.*"}[5m]) / rate(ocbsf_diam_response_network_total{msgType="AAA", appId="16777236"}[5m])) * 100 <=80 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 > 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

Table 5-5 SCP_PEER_UNAVAILABLE

Field	Details
Description	Configured SCP peer is unavailable.
Summary	Configured SCP peer is unavailable.
Severity	Major
Condition	ocbsf_oc_egressgateway_peer_health_status != 0. SCP peer [{{$labels.peer}}] is unavailable.
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

Table 5-6 SCP_PEER_SET_UNAVAILABLE

Field	Details
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

Table 5-7 STALE_CONFIGURATION

Field	Details
Description	In last 10 minutes, the current service config_level does not match the config_level from the config-server.
Summary	In last 10 minutes, the current service config_level does not match the config_level from the config-server.
Severity	Major
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

Table 5-7 (Cont.) STALE_CONFIGURATION

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

5.2.7 BSF_SERVICES_DOWN

Table 5-8 BSF_SERVICES_DOWN

Field	Details
Description	{{$labels.microservice}} service is not running!
Summary	{{$labels.microservice}} 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 BSFTrafficRateAboveMinorThreshold

Table 5-9 BSFTrafficRateAboveMinorThreshold

Field	Details
Description	BSF service Ingress traffic Rate is above threshold of Max MPS(1000) (current value is: {{ $value }})
Summary	Traffic Rate is above 70 Percent of Max requests per second(1000)
Severity	Minor
Condition	The total Binding Management service Ingress traffic rate has crossed the configured threshold of 700 TPS. The default value of this alert trigger point in the `BSF_Alertrules.yaml` file is when the Binding management service Ingress Rate crosses 70% 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.

5.2.9 BSFTrafficRateAboveMajorThreshold

Table 5-10 BSFTrafficRateAboveMajorThreshold

Field	Details
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.

Table 5-10 (Cont.) BSFTrafficRateAboveMajorThreshold

Field	Details
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

Table 5-11 BSFTrafficRateAboveCriticalThreshold

Field	Details
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

Table 5-11 (Cont.) BSFTrafficRateAboveCriticalThreshold

Field	Details
Recommended Actions	The alert gets cleared when the Ingress traffic rate falls below the threshold. **Note**: Threshold levels can be configured using the `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

Table 5-12 BINDING_QUERY_RESPONSE_ERROR_MINOR

Field	Details
Description	At least 30% of the Binding Query connection requests failed with error 'DIAMETER_UNABLE_TO_DELIVER'.
Summary	At least 30% of the Binding Query connection requests failed with error 'DIAMETER_UNABLE_TO_DELIVER'.
Severity	Minor
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. (sum(rate(ocbsf_bindingQuery_response_total {response_code!~"2.*"} [10m]) or (appinfo_service_running * 0)) / sum(rate(ocbsf_bindingQuery_response_total[10m])) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_bindingQuery_response_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.12 BINDING_QUERY_RESPONSE_ERROR_MAJOR

Table 5-13 BINDING_QUERY_RESPONSE_ERROR_MAJOR

Field	Details
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
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. (sum(rate(ocbsf_bindingQuery_response_total {response_code!~"2.*"} [10m]) or (appinfo_service_running * 0)) / sum(rate(ocbsf_bindingQuery_response_total[10m])) * 100 >= 50
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_bindingQuery_response_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.13 BINDING_QUERY_RESPONSE_ERROR_CRITICAL

Table 5-14 BINDING_QUERY_RESPONSE_ERROR_CRITICAL

Field	Details
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
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. (sum(rate(ocbsf_bindingQuery_response_total {response_code!~"2.*"} [10m]) or (appinfo_service_running * 0)) / sum(rate(ocbsf_bindingQuery_response_total[10m])) * 100 >= 70
Metric Used	ocbsf_bindingQuery_response_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.14 DIAM_RESPONSE_NETWORK_ERROR_MINOR

Table 5-15 DIAM_RESPONSE_NETWORK_ERROR_MINOR

Field	Details
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
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.
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_diam_response_network_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.15 DIAM_RESPONSE_NETWORK_ERROR_MAJOR

Table 5-16 DIAM_RESPONSE_NETWORK_ERROR_MAJOR

Field	Details
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
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.
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_diam_response_network_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.16 DIAM_RESPONSE_NETWORK_ERROR_CRITICAL

Table 5-17 DIAM_RESPONSE_NETWORK_ERROR_CRITICAL

Field	Details
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
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.
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_diam_response_network_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.17 DUPLICATE_BINDING_REQUEST_ERROR_MINOR

Table 5-18 DUPLICATE_BINDING_REQUEST_ERROR_MINOR

Field	Details
Description	At least 30% of the Binding Registration requests failed were duplicate failures.
Summary	At least 30% of the Binding Registration requests failed were duplicate failures.
Severity	Minor
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. (sum(rate({_name_=~"ocbsf_collision_detection.*"} [10m]) or (appinfo_service_running * 0)) / sum(rate(ocbsf_ingress_request_total {operation_type="register"} [10m]))) * 100 >= 30
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_ingress_request_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.18 DUPLICATE_BINDING_REQUEST_ERROR_MAJOR

Table 5-19 DUPLICATE_BINDING_REQUEST_ERROR_MAJOR

Field	Details
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
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. (sum(rate({_name_=~"ocbsf_collision_detection.*"} [10m]) or (appinfo_service_running * 0)) / sum(rate(ocbsf_ingress_request_total {operation_type="register"} [10m]))) * 100 >= 50
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_ingress_request_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.19 DUPLICATE_BINDING_REQUEST_ERROR_CRITICAL

Table 5-20 DUPLICATE_BINDING_REQUEST_ERROR_CRITICAL

Field	Details
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
Condition	If 70% of the requests fails for 10 mins, BSF is ablel to raise Critical Alert indicating duplicate Binding request are being detected at BSF. (sum(rate({_name_=~"ocbsf_collision_detection.*"} [10m]) or (appinfo_service_running * 0)) / sum(rate(ocbsf_ingress_request_total {operation_type="register"} [10m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.37.1.2.24
Metric Used	ocbsf_ingress_request_total
Recommended Actions	For any assistance, contact My Oracle Support.

5.2.20 IngressTotalErrorRateAboveMinorThreshold

Table 5-21 IngressTotalErrorRateAboveMinorThreshold

Field	Details
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	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

Table 5-22 IngressTotalErrorRateAboveMajorThreshold

Field	Details
Description	Transaction Error Rate detected above 5 Percent of Total on BSF service (current value is: {{ $value }})
Summary	Transaction Error Rate detected above 5 Percent of Total Transactions
Severity	Major
Condition	The total number of failed transactions for BSF service is above 5 percent of the total transactions.
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 5% of the total transactions. For any assistance, contact My Oracle Support.

5.2.22 IngressTotalErrorRateAboveCriticalThreshold

Table 5-23 IngressTotalErrorRateAboveCriticalThreshold

Field	Details
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

Table 5-23 (Cont.) IngressTotalErrorRateAboveCriticalThreshold

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

Table 5-24 PCFBindingErrorRateAboveMinorThreshold

Field	Details
Description	PCF Binding Error Rate above 1 Percent in {{$labels.microservice}} in {{$labels.namespace}}
Summary	PCF Binding Error Rate in {{$labels.kubernetes_node}} (current value is: {{ $value }})
Severity	Minor
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

Table 5-25 PCFBindingErrorRateAboveMajorThreshold

Field	Details
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

Table 5-25 (Cont.) PCFBindingErrorRateAboveMajorThreshold

Field	Details
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

Table 5-26 PCFBindingErrorRateAboveCriticalThreshold

Field	Details
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

Table 5-27 IngressCreateErrorRateAboveMinorThreshold

Field	Details
Description	BSF Ingress Create Error Rate above 1 Percent in {{$labels.microservice}} in {{$labels.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

Table 5-27 (Cont.) IngressCreateErrorRateAboveMinorThreshold

Field	Details
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

Table 5-28 IngressCreateErrorRateAboveCriticalThreshold

Field	Details
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

Table 5-29 IngressCreateErrorRateAboveMajorThreshold

Field	Details
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

Table 5-29 (Cont.) IngressCreateErrorRateAboveMajorThreshold

Field	Details
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

Table 5-30 IngressDeleteErrorRateAboveMinorThreshold

Field	Details
Description	Ingress Delete Error Rate above 1 Percent in {{$labels.microservice}} in {{$labels.namespace}}
Summary	Ingress Delete Error Rate in {{$labels.kubernetes_node}} (current value is: {{ $value }})
Severity	Minor
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

Table 5-31 IngressDeleteErrorRateAboveMajorThreshold

Field	Details
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

Table 5-31 (Cont.) IngressDeleteErrorRateAboveMajorThreshold

Field	Details
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

Table 5-32 IngressDeleteErrorRateAboveCriticalThreshold

Field	Details
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

Table 5-33 DBTierDownAlert

Field	Details
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

Table 5-33 (Cont.) DBTierDownAlert

Field	Details
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

Table 5-34 CPUUsagePerServiceAboveMinorThreshold

Field	Details
Description	CPU usage for {{$labels.microservice}} service is above 60
Summary	CPU usage for {{$labels.microservice}} 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

Table 5-35 CPUUsagePerServiceAboveMajorThreshold

Field	Details
Description	CPU usage for {{$labels.microservice}} service is above 80
Summary	CPU usage for {{$labels.microservice}} service is above 80
Severity	Major

Table 5-35 (Cont.) CPUUsagePerServiceAboveMajorThreshold

Field	Details
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

Table 5-36 CPUUsagePerServiceAboveCriticalThreshold

Field	Details
Description	CPU usage for {{$labels.microservice}} service is above 90
Summary	CPU usage for {{$labels.microservice}} 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

Table 5-37 MemoryUsagePerServiceAboveMinorThreshold

Field	Details
Description	Memory usage for {{$labels.microservice}} service is above 60
Summary	Memory usage for {{$labels.microservice}} service is above 60
Severity	Minor
Condition	A service pod has reached the configured minor threshold (60%) of its memory usage limits.

Table 5-37 (Cont.) MemoryUsagePerServiceAboveMinorThreshold

Field	Details
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

Table 5-38 MemoryUsagePerServiceAboveMajorThreshold

Field	Details
Description	Memory usage for {{$labels.microservice}} service is above 80
Summary	Memory usage for {{$labels.microservice}} 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

Table 5-39 MemoryUsagePerServiceAboveCriticalThreshold

Field	Details
Description	Memory usage for {{$labels.microservice}} service is above 90
Summary	Memory usage for {{$labels.microservice}} service is above 90
Severity	Critical

Table 5-39 (Cont.) MemoryUsagePerServiceAboveCriticalThreshold

Field	Details
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` For any assistance, contact My Oracle Support.

5.2.39 NRF_COMMUNICATION_FAILURE

Table 5-40 NRF_COMMUNICATION_FAILURE

Field	Details
Description	There has been a external failure communication error with NRF.
Summary	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

Table 5-41 NRF_SERVICE_REQUEST_FAILURE

Field	Details
Description	There has been a Service Request Failure with NRF, either due to Registration failure or Profile update failure.
Summary	There has been a Service Request Failure with NRF, either a Registration failure, Heartbeat failure, or Profile Update Failure.
Severity	Info

Table 5-41 (Cont.) NRF_SERVICE_REQUEST_FAILURE

Field	Details
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

Table 5-42 PERF_INFO_ACTIVE_OVERLOAD_THRESHOLD_FETCH_FAILED

Field	Details
Description	The application fails to get the current active overload level threshold data.
Summary	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

Table 5-43 PodDoc

Field	Details
Description	Pod Congestion status of {{$labels.microservice}} service is DoC
Summary	Pod Congestion status of {{$labels.microservice}} service is DoC
Severity	Major
Condition	The pod congestion status is set to Danger of Congestion.

Table 5-43 (Cont.) PodDoc

Field	Details
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

Table 5-44 PodCongested

Field	Details
Description	Pod Congestion status of {{$labels.microservice}} service is congested
Summary	Pod Congestion status of {{$labels.microservice}} 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

Table 5-45 PodPendingRequestDoC

Field	Details
Description	Pod Resource Congestion status of {{$labels.microservice}} service is DoC for PendingRequest type
Summary	Pod Resource Congestion status of {{$labels.microservice}} 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"}

Table 5-45 (Cont.) PodPendingRequestDoC

Field	Details
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

Table 5-46 PodPendingRequestCongested

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

Table 5-47 PodCPUDoC

Field	Details
Description	Pod Resource Congestion status of {{$labels.microservice}} service is DoC for CPU type
Summary	Pod Resource Congestion status of {{$labels.microservice}} 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"}

Table 5-47 (Cont.) PodCPUDoC

Field	Details
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

Table 5-48 PodCPUCongested

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

Table 5-49 PodMemoryDoC

Field	Details
Description	Pod Resource Congestion status of {{$labels.microservice}} service is DoC for Memory type
Summary	Pod Resource Congestion status of {{$labels.microservice}} 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"}

Table 5-49 (Cont.) PodMemoryDoC

Field	Details
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

Table 5-50 PodMemoryCongested

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

Table 5-51 ServiceOverloaded-Minor

Field	Details
Description	Overload Level of {{$labels.microservice}} service is L1
Summary	Overload Level of {{$labels.microservice}} 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.

Table 5-52 ServiceOverloaded-Major

Field	Details
Description	Overload Level of {{$labels.microservice}} service is L2
Summary	Overload Level of {{$labels.microservice}} 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.

Table 5-53 ServiceOverloaded-Critical

Field	Details
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

Table 5-54 ServiceResourceOverloaded

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

Table 5-54 (Cont.) ServiceResourceOverloaded

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

Table 5-55 ServiceResourceOverloaded

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

Table 5-56 ServiceResourceOverloaded

Field	Details
Description	{{$labels.microservice}} service is L3 for {{$labels.type}} type
Summary	{{$labels.microservice}} service is L3 for {{$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

Table 5-57 ServiceResourceOverloaded

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

Table 5-57 (Cont.) ServiceResourceOverloaded

Field	Details
Summary	{{$labels.microservice}} service is L1 for {{$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.

Table 5-58 ServiceResourceOverloaded

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

Table 5-59 ServiceResourceOverloaded

Field	Details
Description	{{$labels.microservice}} service is L3 for {{$labels.type}} type
Summary	{{$labels.microservice}} service is L3 for {{$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

Table 5-60 ServiceResourceOverloaded

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

Table 5-61 ServiceResourceOverloaded

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

Table 5-62 ServiceResourceOverloaded

Field	Details
Description	{{$labels.microservice}} service is L3 for {{$labels.type}} type
Summary	{{$labels.microservice}} service is L3 for {{$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

Table 5-62 (Cont.) ServiceResourceOverloaded

Field	Details
Metric Used	service_resource_overload_level{type="svc_pending_count"}
Recommended Actions	The alert gets cleared when the number of pending messages of the service is back to normal state. For any additional guidance, contact My Oracle Support.

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

Table 5-63 ServiceResourceOverloaded

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

Table 5-64 ServiceResourceOverloaded

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

Table 5-65 ServiceResourceOverloaded

Field	Details
Description	{{$labels.microservice}} service is L3 for {{$labels.type}} type
Summary	{{$labels.microservice}} service is L3 for {{$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

Table 5-66 SYSTEM_IMPAIRMENT_MAJOR

Field	Details
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

Table 5-67 SYSTEM_IMPAIRMENT_CRITICAL

Field	Details
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_PARTIAL_SHUTDOWN

Table 5-68 SYSTEM_OPERATIONAL_STATE_PARTIAL_SHUTDOWN

Field	Details
Description	System Operational State is now in partial shutdown state.
Summary	System Operational State is now in partial shutdown state.
Severity	Major
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.

5.2.55 SYSTEM_OPERATIONAL_STATE_COMPLETE_SHUTDOWN

Table 5-69 SYSTEM_OPERATIONAL_COMPLETE_SHUTDOWN

Field	Details
Description	System Operational State is now in complete shutdown state
Summary	System Operational State is now in complete shutdown state
Severity	Critical
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.

5.2.56 DIAM_CONN_PEER_DOWN

Table 5-70 DIAM_CONN_PEER_DOWN

Field	Details
Description	Diameter connection to peer {{ $labels.peerHost }} is down.
Summary	Diameter connection to peer down.
Severity	Major
Condition	Diameter connection to peer peerHost 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.

5.2.57 DIAM_CONN_NETWORK_DOWN

Table 5-71 DIAM_CONN_NETWORK_DOWN

Field	Details
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.

5.2.58 DIAM_RESPONSE_REALM_VALIDATION_ERROR_CRITICAL

Table 5-72 DIAM_RESPONSE_REALM_VALIDATION_ERROR_CRITICAL

Field	Details
Description	At least 75% of the Diam Response failed with error 'DIAMETER_REALM_NOT_SERVED', either of BSF realm or PCF Realm doesn't match with received destination realm in diameter message.
Summary	{{ $value }}% of the Diam Response failed with error 'DIAMETER_REALM_NOT_SERVED'.
Severity	CRITICAL
Condition	(sum(increase(ocbsf_diam_realm_validation_failed_total{responseCode="3003", appId="16777236"}[10m])) / sum(increase(ocbsf_diam_response_network_total{appId="16777236"}[10m]))) * 100 >= 75
OID	1.3.6.1.4.1.323.5.3.37.1.2.41
Metric Used	ocbsf_diam_realm_validation_failed_total
Recommended Actions	1. Check if the value of the following keys under Advanced settings of diameter settings page are set to true: • DIAMETER.Enable.Validate.Realm • DIAMETER.BSF.Enable.Validate.Binding.Realm 2. Check the destination-realm in diameter request.

5.2.59 DIAM_RESPONSE_REALM_VALIDATION_ERROR_MAJOR

Table 5-73 DIAM_RESPONSE_REALM_VALIDATION_ERROR_MAJOR

Field	Details
Description	At least 50% of the Diam Response failed with error 'DIAMETER_REALM_NOT_SERVED', either of BSF realm or PCF Realm doesn't match with received destination realm in diameter message.
Summary	{{ $value }}% of the Diam Response failed with error 'DIAMETER_REALM_NOT_SERVED'.
Severity	MAJOR
Condition	(sum(increase(ocbsf_diam_realm_validation_failed_total{responseCode="3003", appId="16777236"}[10m])) / sum(increase(ocbsf_diam_response_network_total{appId="16777236"}[10m]))) * 100 >= 50
OID	1.3.6.1.4.1.323.5.3.37.1.2.41
Metric Used	ocbsf_diam_realm_validation_failed_total
Recommended Actions	1. Check if the value of the following keys under Advanced settings of diameter settings page are set to true: • DIAMETER.Enable.Validate.Realm • DIAMETER.BSF.Enable.Validate.Binding.Realm 2. Check the destination-realm coming in diameter request.

5.2.60 DIAM_RESPONSE_REALM_VALIDATION_ERROR_MINOR

Table 5-74 DIAM_RESPONSE_REALM_VALIDATION_ERROR_MINOR

Field	Details
Description	At least 20% of the Diam Response failed with error 'DIAMETER_REALM_NOT_SERVED', either of BSF realm or PCF Realm doesn't match with received destination realm in diameter message.
Summary	{{ $value }}% of the Diam Response failed with error 'DIAMETER_REALM_NOT_SERVED'.
Severity	MINOR
Condition	(sum(increase(ocbsf_diam_realm_validation_failed_total{responseCode="3003", appId="16777236"}[10m])) / sum(increase(ocbsf_diam_response_network_total{appId="16777236"}[10m]))) * 100 >= 20
OID	1.3.6.1.4.1.323.5.3.37.1.2.41
Metric Used	ocbsf_diam_realm_validation_failed_total

Table 5-74 (Cont.) DIAM_RESPONSE_REALM_VALIDATION_ERROR_MINOR

Field	Details
Recommended Actions	1. Check if the value of the following keys under Advanced settings of diameter settings page are set to true: • DIAMETER.Enable.Validate.Realm • DIAMETER.BSF.Enable.Validate.Binding.Realm 2. Check the destination-realm coming in diameter request.

5.2.61 AUDIT_STALE_NOTIFY_ERROR_RESPONSE_MINOR

Table 5-75 AUDIT_STALE_NOTIFY_ERROR_RESPONSE_MINOR

Field	Details
Description	At least 20% of the BSF Notification Request for Audit have responded with a 5xx or 4xx (not 404) Status in the last 24 hours.
Summary	At least 20% of the BSF Notification Request for Audit have responded with a 5xx or 4xx (not 404) Status in the last 24 hours.
Severity	MINOR
Condition	When 20%, or more, BSF Notification Requests for Audit to PCF (or its respective NF) fail, the alert is triggered. The threshold default value is defined at `BSF_Alertrules.yaml`.
Expression	(sum(increase(ocbsf_query_response_count_total{response_code=~"5..|4..",response_code!="404"}[24h])) / sum(increase(ocbsf_query_response_count_total[24h]))) * 100 >= 20
OID	1.3.6.1.4.1.323.5.3.37.1.2.42
Metric Used	ocbsf_query_response_count_total
Recommended Actions	Determine the reason why these notification requests are failing. This alert indicates that there is a potential issue either with the network communications, or the NF where the audit notifications point to.

5.2.62 AUDIT_STALE_NOTIFY_ERROR_RESPONSE_MAJOR

Table 5-76 AUDIT_STALE_NOTIFY_ERROR_RESPONSE_MAJOR

Field	Details
Description	At least 40% of the BSF Notification Request for Audit have responded with a 5xx or 4xx (not 404) Status in the last 24 hours.
Summary	At least 40% of the BSF Notification Request for Audit have responded with a 5xx or 4xx (not 404) Status in the last 24 hours.
Severity	MAJOR
Condition	When 40%, or more, BSF Notification Requests for Audit to PCF (or its respective NF) fail, the alert is triggered. The threshold default value is defined at `BSF_Alertrules.yaml`.
Expression	(sum(increase(ocbsf_query_response_count_total{response_code=~"5..|4..",response_code!="404"}[24h])) / sum(increase(ocbsf_query_response_count_total[24h]))) * 100 >= 40
OID	1.3.6.1.4.1.323.5.3.37.1.2.42
Metric Used	ocbsf_query_response_count_total
Recommended Actions	Determine the reason why these notification requests are failing. This alert indicates that there is an issue either with the network communications, or the NF where the audit notifications point to, that needs to be addressed as soon as possible.

5.2.63 AUDIT_STALE_NOTIFY_ERROR_RESPONSE_CRITICAL

Table 5-77 AUDIT_STALE_NOTIFY_ERROR_RESPONSE_CRITICAL

Field	Details
Description	At least 60% of the BSF Notification Request for Audit have responded with a 5xx or 4xx (not 404) Status in the last 24 hours.
Summary	At least 60% of the BSF Notification Request for Audit have responded with a 5xx or 4xx (not 404) Status in the last 24 hours.
Severity	CRITICAL
Condition	When 60%, or more, BSF Notification Requests for Audit to PCF (or its respective NF) fail, the alert is triggered. The threshold default value is defined at `BSF_Alertrules.yaml`.

Table 5-77 (Cont.) AUDIT_STALE_NOTIFY_ERROR_RESPONSE_CRITICAL

Field	Details
Expression	(sum(increase(ocbsf_query_response_count_total{response_code=~"5..|4..",response_code!="404"}[24h])) / sum(increase(ocbsf_query_response_count_total[24h]))) * 100 >= 60
OID	1.3.6.1.4.1.323.5.3.37.1.2.42
Metric Used	ocbsf_query_response_count_total
Recommended Actions	Determine the reason why these notification requests are failing. This alert indicates that there is a critical issue either with the network communications, or the NF where the audit notifications point to, that needs to be addressed immediately.

5.2.64 CERTIFICATE_EXPIRY

Table 5-78 CERTIFICATE_EXPIRY

Field	Details
Description	TLS certificate to expire in 6 months.
Summary	security_cert_x509_expiration_seconds - time() <= 15724800
Severity	Minor
Condition	This alert is raised when the TLS certificate is about to expire in six months.
OID	1.3.6.1.4.1.323.5.3.37.1.2.44
Metric Used	security_cert_x509_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

Table 5-79 CERTIFICATE_EXPIRY

Field	Details
Description	TLS certificate to expire in 3 months.
Summary	security_cert_x509_expiration_seconds - time() <= 7862400
Severity	Major
Condition	This alert is raised when the TLS certificate is about to expire in three months.
OID	1.3.6.1.4.1.323.5.3.37.1.2.44
Metric Used	security_cert_x509_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

Table 5-80 CERTIFICATE_EXPIRY

Field	Details
Description	TLS certificate to expire in 1 month.
Summary	security_cert_x509_expiration_seconds - time() <= 2592000
Severity	Critical
Condition	This alert is raised when the TLS certificate is about to expire in one month.
OID	1.3.6.1.4.1.323.5.3.37.1.2.44
Metric Used	security_cert_x509_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.2.65 BSF_CONNECTION_FAILURE

Table 5-81 BSF_CONNECTION_FAILURE

Field	Details
Description	Connection failure on Egress and Ingress Gateways for incoming and outgoing connections.
Summary	sum(increase(ocbsf_oc_ingressgateway_connection_failure_total[5m]) >0 or (ocbsf_oc_ingressgateway_connection_failure_total unless ocbsf_oc_ingressgateway_connection_failure_total offset 5m)) by (namespace,app, error_reason) > 0 or sum(increase(ocbsf_oc_egressgateway_connection_failure_total[5m]) >0 or (ocbsf_oc_egressgateway_connection_failure_total unless ocbsf_oc_egressgateway_connection_failure_total offset 5m)) by (namespace,app, error_reason) > 0
Severity	Major
Condition	This alert is raised when the TLS certificate is about to expire in three months.
OID	1.3.6.1.4.1.323.5.3.37.1.2.43
Metric Used	ocbsf_oc_ingressgateway_connection_failure_total
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.2.66 INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Table 5-82 INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Field	Details
Description	This alarm is raised when OCNADD is not reachable.

Table 5-82 (Cont.) INGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

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

5.2.67 EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

Table 5-83 EGRESS_GATEWAY_DD_UNREACHABLE_MAJOR

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

5.2.68 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

Table 5-84 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

Field	Details
Description	Certificate expiry in less than 6 months.
Summary	Certificate expiry in less than 6 months.
Severity	Minor
Condition	dgw_tls_cert_expiration_seconds - time() <= 15724800
OID	1.3.6.1.4.1.323.5.3.37.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds

Table 5-84 (Cont.) DIAM_GATEWAY_CERTIFICATE_EXPIRY_MINOR

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

5.2.69 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR

Table 5-85 DIAM_GATEWAY_CERTIFICATE_EXPIRY_MAJOR

Field	Details
Description	Certificate expiry in less than 3 months.
Summary	Certificate expiry in less than 3 months.
Severity	Major
Condition	dgw_tls_cert_expiration_seconds - time() <= 7862400
OID	1.3.6.1.4.1.323.5.3.37.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.2.70 DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

Table 5-86 DIAM_GATEWAY_CERTIFICATE_EXPIRY_CRITICAL

Field	Details
Description	Certificate expiry in less than 1 month.
Summary	Certificate expiry in less than 1 month.
Severity	Critical
Condition	dgw_tls_cert_expiration_seconds - time() <= 2592000
OID	1.3.6.1.4.1.323.5.3.37.1.2.75
Metric Used	dgw_tls_cert_expiration_seconds
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.2.71 DGW_TLS_CONNECTION_FAILURE

Table 5-87 DGW_TLS_CONNECTION_FAILURE

Field	Details
Description	Alert for TLS connection establishment.
Summary	TLS Connection failure when Diam gateway is an initiator.
Severity	Major

Table 5-87 (Cont.) DGW_TLS_CONNECTION_FAILURE

Field	Details
Condition	sum by (namespace,reason) (ocbsf_diam_failed_conn_network) > 0
OID	1.3.6.1.4.1.323.5.3.37.1.2.81
Metric Used	ocbsf_diam_failed_conn_network
Recommended Actions	For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.2.72 BINDING_REVALIDATION_PCF_BINDING_MISSING_MINOR

Table 5-88 BINDING_REVALIDATION_PCF_BINDING_MISSING_MINOR

Field	Details
Description	At least 30% but less than 50% of the PCF BINDING missing among all binding revalidation records in the last 5 minutes.
Summary	At least 30% but less than 50% of the PCF BINDING missing among all Binding Revalidation records in the last 5 minutes.
Severity	Minor
Condition	(sum by (namespace) (rate(ocbsf_binding_revalidation_pcfBinding_missing_total[5m])) / sum by (namespace) (rate(ocbsf_binding_revalidation_response_total[5m]))) * 100 >= 30 < 50
OID	1.3.6.1.4.1.323.5.3.37.1.2.51
Metric Used	
Recommended Actions	Check BSF Management service health history. Increase binding audit frequency. For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.2.73 BINDING_REVALIDATION_PCF_BINDING_MISSING_MAJOR

Table 5-89 BINDING_REVALIDATION_PCF_BINDING_MISSING_MAJOR

Field	Details
Description	At least 50% but less than 70% of the PCF BINDING missing among all binding revalidation records in the last 5 minutes.
Summary	At least 50% but less than 70% of the PCF BINDING missing among all binding revalidation records in the last 5 minutes.
Severity	Major

Table 5-89 (Cont.) BINDING_REVALIDATION_PCF_BINDING_MISSING_MAJOR

Field	Details
Condition	(sum by (namespace) (rate(ocbsf_binding_revalidation_pcfBinding_missing_total[5m])) / sum by (namespace) (rate(ocbsf_binding_revalidation_response_total[5m]))) * 100 >= 50 < 70
OID	1.3.6.1.4.1.323.5.3.37.1.2.51
Metric Used	
Recommended Actions	Check BSF Management service health history. Increase binding audit frequency. For any additional guidance, contact My Oracle Support (https://support.oracle.com).

5.2.74 BINDING_REVALIDATION_PCF_BINDING_MISSING_CRITICAL

Table 5-90 BINDING_REVALIDATION_PCF_BINDING_MISSING_CRITICAL

Field	Details
Description	At least 70% of the PCF BINDING missing among all binding revalidation records in the last 5 minutes.
Summary	At least 70% of the PCF BINDING missing among all binding revalidation records in the last 5 minutes.
Severity	Critical
Condition	(sum by (namespace) (rate(ocbsf_binding_revalidation_pcfBinding_missing_total[5m])) / sum by (namespace) (rate(ocbsf_binding_revalidation_response_total[5m]))) * 100 >= 70
OID	1.3.6.1.4.1.323.5.3.37.1.2.51
Metric Used	
Recommended Actions	Check BSF Management service health history. Increase binding audit frequency. For any additional guidance, contact My Oracle Support (https://support.oracle.com).

6
BSF KPIs

This section provides information about Key Performance Indicators (KPIs) used for Oracle Communications Cloud Native Core Binding Support Function (BSF).

> **Note**
>
> Sample BSF dashboard for Grafana is delivered to the customer through CNC BSF Custom Templates. The metrics and functions used to achieve KPIs are covered in CNC BSF Custom Templates as well.

KPIs

The following table lists the KPIs used for various operations related to BSF:

Table 6-1 BSF KPIs

KPI Details	Metric used for KPI	Service Operation	Response Code
The **BSF Management Service Pod Count** KPI measures the number of BSF pods that are available in the system.	count(container_memory_usage_bytes{container='bsf-management-service',namespace=\"$namespace\"})	Not Applicable	Not Applicable
The **Ingress-Gateway Pod Count** KPI measures the number of Ingress Gateway pods that are available in the system.	count(container_memory_usage_bytes{container='ocbsf-ingress-gateway',namespace=\"$namespace\"})	Not Applicable	Not Applicable
The **Egress-Gateway Pod Count** KPI measures the number of Egress Gateway pods that are available in the system.	count(container_memory_usage_bytes{container='ocbsf-egress-gateway',namespace=\"$namespace\"})	Not Applicable	Not Applicable
The **Total-TPS** KPI measures the rate of Ingress Gateway requests at BSF.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"ocbsf-ocbsf-ingress-gateway\"}[5m]))	All	Not Applicable
This **Memory-Usage** KPI measures the current memory usage in bytes.	sum(container_memory_usage_bytes{image!='',namespace=\"$namespace\"})	Not Applicable	Not Applicable
This **Memory-Usage** KPI measures the memory usage (in bytes) for the top 16 memory users by each container.	topk(16,sum(container_memory_usage_bytes{image!='',namespace=\"$namespace\"}) by (container_name))	Not Applicable	Not Applicable
This **CPU-Usage** KPI measures the number of cores that are being used by each container.	sum(rate(container_cpu_usage_seconds_total{image!='',namespace=\"$namespace\",container_name!='POD'}[2m])) by (container_name)	Not Applicable	Not Applicable

Table 6-1 (Cont.) BSF KPIs

KPI Details	Metric used for KPI	Service Operation	Response Code
This **Binding-Registration** KPI measures the rate of successful binding registration requests at BSF.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"bsf-management-service\",method=\"POST\",status=\"201\"}[2m]))	NF Register	201
This **Binding-Registration** KPI measures the rate of unsuccessful binding registration requests at BSF.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"bsf-management-service\",method=\"POST\",status=\"400\"}[2m]))	NF Register	400
This **Binding-Deregistration** KPI measures the rate of successful deregistration requests at BSF.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"bsf-management-service\",method=\"DELETE\",status=\"204\"}[2m]))	NF Deregister	204
This **Binding-Deregistration** KPI measures the rate of unsuccessful deregistration requests at BSF.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"bsf-management-service\",method=\"DELETE\",status=\"404\"}[2m]))	NF Deregister	404
This **Binding-Discovery** KPI measures the rate of successful discovery requests at BSF.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"bsf-management-service\",method=\"GET\",status=\"200\"}[2m]))	NF Discovery	200
This **Binding-Discovery** KPI measures the rate of discovery requests that have been rejected by BSF due to errors that may have occurred at NF consumer.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"bsf-management-service\",method=\"GET\",status=\"404\"}[2m]))	NF Discovery	404
This **Binding-Discovery** KPI measures the rate of discovery requests that have been stated invalid by BSF due to errors that may have occurred at NF consumer.	sum (rate(http_server_requests_seconds_count{kubernetes_namespace=\"$namespace\",microservice=\"bsf-management-service\",method=\"GET\",status=\"400\"}[2m]))	NF Discovery	400
This **Diameter_ingress-request-response** KPI measures the rate of AAR request messages sent to network NFs like AF or PCF (in case of BSF).	sum (rate(ocbsf_diam_request_network_total{kubernetes_namespace=\"$namespace\",msgType=\"AAR\"}[2m]))	All	Not Applicable
This **Diameter_ingress-request-response** KPI measures the rate of AAA messages going out to network where response code in AAA is 2001, that is, Diameter_Success.	sum (rate(ocbsf_diam_request_network_total{kubernetes_namespace=\"$namespace\",msgType=\"AAA\",responseCode=\"2001\"}[2m]))	All	201

Table 6-1 (Cont.) BSF KPIs

KPI Details	Metric used for KPI	Service Operation	Response Code
This **Diameter_ingress-request-response** KPI measures the rate of STR request messages sent to network NFs.	sum (rate(ocbsf_diam_request_network_total{ kubernetes_namespace=\"$namespace\", msgType=\"STR\"}[2m]))	All	Not Applicable
This **Diameter_ingress-request-response** KPI measures the rate of STA messages going out to network where response code in STA is 2001, that is, Diameter_Success.	sum (rate(ocbsf_diam_request_network_total{ kubernetes_namespace=\"$namespace\", msgType=\"STA\",responseCode=\"2001\" }[2m]))	All	201
This **Egress-Request-Response** KPI measures the rate of Delete requests sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_requests_total{kubernetes_namespace=\"$namespace\",Method='DELETE'}[2m]))	Delete	Not Applicable
This **Egress-Request-Response** KPI measures the rate of responses, to Delete requests (initiated at BSF), by external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_responses_total{kubernetes_namespace=\"$namespace\",Method='DELETE'}[2m]))	Delete	Not Applicable
This **Egress-Request-Response** KPI measures the rate of GET requests sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_requests_total{kubernetes_namespace=\"$namespace\",Method='GET'}[2m]))	GET	Not Applicable
This **Egress-Request-Response** KPI measures the rate of responses, to GET requests (initiated at BSF), by external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_responses_total{kubernetes_namespace=\"$namespace\",Method='GET'}[2m]))	GET	Not Applicable
This **Egress-Request-Response** KPI measures the rate of POST requests sent to external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_requests_total{kubernetes_namespace=\"$namespace\",Method='POST'}[2m]))	POST	Not Applicable
This **Egress-Request-Response** KPI measures the rate of responses, to POST requests (initiated at BSF), by external NFs through Egress Gateway.	sum(rate(oc_egressgateway_http_responses_total{kubernetes_namespace=\"$namespace\",Method='POST'}[2m]))	POST	Not Applicable
This **Diameter-egress-Request-Response** KPI measures the rate of Update Notify requests sent to external NFs through Egress Gateway.	sum (rate(ocpm_egress_request_total{kubernetes_namespace=\"$namespace\",operation_type=\"update_notify\",servicename_3gpp=\"rx\"}[2m]))	Update Notify	Not Applicable

Table 6-1 (Cont.) BSF KPIs

KPI Details	Metric used for KPI	Service Operation	Response Code
This **Diameter-egress-Request-Response** KPI measures the rate of Update Notify requests sent to external NFs through Egress Gateway.	sum (rate(ocpm_egress_response_total{kubernetes_namespace=\"$namespace\",operation_type=\"update_notify\",servicename_3gpp=\"rx\",response_code=\"2xxx\"}[2m])) **Note** Different microservices may have different nomenclature. For example, operation_type or operationType.	Update Notify	2xxx
This **Diameter Connections** KPI measures the total number of connections with network peer.	sum (rate(occnp_diam_conn_network{kubernetes_namespace=\"$namespace\"}[2m]))	Not Applicable	Not Applicable
This **Diameter Connections** KPI measures the number of connections with network peer for a given application ID.	sum (rate(occnp_diam_conn_app_network{kubernetes_namespace=\"$namespace\"}[2m]))	Not Applicable	Not Applicable

7
Binding Support Function Metrics

BSF Metrics

This chapter includes information about Metrics for Oracle Communications Cloud Native Core, Binding Support Function (BSF).

BSF uses the observability tool Grafana to analyze and visualize data. The Grafana Dashboard consists of panels displaying the data as graphs, charts or other visualizations. A dashboard in Grafana is represented by a JSON object, which stores the metadata of its dashboard. Following Grafana dashboards are created for BSF Observability and debugging purposes:

- **Observability Dashboard**:
  - This dashboard metadata is stored in the `BSF_Observability_Dashboard.json` file.
  - This dashboard has the panels that monitors the overall health status of the setup & contains details like resource utilization, kmps, latency, etc.
  - Customers can use this Dashboard on a regular basis for observing the status of the setup and also for assessing the setup performance with a run.
  - Depending upon the applicability of a panel or row, the customers have the flexibility to either remove, update or add content to the Dashboard.
- **Debug Dashboard**:
  - This dashboard metadata is stored in the `BSF_Debug_Dashboard.json` file.
  - This dashboard has the panels that monitor the operational status of the setup and is used for debugging & troubleshooting purposes.
  - Customers can use this Dashboard when any issue occur in the NF and also when reporting a probable issue to Oracle Customer Support from the setup.
  - Depending upon the applicability of a panel or row, the customers have the flexibility to either remove, update or add content to the Dashboard.

The name of the metrics may contain suffix such as total, seconds, max and so on. It gets added by the Micrometer registry if it is not present in the metrics name. The metric name has the following format for suffix:

The metric name is equal to <Basename of the metric>_<Suffix>

Table 7-1 Metrics type and Suffix

Metric Type	Suffix
Counter	_total
Gauge	N/A
TimerGauge	_seconds
MultiGauge	N/A

Table 7-1 (Cont.) Metrics type and Suffix

Metric Type	Suffix
Timer	_seconds_max or _seconds **Note**: There are two types of suffix used for timer metrics. For example, my_timer_seconds_max gauge and my_timer_seconds summary. In summary type, there will be further addition of suffix such as _count or _sum.
DistributionSummary	N/A or _max **Note**: There are two types of suffix used for DistributionSummary. For example, my_distribution_ratio histogram and my_distribution_ratio_max gauge. In the histogram type there will be further addition of suffix such as bucket, _count, or sum.
LongTaskTimer	_seconds_max or _seconds **Note:** There are two types of suffix used for LongTaskTimer. For example, long_task_timer_seconds_max gauge and long_task_timer_seconds summary. In summary type there will be further addition of suffix such as _active_count or _duration_sum.

Table 7-2 Dimension Description

Dimension	Description
operation_type	Type of operation Values: • create • get • put • update • terminate • update_notify • terminate_notify • subscribe • unsubscribe • transfer • resubscribe
dnn	Data Network Name or Access Point Name
snssai	Single Network Slice Selection Assistance Information
response_code	Response code **HTTP interfaces:** • 1xx • 2xx • 3xx • 4xx • 5xx **Diameter interfaces:** • 2xxx • 3xxx • 4xxx • 5xxx

Table 7-2 (Cont.) Dimension Description

Dimension	Description
latency	The total time in between request and response. If latency between request and response is 203, then bucket number is 4. Max bucket set to 10 (0-9), Range 50ms.
nf_instance_Id	Unique id of the nf Instance. • ingress: source nfInstanceId • egress: destination nfInstanceId **HTTP interfaces:** **Diameter interfaces:** • ingress: Origin-Host AVP • egress: Destination-Host AVP
nf_name	This represents the FQDN corresponding to the NF InstanceID present in the nf_instance_id dimension. **HTTP interface:** egress: NF FQDN
sbi_priority	Service Based Interface
service_version	Service version Value: [UDR = "v1,v2", CHF = "v1"]
service	The complete name of current service. Value: string
namespace	The namespace of current service. Value: string
category	The category of current service. Value: • database • common • infra • pcf • bsf
destHost	Value of destination Host received or sent in the corresponding request message
destRealm	Value of destination Realm received or sent in the corresponding request message
origHost	Value of origination Host received or sent in the corresponding request message
origRealm	Value of origination Realm received or sent in the corresponding request message
reqDestHost	Value of destination Host in corresponding request message of response message.
reqDestRealm	Value of destination Realm in corresponding request message of response message.
reqOrigHost	Value of origination Host in corresponding request message of response message.
reqOrigRealm	Value of origination Realm in corresponding request message of response message.
direction	Indicates direction of message flow. • "In" means coming towards POD/micro-service • "Out" means going out from POD/micro-service
appId	Application ID exchanged in CEX messages or used in the respective message of an application.

Table 7-2 (Cont.) Dimension Description

Dimension	Description
applicationName	Human readable name of corresponding application ID 16777236 => Rx 16777238 => Gx 16777302 => Sy 16777217 => Sh **Note**: Sh interface is not supported for Converged Policy mode of deployment. 0xffffffff => Relay
cmdCode	Command code value in the received or sent, request or answer message
msgType	Type of the message, for example CCRT-T, CCR-I etc.
responseCode	result code in diameter message
spendingLimitDataSource	Specifies the source from which PCF fetches policy counters. Value: OCS
retry	Identify message is a retry message. Value: • true • false
retryAnswer	Reason for the retry message. Value: • error code • timeout
level	Indicates the current load level or the level of pod congestion. Value: • 0 = Normal • 1 = DOC • 2 = Congested
type	Resource type Value: • PendingRequest • CPU • Memory
le	le is abrreviated as "Less than equal to".Value of a defined bucket for a Histogram.
sessRuleReports	Indicates that session rule report is received at PCF.
policyDecFailureReports	Indicates that Policy decision failure report is received at PCF.
isLeaderPod	Indicates if the pod calculating the threshold level is a leader pod.
prevLevel	Indicates the previous load level prior to current load level calculation.
levelChangeType	Indicates the level change type. The value of this dimension can be: • None: when load level is same • Increment: when level changes to higher level
servicenameNon3gpp	-
serviceResource	-
params	Lists the API parameters.
outcome	Shows the outcome of an operation such as SUCCESS, FAILURE, TIMEOUT.
cause	Contains the error cause.
peerHost	Indicates the value of peer host received or sent in corresponding connection request message.

Table 7-2 (Cont.) Dimension Description

Dimension	Description
perRealm	Indicates the value of peer realm received or sent in corresponding connection request message.

7.1 Egress Gateway Metrics for SCP

This section provides details about SCP health monitoring metrics and the respective dimensions.

Table 7-3 ocbsf_oc_egressgateway_peer_health_status

Field	Details
Description	It defines Egress Gateway peer health status. • This metric is set to 1, if a peer is unhealthy. • This metric is reset to 0, when it becomes healthy again. • This metric is set to -1, if peer is removed from peerconfiguration.
Type	Gauge
Dimensions	• peer • vfqdn
Examples	• ocbsf_oc_egressgateway_peer_health_status{"peer":"10.75.213.172:8080"} 1.0 • ocbsf_oc_egressgateway_peer_health_status{"peer":"10.75.213.172:8080"} 0.0 • ocbsf_oc_egressgateway_peer_health_status{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 1.0 • ocbsf_oc_egressgateway_peer_health_status{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 0.0

Table 7-4 ocbsf_oc_egressgateway_peer_health_ping_request_total

Field	Details
Description	This metric is incremented every time a health ping is sent toward a peer.
Type	Counter
Dimensions	• peer • vfqdn
Examples	• ocbsf_oc_egressgateway_peer_health_ping_request_total{"peer":"10.75.213.172:8080"} 389.0 • ocbsf_oc_egressgateway_peer_health_ping_request_total{"peer":"10.75.213.172:8080"} 439.0 • ocbsf_oc_egressgateway_peer_health_ping_request_total{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 389.0 • ocbsf_oc_egressgateway_peer_health_ping_request_total{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080"} 439.0

Table 7-5 ocbsf_oc_egressgateway_peer_health_ping_response_total

Field	Details
Description	This metric is incremented every time a health ping response is received from a peer irrespective of success or failure.
Type	Counter
Dimensions	• peer • vfqdn • statusCode • cause
Examples	• ocbsf_oc_egressgateway_peer_health_ping_response_total{"peer":"10.75.213.172:8080","status":"httpstatus","cause":""} 89.0 • ocbsf_oc_egressgateway_peer_health_ping_response_total{"peer":"10.75.213.172:8080","status":"Exception","cause":"exception cause"} 39.0 • ocbsf_oc_egressgateway_peer_health_ping_response_total{"vfqdn":"http://abc.com","status":"httpstatus","cause":""} 89.0 • ocbsf_oc_egressgateway_peer_health_ping_response_total{"vfqdn":"http://abc.com","status":"Exception","cause":"exception cause"} 39.0

Table 7-6 ocbsf_oc_egressgateway_peer_health_status_transitions_total

Field	Details
Description	This metric is incremented every time a peer is transitioned from Availble to Unavailable or from Unavailable to Available.
Type	Counter
Dimensions	• peer • vfqdn • from • to
Examples	• ocbsf_oc_egressgateway_peer_health_status_transitions_total{"identifier":"10.75.213.172:8080","from":"available","to":"unavailable"} 14.0 • ocbsf_oc_egressgateway_peer_health_status_transitions_total{"identifier":"10.75.213.172:8080","from":"unavailable","to":"available"} 34.0 • ocbsf_oc_egressgateway_peer_health_status_transitions_total{"vfqdn":"http://abc.com",*"peer":"10.75.213.172:8080"*,"from":"unavailable","to":"available"} 34.0 • ocbsf_oc_egressgateway_peer_health_status_transitions_total{"vfqdn":"http://abc.com","peer":"10.75.213.172:8080","from":"available","to":"unavailable"} 14.0

Table 7-7 ocbsf_oc_egressgateway_peer_count

Field	Details
Description	This metric is incremented every time for the peer count.
Type	Gauge
Dimensions	• peerset
Example	ocbsf_oc_egressgateway_peer_count{"peerset":"set-0"} 3.0

Table 7-8 ocbsf_oc_egressgateway_peer_available_count

Field	Details
Description	This metric is incremented every time for the available peer count.
Type	Gauge
Dimensions	• peerset
Example	ocbsf_oc_egressgateway_peer_available_count{"peerset":"set-0"} 4.0

7.2 Correlation-Info Header Metrics

For every correlation-info header received or newly generated, a metric will be pegged. Following are the list of metrics:

Below mention table list the metrics that shall be implemented as part of this feature with the following Dimensions:

1. operation_type= {"create","update","delete","subscribe","unsubscribe","terminate","register","deregister"....}
2. correlation_info_type={"imsi", "msisdn", "imsi,msisdn"}

Table 7-9 ocbsf_correlation_info_header_received

Field	Details
Description	BSF reports total outgoing request that are carried by the correlation-info header.
Type	Counter
Dimensions	• operation_type • correlation_info_type
Example	ocbsf_correlation_info_header_received_total '{correlation_info_type="imsi", operation_type="create"}',2

Table 7-10 ocbsf_correlation_info_header_forwarded

Field	Details
Description	BSF reports total incoming request that are carried by the correlation-info header.
Type	Counter
Dimensions	• operation_type • correlation_info_type
Example	ocbsf_correlation_info_header_received_total '{correlation_info_type="imsi", operation_type="update"}',1

Table 7-11 ocbsf_correlation_info_header_generated

Field	Details
Description	BSF reports the total responses carried by the correlation-info header.
Type	Counter
Dimensions	• operation_type • correlation_info_type

Table 7-11 (Cont.) ocbsf_correlation_info_header_generated

Field	Details
Examples	• ocbsf_correlation_info_header_forwarded_total '{correlation_info_type="imsi", operation_type="subscribe"}',2 • ocbsf_correlation_info_header_generated_total '{correlation_info_type="imsi", operation_type="create"}',2

7.3 Configuration Server Metrics

Table 7-12 topic_version

Field	Details
Description	Configuration service will have this metrics a database value from each topic version. The Services fetching the configurations from Configuration Server, will have its current topic version till which configurations has been fetched successfully.
Type	Gauge
Dimensions	• Service Name • Pod Name
Examples	• topic_version{topicName="common.congestionthreshold.diam-gateway",} 1.0 • topic_version{topicName="common.auditservice.cfg",} 1.0 • topic_version{topicName="bsf.sbi.errorcodes",} 36.0 • topic_version{topicName="common.diamsetting",} 2.0 • topic_version{topicName="common.public.diammessagepriority",} 2.0 • topic_version{topicName="bsf.managementservice",} 1.0 • topic_version{topicName="subscriber.activity.logging.idlist.bsf",} 1.0 • topic_version{topicName="public.policy.error.handler.config",} 1.0 • topic_version{topicName="common.public.diampeernode",} 5.0 • topic_version{topicName="nrfclient.cfg",} 1.0 • topic_version{topicName="common.public.diamloadshedding",} 2.0 • topic_version{topicName="diameter.errorcodes",} 7.0 • topic_version{topicName="common.public.diamroutingtable",} 1.0 • topic_version{topicName="subscriber.activity.logging.mapping.bsf",} 1.0 • topic_version{topicName="bsf.global.cfg",} 1.0 • topic_version{topicName="common.public.diamcontrolledshutdown",} 1.0 • topic_version{topicName="config.level",} 53.0 • topic_version{topicName="diameter.customerrorcodes",} 1.0

7.4 Active Sessions Count Metrics

Table 7-13 oc_db_active_session_count

Field	Details
Description	Active sessions count
Type	Gauge
Dimensions	• Service • Table

Table 7-14 inbound_requests_total

Field	Details
Description	Inbound requests total (number of requests received via CM/REST to get instantaneous Active Session Count)
Type	Counter
Dimensions	• requestType (onDemandActiveSessionCount, register, deregister) • tableName

7.5 AppInfo Metrics

Table 7-15 appinfo_service_running

Field	Details
Description	Provides the status of monitored services.
Type	Gauge
Dimensions	• service • namespace • category
Example	appinfo_service_running{service="xxx",namespace="xxx",category="xxx"} 1

Table 7-16 appinfo_category_running

Field	Details
Description	Provides the status of monitored categories.
Type	Gauge
Dimensions	• namespace • category
Example	• appinfo_category_running{category="xxx",namespace="xxx"} 1 • appinfo_category_good{category="xxx",namespace="xxx"} 1

Table 7-17 appinfo_category_good

Field	Details
Description	Provides the readiness of monitored categories.
Type	Gauge
Dimensions	• namespace • category

Table 7-18 nfscore

Field	Details
Description	• *factor* – Contains one of the values: all, successTPS, serviceHealth, signallingConnections, replicationHealth, localityPreference. – When the factor is set to *all* that means NF score is calculated for all the factors. • *status* – *success*: when the factor is enabled and its value is fetched successfully. – *failed*: when the factor is enabled and fetching the value fails. – *notCalculated*: when the factor is disabled.
Type	Gauge
Dimensions	• nfInstanceID • factor • Status
Example	• nfscore{app="testing-appinfo", app_kubernetes_io_instance="testing", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="appinfo", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.7.1.0.0", application="ocbsf", calculatedStatus="success", container="appinfo", endpoint="cnc-metrics", engVersion="22.4.0-rc.5", factor="localityPreference", helm_sh_chart="appinfo-22.4.0-rc.5", instance="10.233.117.146:9000", job="occne-infra/occne-nf-cnc-podmonitor", microservice="bsf-app-info", mktgVersion="1.7.1.0.0", namespace="biloxi-ns", nfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0666", pod="testing-appinfo-78dc65865f-hgrhk", pod_template_hash="78dc65865f", vendor="Oracle"} 5

Table 7-19 nfScoringFactorActualValue

Field	Details
Description	factor tag would contain one of the following values: successTPS, serviceHealth, signallingConnections, replicationHealth, localityPreference
Type	Gauge
Dimensions	• nfInstanceID • factor
Example	• nfScoringFactorActualValue{app="testing-appinfo", app_kubernetes_io_instance="testing", app_kubernetes_io_managed_by="Helm", app_kubernetes_io_name="appinfo", app_kubernetes_io_part_of="ocbsf", app_kubernetes_io_version="1.7.1.0.0", application="ocbsf", calculatedStatus="success", container="appinfo", endpoint="cnc-metrics", engVersion="22.4.0-rc.5", factor="localityPreference", helm_sh_chart="appinfo-22.4.0-rc.5", instance="10.233.117.146:9000", job="occne-infra/occne-nf-cnc-podmonitor", microservice="bsf-app-info", mktgVersion="1.7.1.0.0", namespace="biloxi-ns", nfInstanceID="fe7d992b-0541-4c7d-ab84-c6d70b1b0666", pod="testing-appinfo-78dc65865f-hgrhk", pod_template_hash="78dc65865f", vendor="Oracle"} 5

7.6 Audit Service Metrics

The following table describes the Audit Service metrics and respective dimensions:

Table 7-20 audit_recs_stale_total

Field	Details
Description	Number of records detected as stale.
Type	Counter
Dimensions	• ServiceName • TableName
Example	audit_recs_stale_total{ServiceName="bsf-management-service",TableName="pcf_binding",} 1.0

Table 7-21 audit_recs_notif_total

Field	Details
Description	Number of stale record notifications sent, applicable for modes: NOTIFY and DELETE_NOTIFY.
Type	Counter
Dimensions	ServiceName
Example	audit_recs_notif_total{ServiceName="bsf-management-service",} 1.0

Table 7-22 audit_recs_deque_for_notif_total

Field	Details
Description	Number of stale records dequeued to send Notification.
Type	Counter
Dimensions	ServiceName
Example	audit_recs_deque_for_notif_total{ServiceName="bsf-management-service",} 1.0

Table 7-23 audit_recs_enque_for_notif_total

Field	Details
Description	Number of stale records enqueued from Database.
Type	Counter
Dimensions	ServiceName
Example	audit_recs_enque_for_notif_total{ServiceName="bsf-management-service",} 1.0

Table 7-24 oc_db_active_session_count

Field	Details
Description	Reports the session for a given service.
Type	Gauge
Dimensions	• ServiceName • TableName

Table 7-24 (Cont.) oc_db_active_session_count

Field	Details
Example	oc_db_active_session_count{Service="bsf-management-service",Table="pcfbinding",} 1.0

Table 7-25 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimensions	• Service Name • Pod Name

7.7 BSF Management Service

This section describes the metrics used for BSF Management service.

The following table provides information about metrics related to BSF Management service.

Table 7-26 ocbsf_ingress_response_total

Field	Details
Description	This metric is pegged when BSF sends a response message through Ingress Gateway.
Type	Gauge
Dimensions	operation_type dnn snssai application_error_code response_code binding_level binding_id
Example	ocbsf_ingress_response_total{application="bsf-management-service",application_error_code="",binding_id="setxyz.bsfset.5gc.mnc015.mcc360,setxyz.bsfset.5gc.mnc015.mcc350",binding_level="nf-set",dnn="dnn1",operation_type="register",response_code="2xx",snssai="100-D143A5",}

Table 7-27 ocbsf_ingress_request_total

Field	Details
Description	This metric is pegged when BSF receives a request message through Ingress Gateway.

Table 7-27 (Cont.) ocbsf_ingress_request_total

Field	Details
Type	Gauge
Dimensions	operation_type dnn snssai pcf_set_id pcf_id
Example	ocbsf_ingress_request_total{application="bsf-management-service",dnn="dnn1",operation_type="register",pcf_id="somePcfId",pcf_set_id="somePcfSetId",snssai="100-D143A5",} 1.0

Table 7-28 ocbsf_audit_notif_request_count_total

Field	Details
Description	This metric is pegged when BSF receives a notification request from the audit service for stale bindings.
Type	Counter
Dimensions	application
Example	ocbsf_audit_notif_request_count_total{application="bsf-management-service",operation_type="audit_notify",} 1.0

Table 7-29 ocbsf_audit_notif_response_count_total

Field	Details
Description	This metric is pegged when BSF sends a notification response for the request received from the Audit service for stale bindings.
Type	Counter
Dimensions	application
Example	ocbsf_audit_notif_response_count_total{application="bsf-management-service",operation_type="audit_notify",response_code="2xx",} 1.0

Table 7-30 ocbsf_audit_delete_records_count_total

Field	Details
Description	This metric is pegged when BSF successfully deletes stale bindings.
Type	Counter
Dimensions	application
Example	ocbsf_audit_delete_records_count_total{application="bsf-management-service",operation_type="audit_notify",} 1.0

Table 7-31 ocbsf_audit_delete_records_max_ttl_count_total

Field	Details
Description	This metric is pegged when the BSF successfully deletes bindings on receiving maxTTL as 'true'
Type	Counter
Dimensions	application
Example	ocbsf_audit_delete_records_count_total{application="bsf-management-service",operation_type="audit_notify",} 1.0

Table 7-32 ocbsf_diamgw_notification_request_count_total

Field	Details
Description	This metric is pegged when BSF management service receives stale binding notification request from Diameter Gateway.
Type	Counter
Dimensions	application
Example	ocbsf_diamgw_notification_request_count_total{application="bsf-management-service",operation_type="audit_notify",} 1.0

Table 7-33 ocbsf_diamgw_notification_response_count_total

Field	Details
Description	This metric is pegged when BSF management service sends a response for the stale binding notification request from Diameter Gateway.
Type	Counter
Dimensions	application
Example	ocbsf_diamgw_notification_response_count_total{application="bsf-management-service",operation_type="audit_notify",} 1.0

Table 7-34 ocbsf_diamgw_delete_records_count_total

Field	Details
Description	This metric is pegged when BSF management service successfully deletes stale PCF bindings due to Diameter Gateway notification requests.
Type	Counter
Dimensions	application
Example	ocbsf_diamgw_delete_records_count_total{application="bsf-management-service",operation_type="audit_notify",} 1.0

Table 7-35 ocbsf_query_request_count_total

Field	Details
Description	This metric is pegged when BSF management service sends request to PCF to confirm if PcfBinding is stale or not.
Type	Counter

Table 7-35 (Cont.) ocbsf_query_request_count_total

Field	Details
Dimensions	• application • operation_type • response_code
Example	ocbsf_query_request_count_total{application="bsf-management-service",operation_type="query",response_code="2xx",} 1.0

Table 7-36 ocbsf_query_response_count_total

Field	Details
Description	This metric is pegged when BSF management service receives a response for PcfBinding stale confirmation request.
Type	Counter
Dimensions	application
Example	ocbsf_query_response_count_total{application=“bsf-management-service”,operation_type=“query”,response_code=“timeout”,} 1.0

Table 7-37 ocbsf_http_out_conn_request_total

Field	Details
Description	This metric is pegged when BSF sends notification request using HTTP in Diameter Gateway.
Type	Counter
Dimensions	operation_type (delete) serviceResource servicename3gpp (DiameterGateway)

Table 7-38 ocbsf_http_out_conn_response_total

Field	Details
Description	This metric is pegged when BSF receives response for notification request requests using HTTP in Diameter Gateway.
Type	Counter
Dimensions	operation_type (delete) responseCode serviceResource servicename3gpp (DiameterGateway)

Table 7-39 ocbsf_bindingQuery_request_total

Field	Details
Description	This metric is pegged when BSF receives a query request for PCF bindings. PCF Binding query-service sends SUPI, GPSI, IPv4 address, IPv6 address, and mac address to BSF.
Type	Counter
Dimensions	operation_type (query) criteria_type (SUPI/GPSI/UE Address)
Example	ocbsf_bindingQuery_request_total{application="bsf-managementservice",gpsi="false",ipv4Addr="true",ipv6Prefix="false",macAddr48="false",operation_type="query",supi="true",} 1.0

Table 7-40 ocbsf_bindingQuery_response_total

Field	Details
Description	This metric is pegged when BSF sends a response message for a PCF bindings query request. PCF Binding query-service sends SUPI, GPSI, IPv4 address, IPv6 address, and mac address to BSF.
Type	Counter
Dimensions	response_code (2xx, 4xx) operation_type (query) criteria_type (SUPI/GPSI/UE Address)
Example	ocbsf_bindingQuery_response_total{application="bsf-managementservice",application_error_code="",gpsi="false",ipv4Addr="true",ipv6Prefix="false",macAddr48="false",operation_type="query",response_code="2xx",supi="true",} 1.0

Table 7-41 ocbsf_bindingDelete_request_total

Field	Details
Description	This metric is pegged when BSF receives a request to delete PCF bindings. PCF binding sends the binding ids to BSF.
Type	Counter
Dimensions	application operation_type (DELETE)
Example	ocbsf_bindingDelete_request_total{application="bsf-management-service",operation_type="manual_delete",pcf_binding_delete_count="3",}1.0

Table 7-42 ocbsf_bindingDelete_response_total

Field	Details
Description	This metric is pegged when BSF sends a response message to the delete PCF bindings request. PCF binding sends the binding ids to BSF.
Type	Counter

Table 7-42 (Cont.) ocbsf_bindingDelete_response_total

Field	Details
Dimensions	application response_code (2xx,5xx) operation_type (DELETE)
Example	ocbsf_bindingDelete_response_total{application="bsf-management-service",application_error_code="",operation_type="manual_delete",pcf_binding_delete_count="3",response_code="2xx",}1.0

Table 7-43 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimensions	• Service Name • Pod Name
Example	-

Table 7-44 http_server_requests_seconds_count

Field	Details
Description	BSF Management service overall processing time.
Type	Counter
Dimensions	• application • exception • method • outcome • status • uri
Example	http_server_requests_seconds_count{application="bsf-management-service",exception="None",method="GET",outcome="SUCCESS",status="200",uri="/v3/api-docs/swagger-config",} 1.0

Table 7-45 http_server_requests_seconds_sum

Field	Details
Description	BSF Management service overall processing time.
Type	Gauge
Dimensions	• application • exception • method • outcome • status • uri

Table 7-45 (Cont.) http_server_requests_seconds_sum

Field	Details
Example	http_server_requests_seconds_sum{application="bsf-management-service",exception="None",method="GET",outcome="SUCCESS",status="200",uri="/v3/api-docs/swagger-config",} 0.008189215

Table 7-46 error_handler_exec_total

Field	Details
Description	This metric is incremented on error handling performed by framework.
Type	Counter
Dimensions	• application • applicationException • error_type • operation • origin • rule_name • source_interface • target_interface • wrapped_exception
Example	ocbsf_error_handler_exec_total{application="bsf-management-service",application_exception="JavaException",error_type="INTERNAL",operation="CREATE",origin="JAVA",rule_name="REJECT_WITH_ENHANCED_DETAIL",source_interface="POLICY",status="400",target_interface="BSF",wrapped_exception="ServiceException",}

Table 7-47 error_handler_in_total

Field	Details
Description	This metric is incremented on initialization of error handling.
Type	Counter
Dimensions	• application • applicationException • wrapped_exception
Example	ocbsf_error_handler_in_total{application="bsf-management-service",application_exception="JavaException",status="500",wrapped_exception="ServiceException",}

Table 7-48 error_handler_out_total

Field	Details
Description	This metric is incremented on completion of error handling.
Type	Counter
Dimensions	• application • applicationException • error_resolved • wrapped_exception

Table 7-48 (Cont.) error_handler_out_total

Field	Details
Example	ocbsf_error_handler_out_total{application="bsf-management-service",application_exception="JavaException",error_resolved="true",status="400",wrapped_exception="ServiceException",}

Table 7-49 ocbsf_binding_revalidation_request_total

Field	Details
Description	This metric is pegged everytime BSF receives a request for binding revalidation.
Type	Counter
Dimensions	• DNN • snssai • PCF FQDN
Example	-

Table 7-50 ocbsf_binding_revalidation_response_total

Field	Details
Description	This metric is pegged everytime BSF responds to binding revalidation request.
Type	Counter
Dimensions	• DNN • snssai • PCF FQDN • responseCode • action • latency
Example	-

Table 7-51 ocbsf_binding_revalidation_pcfBinding_missing_total

Field	Details
Description	This metric is pegged when PCF Binding is detected as missing in BSF while responding to binding revalidation request.
Type	Counter
Dimensions	• DNN • snssai • PCF FQDN • responseCode • action • latency
Example	-

7.8 Collision Detection Metrics

Table 7-52 ocbsf_collision_detection_bad_request_code

Field	Details
Description	This metric is pegged when a BAD_REQUEST error code is detected.
Metric Type	Counter
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

Table 7-53 ocbsf_collision_detection_not_found_code

Field	Details
Description	This metric is pegged when a NOT_FOUND error code is detected.
Type	Counter
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

Table 7-54 ocbsf_collision_detection_forbidden_code

Field	Details
Description	This metric is pegged when a FORBIDDEN error code is detected.
Type	Counter
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

Table 7-55 ocbsf_collision_detection_unauthorized_code

Field	Details
Description	This metric is pegged when an UNAUTHORIZED error code is detected.
Type	Counter

Table 7-55 (Cont.) ocbsf_collision_detection_unauthorized_code

Field	Details
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

Table 7-56 ocbsf_collision_detection_not_acceptable_code

Field	Details
Description	This metric is pegged when a NON_ACCEPTABLE error code is detected.
Type	Counter
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

Table 7-57 ocbsf_collision_detection_service_unavailable_code

Field	Details
Description	This metric is pegged when an UNAVAILABLE error code is detected.
Type	Counter
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

Table 7-58 ocbsf_collision_detection_method_not_allowed_code

Field	Details
Description	This metric is pegged when a NOT_ALLOWED error code is detected.
Type	Counter
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

Table 7-59 ocbsf_collision_detection_error_code

Field	Details
Description	This metric is pegged when a GENERAL error code is detected.
Type	Counter
Dimensions	• DNN • SNSSAI • APPLICATION_ERROR_CODE • RESPONSE_CODE • BINDING_LEVEL • BINDING_ID

7.9 CM Service Metrics

The following table describes the CM Service metrics and respective dimensions:

Table 7-60 system_operational_state

Field	Details
Description	This metric indicates the current operational state
Type	Gauge
Dimensions	• application • eng_version • namespace • node • pod • vendor
Example	system_operational_state{application="config-server",eng_version="",microservice="",namespace="",node="",pod="occnp-config-mgmt",vendor="oracle",} 1.0

7.10 Diameter Gateway Metrics

Table 7-61 ocbsf_diam_response_local_total

Field	Details
Description	When the diameter request is timed out from the backend peer (diameter connector), this metric is incremented.
Type	Counter
Dimensions	• appId • cmdCode • msgType • reqDestHost • reqDestRealm • reqOrigHost • responseCode • reqOrigRealm

Table 7-61 (Cont.) ocbsf_diam_response_local_total

Field	Details
Example	ocbsf_diam_response_local_total{appId="16777236",cmdCode="265",direction="in",msgType="AAA",reqDestHost="ocbsf",reqDestRealm="xxx.com",reqOrigHost="",reqOrigRealm="",responseCode="timeout",} 1.0

Table 7-62 ocbsf_diam_response_network_total

Field	Details
Description	When the diameter request is timed out from the external NF (AF or PCF), this metric is incremented.
Type	Counter
Dimensions	• appId • cmdCode • direction • msgType • reqDestHost • reqDestRealm • reqOrigHost • responseCode • reqOrigRealm
Example	ocbsf_diam_response_network_total{appId="16777236",cmdCode="265",direction="in",msgType="AAA",reqDestHost="oc-diam-gateway",reqDestRealm="xxx.com",reqOrigHost="",reqOrigRealm="",responseCode="timeout",} 1.0

Table 7-63 diam_controlled_shutdown_message_reject_total

Field	Details
Description	Indicates failure count because of forced shutdown feature.
Type	Counter
Dimensions	• state • response_code • destHost • destRealm • origHost • origRealm • appId • cmdCode • msgType • direction
Example	diam_controlled_shutdown_message_reject_total{msgType="Gx_CCR_I",appId="16777238",cmdCode="272",destHost="",destRealm="xxx.com",operationalState="PARTIAL_SHUTDOWN",origHost="pgw.xxx.com",origRealm="test.example.com",responseCode="5012",} 1.0

Table 7-64 topic_version

Field	Details
Description	Describes the current applied version of a given topic (mentioned in dimension topic_name) into the pod.
Type	Gauge
Dimensions	• Service Name • Pod Name

Table 7-65 ocbsf_diam_request_network_total

Field	Details
Description	Tracks total number of request messages of given command code to or from network.
Type	Counter
Dimensions	• appId • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • retry • retryReason

Table 7-66 ocbsf_diam_request_inter_total

Field	Details
Description	Tracks total number of request messages of given command code to or from host services.
Type	Counter
Dimensions	• appId • cmdCode • destHost • destRealm • direction • msgType • origHost • origRealm • retry • retryReason

Table 7-67 ocbsf_diam_realm_validation_failed_total

Field	Details
Description	Used to count the number of failed Destination-Realm validation at Diameter Gateway for BSF.
Type	Counter

Table 7-67 (Cont.) ocbsf_diam_realm_validation_failed_total

Field	Details
Dimensions	• appId • cmdCode • destHost • destRealm • origHost • origRealm • responseCode • validateRealmFailed • validateBindingRealmFailed
Example	ocbsf_diam_realm_validation_failed_total{appId="16777236",cmdCode="265",destHost="",destRealm="xxx.com",origHost="af.xxx.com",origRealm="xxx.com",responseCode="3003",validateRealmFailed="false", validateBindingRealmFailed="true"} 1.0 ; Type-Counter

7.11 NRF Management Service

Table 7-68 NRF Instance Status

Field	Details
Description	If the metric has value 0 - NRF is unavailable/unhealthy 1 - NRF is available/healthy
Type	Gauge
Dimensions	NrfUri - URI of the NRF Instance

Table 7-69 NRF Instance Status Count

Field	Details
Description	The apiRoot shall be specified in the following format: *'scheme'://'fqdn':'port'* If health check procedure is disabled, all NRF instances are marked as HEALTHY after successful NfRegistration.
Type	Gauge
Dimensions	NrfUri - URI of the NRF Instance HealthStatus FailureReason - Reason for the status

Table 7-70 NRF Instance Consecutive Healthy Count

Field	Details
Description	The metric shall have a minimum value of 0 and maximum value of healthCheckCount.
Type	Gauge
Dimensions	NrfUri - URI of the NRF Instance

Table 7-71 NRF Instance Consecutive Unhealthy Count

Field	Details
Description	The metric shall have a minimum value of 0 and maximum value of healthCheckCount.
Type	Gauge
Dimensions	NrfUri - URI of the NRF Instance

Table 7-72 DNS lookup requests

Field	Details
Description	The metric shall be pegged only if enableVirtualNrfResolution is set to true.
Type	Gauge
Dimensions	Scheme - http or https VirtualFqdn - Fqdn that shall be used by the alternate service for the DNS lookup.

Table 7-73 DNS lookup responses

Field	Details
Description	The metric shall be pegged only if enableVirtualNrfResolution is set to true.
Type	Gauge
Dimensions	Scheme - http or https VirtualFqdn - Fqdn that shall be used by the alternate service for the DNS lookup. HttpStatusCode - The status code as received in the response.

Table 7-74 DNS setup requests

Field	Details
Description	The metric shall be pegged only if enableVirtualNrfResolution is set to true.
Type	Counter
Dimensions	Scheme - http or https VirtualFqdn - Fqdn that shall be used by the alternate service for the DNS lookup.

Table 7-75 nrfclient_nfUpdate_status

Field	Details
Description	Indicates if the NfRegister/NfUpdate operation is successful with NRF after the NfProfile has been updated using the REST API. 0 - Update is not successful. 1 - Update is successful. NFs may use this metric to configure alerts.
Type	Gauge
Dimensions	• NfInstanceId - The NF's nfInstanceId as present in the NfProfile. • NfFqdn - The NF's FQDN as present in the NfProfile.

7.12 Overload Control Metrics

Table 7-76 service_resource_stress

Field	Details
Description	This metric tracks CPU, memory, failure count, and pending requests on the basis of which the overload level of a service is calculated.
Type	Gauge
Dimensions	type, Service

Table 7-77 service_resource_overload_level

Field	Details
Description	This metric tracks an individual resource's overload level that is calculated based on the resource usage and configured threshold.
Type	Gauge
Dimensions	type, Service

Table 7-78 load_level

Field	Details
Description	Provides information about the overload manager load level.
Type	Gauge
Dimensions	Service, namespace

Table 7-79 diam_overload_message_reject_total

Field	Details
Description	This metric tracks the total number of messages rejected due to overload on Diameter interface.
Type	Counter
Dimensions	priority, response_code **Other dimensions:**destHost, destRealm, origHost, origRealm, appId, cmdCode, msgType, direction

7.13 PerfInfo Metrics

Table 7-80 nf_load_info

Field	Details
Description	Provides information about service load.
Type	Gauge
Dimensions	• service • namespace
Example	nf_load_info{namespace="xxx",service="xxx"} 0.8486912141984638

Table 7-81 jvm_cpu_usage

Field	Details
Description	Springboot per service jvm_cpu_usage.
Type	Gauge
Dimensions	• service • namespace
Example	jvm_cpu_usage{namespace="xxx",service="xxx"} 0.2758240242725142

Table 7-82 jvm_memory

Field	Details
Description	Springboot per service jvm_memory.
Type	Gauge
Dimensions	• service • namespace
Example	jvm_memory{namespace="ttz",service="xxx"} 18.361382484436035

Table 7-83 cgroup_cpu_nanoseconds

Field	Details
Description	Reports the total CPU time (in nanoseconds) on each CPU core for all the tasks in the cgroup.
Type	Gauge
Dimensions	NA
Example	cgroup_cpu_nanoseconds 2.1782821080274e+013

Table 7-84 cgroup_memory_bytes

Field	Details
Description	Reports the memory usage.
Type	Gauge
Dimensions	NA
Example	cgroup_memory_bytes 1.31289088e+08

Table 7-85 load_level

Field	Details
Description	This metric provides information about the load level of a service.
Type	Gauge
Dimension	• service • namespace • isLeaderPod
Example	load_level{serivce="xxx"} L1

Table 7-86 system_overload_threshold_config_mode

Field	Details
Description	Indicates whether the overload level threshold configuration is based on STANDALONE or PROFILE mode.
Type	Gauge
Dimension	• namespace • isLeaderPod
Example	system_overload_threshold_config_mode 1.0

Table 7-87 active_overload_threshold_fetch_failed

Field	Details
Description	Indicates whether the active profile data is fetched successfully or failed to fetch.
Type	Gauge
Dimension	• namespace • isLeaderPod The value of this dimension can be either 0 or 1. Where 0, represents "Successfully fetched the active threshold"and 1 represents "Failure in fetching the active threshold".
Example	active_overload_threshold_fetch_failed 1.0

Table 7-88 load_level_report_total

Field	Details
Description	This metric is used to track: • the number of times load level calculation is performed • the number of times load level changes • how long the particular level was active
Type	Counter
Dimension	• level • service • prevLevel • namespace • levelChangeType • isLeaderPod
Example	load_level_report_total{namespace="hi-riley", service="pcf-occnp-pcrf-core", isLeaderPod="True", level="Normal", levelChangeType="-"} 2.0

Table 7-89 service_resource_stress

Field	Details
Description	This metric tracks CPU, memory, failure count, and pending requests on the basis of which the overload level of a service is calculated.
Type	Gauge
Dimension	• type • service • namespace • isLeaderPod
Example	service_resource_stress{service="xxx", type="xxx"} 10.0

Table 7-90 service_resource_overload_level

Field	Details
Description	This metric tracks an individual resource's overload level that is calculated based on the resource usage and configured threshold.
Type	Gauge
Dimension	• type • service • namespace • isLeaderPod
Example	service_resource_overload_level{service="xxx", type="xxx"}2.0

Table 7-91 service_resource_overload_level_report_total

Field	Details
Description	This metric is used to track: • the number of times load level calculation is performed. • the number of times load level changes. • for how long the particular level was active for each metric type.
Type	Counter

Table 7-91 (Cont.) service_resource_overload_level_report_total

Field	Details
Dimension	• level Possible values: – L1 – L2 – L3 – Normal • service • prevLevel • levelChangeType Possible values: – increment – decrement • isLeaderPod Possible values: – True – False • type Possible values: – cpu – memory – svc_failure_count – svc_pending_count • namespace
Example	service_resource_overload_level_report_total{namespace="hi-riley", service="pcf-occnp-pcrf-core", isLeaderPod="True", level="Normal", levelChangeType="-", type="cpu"} 2.0

Table 7-92 http_out_conn_request

Field	Details
Description	This counter metric is used to count the number of http API Egress requests.
Type	Counter
Dimension	• servicenameNon3gpp • serviceResource • serviceVersion • operationType • namespace • params • isLeaderPod
Example	-

Table 7-93 http_out_conn_response

Field	Details
Description	This counter metric is used to count the number of http API Egress responses.
Type	Counter

Table 7-93 (Cont.) http_out_conn_response

Field	Details
Dimension	• servicenameNon3gpp • serviceResource • serviceVersion • outcome • namespace • operationType • responseCode • params • cause • isLeaderPod
Example	-

Table 7-94 overload_manager_enabled

Field	Details
Description	This metric indicates whether overload manager is enabled or disabled.
Type	Gauge
Dimension	• source Possible values: – DIAM_GW – INGRESS_GW – PERF_INFO • namespace
Example	overload_manager_enabled{namespace="hi-riley", source="DIAM_GW"} 1

Table 7-95 leader_pod

Field	Details
Description	This metric is used to know the leader pod.
Type	Gauge
Dimension	• namespace
Example	leader_pod{namespace="hi-riley"} 1

For more information about dimensions, see Binding Support Function Metrics.

7.14 Pod Congestion Metrics

Table 7-96 ocbsf_pod_congestion_state

Field	Details
Description	Tracks congestion state of pod.
Type	Gauge
Dimensions	level = 0,1,2 (0 = Normal, 1 = DoC, 2 = Congested)

Table 7-97 ocbsf_pod_resource_stress

Field	Details
Description	Tracks CPU, memory, queue usage (percentage) based on which POD is calculating its congestion state.
Type	Gauge
Dimensions	type = "PendingRequest","CPU","Memory"

Table 7-98 ocbsf_pod_resource_congestion_state

Field	Details
Description	Tracks individual resource's congestion state calculated based on the resource usage and configured threshold.
Type	Gauge
Dimensions	type = "PendingRequest","CPU","Memory" level = 0,1,2 (0 = Normal, 1 = DoC, 2 = Congested)

Table 7-99 ocbsf_diam_congestion_message_reject_total

Field	Details
Description	Tracks number of messages rejected due to congestion.
Type	Counter
Dimensions	priority = calculated or received DRMP priority of message being rejected response_code = response code sent with rejected message destHost, destRealm, origHost, origRealm, appId, cmdCode, *msgType*, direction

7.15 User-Agent Header Metrics

The following metric is introduced for User-Agent Header:

Table 7-100 oc.ingressgateway.http.requests

Field	Details
Description	This metric is pegged for every incoming request. If the User-Agent header is not present, then UNKNOWN will be pegged. This will be independent of the User Agent validation feature at the Ingress Gateway.
Type	Counter
Dimensions	• consumerNfType • consumerInstanceId • ConsumerFqdn

7.16 Query Service Metrics

Table 7-101 queryservice_request

Field	Details
Description	Number of query requests received.
Type	Counter
Dimensions	RequestType
Example	queryservice_response_total{Code="2xx",ReqType="GET",} 195.0

Table 7-102 queryservice_response

Field	Details
Description	Number of responses sent for query requests.
Type	Counter
Dimensions	RequestType
Example	queryservice_request_total{ReqType="GET",} 257.0

Table 7-103 queryservice_sessionDelete_request

Field	Details
Description	Total number of query requests to delete PCF bindings.
Type	Counter
Dimensions	• ResourceType • Result_Code
Example	queryservice_sessionDelete_request{ReqType="DELETE",} 257.0

Table 7-104 queryservice_sessionDelete_response

Field	Details
Description	Total number of responses for delete PCF bindings query requests.
Type	Counter
Dimensions	• ResourceType • Result_Code
Example	queryservice_sessionDelete_response{Code="2xx",ReqType="DELETE",} 195.0

7.17 TLS Metrics

The following table describes the TLS metrics and the respective dimensions:

Table 7-105 oc_ingressgateway_incoming_tls_connections

Field	Details
Description	Number of TLS Connections received on the Ingress Gateway and their negotiated TLS versions. The versions can be TLSv1.3 or TLSv1.2

Table 7-105 (Cont.) oc_ingressgateway_incoming_tls_connections

Field	Details
Type	Gauge
Dimensions	• host • NegotiatedTLSVersion • direction • instanceIdentifier
Example	-

Table 7-106 oc_egressgateway_incoming_tls_connections

Field	Details
Description	Number of TLS Connections received on the Egress Gateway and their negotiated TLS versions. The versions can be TLSv1.3 or TLSv1.2
Type	Gauge
Dimensions	• host • NegotiatedTLSVersion • direction • instanceIdentifier
Example	-

Table 7-107 security_cert_x509_expiration_seconds

Field	Details
Description	Indicates the time to certificate expiry in epoch seconds.
Type	Histogram
Dimensions	serialNumber
Example	-

Table 7-108 diam_conn_network

Field	Details
Description	Indicates the number of TLS connections per TLS version.
Type	Gauge
Dimensions	tlsversion, peerHost, and peerRealm
Example	-

Table 7-109 diam_failed_conn_network

Field	Details
Description	Indicates the number of failed TLS connections. **Note:** It is applicable when we configure **Initiate Connection** to `true` in peer node configurations in the CNC Console.
Type	Gauge
Dimensions	• tlsversion • reason

Table 7-109 (Cont.) diam_failed_conn_network

Field	Details
Example	diam_failed_conn_network{peerName="dgw",reason="SSL Handshake Exception",} 1.0

Table 7-110 diam_conn_network_responder

Field	Details
Description	Indicates the number of allowed TLS responder connections with or without the peer configuration.
Type	Gauge
Dimensions	• tlsversion • peerconfigvalidated • peerHost • peerRealm
Example	-

Table 7-111 dgw_tls_cert_expiration_seconds

Field	Details
Description	Indicates the number of allowed TLS responder connections with or without the peer configuration.
Type	Gauge
Dimensions	• serialNumber (a number assigned by CA to each certificate) • subject (information about the cert issuer)
Example	dgw_tls_cert_expiration_seconds{serialNumber="122859034516052844067924392230910496431389299229",subject="OU=CGIU, O=ORCL, L=BLR, ST=KA, C=IN",} 1.797882352E9

7.18 NRF Client Metrics

NF status and NF load metrics

Table 7-112 nrfclient_perf_info_nf_profile_load

Field	Details
Description	The current Load of the NF.
Type	Gauge
Dimensions	-

Table 7-113 nrfclient_current_nf_status

Field	Details
Description	The current operative status of the NF. The gauge shall be indicate the status as below: • 0 - REGISTERED • 1 - DEREGISTERED • 2 - SUSPENDED • 3 - UNDISCOVERABLE • 4 - UNKNOWN
Type	Gauge
Dimensions	• NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Table 7-114 nrfclient_nf_status_with_nrf

Field	Details
Description	The operative status of the NF communicated to the NRF. The gauge shall be indicate the status as below: • 0 - REGISTERED • 1 - DEREGISTERED • 2 - SUSPENDED • 3 - UNDISCOVERABLE • 4 - UNKNOWN
Type	Gauge
Dimensions	• NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

NRF Health Status

Table 7-115 nrfclient_nrf_operative_status

Field	Details
Description	The current operative status of the NRF Instance. If the metric has value • 0 - NRF is unavailable or unhealthy • 1 - NRF is available or healthy
Type	Gauge
Dimensions	NrfUri - URI of the NRF Instance

Table 7-116 nrfclient_nrf_status_total

Field	Details
Description	Total number of times an NRF instance is marked as healthy or unhealthy. The apiRoot is specified in the format *'scheme'://'fqdn':'port'*. **Note**: If health check procedure is disabled, all NRF instances are marked as HEALTHY after successful NF registration.
Type	Counter

Table 7-116 (Cont.) nrfclient_nrf_status_total

Field	Details
Dimensions	NrfUri- URI of the NRF InstanceHealthStatus FailureReason - Reason for the status

Table 7-117 nrfclient_nrf_successive_healthy_count

Field	Details
Description	The metric shows the consecutive number of times the NRF is considered as healthy. The metric has a minimum value of 0 and maximum value of *healthCheckCount*.
Type	Counter
Dimensions	NrfUri- URI of the NRF Instance

Table 7-118 nrfclient_nrf_successive_unhealthy_count

Field	Details
Description	The metric shows the consecutive number of times the NRF is considered as unhealthy
Type	Counter
Dimensions	NrfUri- URI of the NRF Instance

NF - NRF-Client metrics

Table 7-119 nrfclient_on_demand_conn_in_request_total

Field	Details
Description	Total number of on-demand requests received from the backend NF to NRF Client.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Table 7-120 nrfclient_on_demand_conn_out_response_total

Field	Details
Description	Total number of on-demand responses sent to the backend NF to NRF Client.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile. • StatusCode - The HttpStatusCode as received from the NRF or generated by NRF-client.

Table 7-121 nrfclient_on_demand_processing_latency_ms

Field	Details
Description	Total message processing time duration in milliseconds.
Type	Histogram
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Table 7-122 ocpm_nrf_tracing_request_timeout_total

Field	Details
Description	Total number of requests timeout sent to the backend NF from NRF Client.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

NRF-Client - NRF metrics

Table 7-123 nrfclient_nw_conn_out_request_total

Field	Details
Description	Total number of times NRF-client has sent a request to NRF. This includes autonomous requests as well as on-demand requests.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

Table 7-124 nrfclient_nw_conn_in_response_total

Field	Details
Description	Total number of times NRF-client has received a response from NRF.
Type	Counter
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile. • StatusCode - The HttpStatusCode as received from the NRF or generated by NRF-client.

Table 7-125 nrfclient_nw_conn_in_notify_request_total

Field	Details
Description	Total number of nfStatusNotify requests received from NRF.
Type	Counter
Dimensions	• EventType - The EventType for which the notification is triggered. • NfInstanceID - The NfInstanceId for which the notification is triggered.

Table 7-126 nrfclient_nw_conn_out_notify_response_total

Field	Details
Description	Total number of *nfStatusNotify* responses sent to NRF.
Type	Counter
Dimensions	• EventType - The EventType for which the notification is triggered. • NfInstanceID - The NfInstanceId for which the notification is triggered. • HttpStatusCode - The HttpStatusCode sent by NRF-Client.

Table 7-127 nrfclient_network_message_processing_latency

Field	Details
Description	Total message processing time duration.
Type	Histogram
Dimensions	• MessageType - The service request Type. • NfType - The NF's NfType as present in the registered NfProfile. • NfInstanceID - The NF's nfInstanceId as present in the registered NfProfile. • NfFqdn - The NF's FQDN as present in the registered NfProfile.

7.19 Metrics for Automated Certificate Lifecycle Management

The following metrics are used to support automated certificate lifecycle management for BSF:

Table 7-128 oc_certificatemanagement_tls_certificate_info

Field	Details
Description	This metric is used to peg status of TLS certificates. This metric is further used for raising alarms.
Type	Gauge
Dimensions	• CertificateName • SecretName • Status (VALID, CORRUPT, MISSING, EXPIRED) • Service (IngressGateway, EgressGateway)
Example	occnp_oc_certificatemanagement_tls_certificate_info{CertificateName="key-password.txt,bsf.cer,pcf.pem,trust-chain-password.txt,trust-chain.cer,",SecretName="bsf-igw-tls-ssl-bundle",Service="IngressGateway",Status="VALID",} 1.0

A
Ingress Gateway Metrics

Ingress Gateway Metrics

Table A-1 oc_ingressgateway_http_requests_total

Field	Details
Description	This metric is pegged as soon as the request reaches the Ingress gateway in the first custom filter of the application.
Type	Counter
Dimension	• NFType • NFServiceType • Host • HttpVersion • Scheme • Route_path • InstanceIdentifier • ClientCertIdentity

Table A-2 oc_ingressgateway_http_responses_total

Field	Details
Description	This metric is pegged in the last custom filter of the Ingress gateway while the response is being sent back to the consumer NF.
Type	Counter
Dimension	• Status • Method • Route_path • NFType • NFServiceType • Host • HttpVersion • Scheme • Identifier • ClientCertIdentity

Table A-3 oc_ingressgateway_request_latency_seconds

Field	Details
Description	This metric is pegged in the last custom filter of the Ingress gateway while the response is being sent back to the consumer NF. This metric tracks the amount of time taken for processing the request. It starts as soon the request reaches the first custom filter of the application and lasts till the response is sent back to the consumer NF from the last custom filter of the application.
Type	Timer

Table A-3 (Cont.) oc_ingressgateway_request_latency_seconds

Field	Details
Dimension	• quantile • InstanceIdentifier

Table A-4 oc_ingressgateway_connection_failure_total

Field	Details
Description	This metric is pegged in the customized Jetty Client as soon as it fails to connect to the destination service with direction as ingressOut. Here in case of Ingress gateway, the destination service is a backend microservice of the NF. And TLS connection failure metrics when connecting to ingress with direction as ingress.
Type	Counter
Dimension	• Host • Port • Direction • InstanceIdentifier • error_reason

Table A-5 oc_ingressgateway_global_ratelimit_total

Field	Details
Description	This metric is pegged in the custom filter implemented to check the global rate limit conditions.
Type	Counter
Dimension	• Method • Route_path • Scheme • InstanceIdentifier • Status (Rate limit Status field is different here)

Table A-6 oc_ingressgateway_route_ratelimit_total

Field	Details
Description	This metric is pegged in the custom filter implemented to check the route level rate limit conditions.
Type	Counter
Dimension	• Method • Route_path • Scheme • InstanceIdentifier • Status (Rate limit Status field is different here)

Table A-7 oc_ingressgateway_request_processing_latency_seconds

Field	Details
Description	This metric is pegged in the last custom filter of the Ingress gateway while the response is being sent back to the consumer NF. This metric captures the amount of time taken for processing of the request only within Ingress gateway. It starts as soon the request reaches the first custom filter of the application and lasts till the request is forwarded to the destination.
Type	Timer
Dimension	• quantile • InstanceIdentifier

Table A-8 oc_ingressgateway_jetty_request_stat_metrics_total

Field	Details
Description	This metric is pegged for every event occurred when a request is sent to IGW.
Type	Counter
Dimension	• event • client_type • InstanceIdentifier

Table A-9 oc_ingressgateway_jetty_response_stat_metrics_total

Field	Details
Description	This metric is pegged for every event occurred when a response is received by IGW
Type	Counter
Dimension	• event • client_type • InstanceIdentifier

Table A-10 oc_ingressgateway_jetty_latency_seconds

Field	Details
Description	This metric is pegged in Jetty response listener that captures the amount of time taken for processing of the request by jetty client.
Type	Timer
Dimension	• quantile • InstanceIdentifier

Table A-11 oc_ingressgateway_netty_latency_seconds

Field	Details
Description	This metric is pegged in Netty outbound handler that captures the amount of time taken for processing of the request by netty server.
Type	Timer
Dimension	• quantile • InstanceIdentifier

Table A-12 oc_ingressgateway_request_content_metrics_total

Field	Details
Description	This metric is pegged by default filter RequestContentMetrics. It pegs whether request has request body or not.
Type	Counter
Dimension	• method • content_available • InstanceIdentifier

Table A-13 oc_ingressgateway_xfcc_header_validate_total

Field	Details
Description	This metric is pegged when xfccHeaderValidation is enabled in XfccHeaderValidationFilter. This metric along with the specified dimension captures the successful/ un-successful validation of XFCC header in the incoming request.
Type	Counter
Dimension	• Route_path • Status • Cause • CertsCompared • InstanceIdentifier • ErrorOriginator

Table A-14 oc_configclient_request_total

Field	Details
Description	This metric is pegged whenever config client is polling for configuration update from common configuration server.
Type	Counter
Dimension	• Release version • Config version

Table A-15 oc_configclient_response_total

Field	Details
Description	This metrics is pegged whenever config client receives response from common configuration server.
Type	Counter
Dimension	• Release version • Config version • Updated

Table A-16 oc_ingressgateway_incoming_tls_connections

Field	Details
Description	Number of TLS Connections received on the Ingress Gateway and their negotiated TLS versions. The versions can be TLSv1.3 or TLSv1.2.
Type	Gauge
Dimension	• NegotiatedTLSVersion • Host • Direction • InstanceIdentifier

Table A-17 security_cert_x509_expiration_seconds

Field	Details
Description	Indicates the time to certificate expiry in epoch seconds.
Type	Histogram
Dimension	• NegotiatedTLSVersion • Host • Direction • InstanceIdentifier

Ingress Metrics Common Tags

Tags	Description	Possible Values
Method	Http method	GET, PUT, POST, DELETE, PATCH
NFType	Name of the NF Type.	For example: Path is /n**xxx-yyy**/v**z**/..... Where **XXX(Upper Case)** is NFType UNKNOWN if unable to extract NFType from the path
NFServiceType	Name of the Service within the NF.	For example: Path is /n**xxx-yyy**/v**z**/..... Where nxxx-yyy is NFServiceType UNKNOWN if unable to extract NFServiceType from the path
Host	(Ip or fqdn): port of ingress gateway	NA
HttpVersion	Http protocol version	HTTP/1.1, HTTP/2.0
Scheme	Http protocol scheme	HTTP, HTTPS, UNKNOWN
ClientCertIdentity	Cerificate Identity of the client	SAN=127.0.0.1,localhost CN=localhost, N/A if data is not available
Route_Path	Path predicate/Header predicate that matched the current request	NA
InstanceIdentifier	Prefix of the pod configured in helm when there are multiple instances in same deployment	Prefix configured in helm otherwise UNKNOWN

Tags	Description	Possible Values
ErrorOriginator	This tag captures the ErrorOriginator	ServiceProducer, Nrf, IngresGW, None
oc_ingressgateway_route_ratelimit_**Status** oc_ingressgateway_global_ratelimit_**Status**	Request accepted or dropped	accepted, dropped
oc_ingressgateway_connection_failure_**Host**	destination ip/fqdn	NA
oc_ingressgateway_connection_failure_**Port**	destination port	NA
oc_ingressgateway_xfcc_header_validate_**Status**	Https Status value after performing xfccHeaderValidation at IGW	200 (OK), 400 (BAD_REQUEST)
oc_ingressgateway_xfcc_header_validate_**Cause**	This tag determines the validation cause for the xfcc header validation metric being pegged	VALIDATION_FAILURE, VALIDATION_SUCCESS, HEADER_NOT_FOUND
oc_ingressgateway_xfcc_header_validate_**CertsCompared**	This tag captures the total number of certificates compared in XFCC header at IGW during the header validation	Count of the certificates compared (0,1,2..)
oc_configclient_request_total_**releaseVersion**	This tag indicates the current release version of ingress gateway	Picked from helm chart{{ .Chart.Version }}
oc_configclient_request_total_**configVersion**	This tag indicates the configuration version that ingress gateway is currently maintaining	Initial value is 0. Incremental value received from config server whenever there is an update from config server (0, 1, 2...)
oc_configclient_response_total_**releaseVersion**	This tag indicates the current release version of ingress gateway	Picked from helm chart {{ .Chart.Version }}
oc_configclient_response_total_**configVersion**	This tag indicates the configuration version that ingress gateway is currently maintaining	Value received from config server (1, 2...)
oc_configclient_response_total_**updated**	This tag indicates whether the configuration was updated or not	true/false

OAuth Metrics

Below are the metrics and their respective tags that are available in OAuth:

Table A-18 oc_oauth_validation_successful _total

Field	Details
Description	This metric is pegged in the OAuth validator implementation if the received OAuth token is validated successfully. The implementation of OAuth validator is used in Ingress Gateway.
Type	Counter
Dimension	• issuer • subject • scope

Table A-19 oc_oauth_validation_failure _total

Field	Details
Description	This metric is pegged in the implementation of OAuth validator if the validation of the the received OAuth token fails. The implementation of OAuth validator is used in Ingress G;ateway.
Type	Counter
Dimension	• issuer • subject • scope • reason

OAuth Metrics Common Tags

Tags	Description	Possible Values
scope	NF service name(s) of the NF service producer(s), separated by whitespaces	NA
issuer	NF instance id of NRF	NA
subject	NF instance id of service consumer	NA
reason	reason contains the human readable message for OAuth validation failure	NA

Table A-20 oc_ingressgateway_msgcopy_requests_total

Field	Details
Description	This is incremented whenever ingress request message is sent or acknowledged from Kafka.
Type	Counter
Dimension	

Table A-21 oc_ingressgateway_msgcopy_responses_total

Field	Details
Description	This is incremented whenever ingress response message is sent or acknowledged from Kafka.
Type	Counter
Dimension	

B
Egress Gateway Metrics

Egress Gateway Metrics

Table B-1 oc_egressgateway_http_requests_total

Field	Details
Available Tags	• Method • NFType • NFServiceType • Host • HttpVersion • Scheme • Proxy • InstanceIdentifier
Pegging Instance	This metric is pegged as soon as the request reaches the Egress Gateway in the first custom filter of the application.

Table B-2 oc_egressgateway_http_responses_total

Field	Details
Available Tags	• Status • Method • NFType • NFServiceType • Host • HttpVersion • Scheme • InstanceIdentifier • Direction • BlacklistedFqdn
Pegging Instance	This metric will be pegged in the last custom filter of the Egress gateway while the response is being sent back to backend NF microservice with direction as egress. This will also be pegged when the response is fetched in Jetty responseListener with direction as egressOut. BlacklistedFqdn tag will be filled with BlacklistedFqdn when request is sent with blacklisted producer.

Table B-3 oc_egressgateway_request_latency_seconds

Field	Details
Available Tags	• quantile • InstanceIdentifier
Pegging Instance	This metric is pegged in the last custom filter of the Ingress Gateway while the response is being sent back to the consumer NF. This metric tracks the amount of time taken for processing the request. It starts as soon as the request reaches the first custom filter of the application and lasts till, the response is sent back to the the consumer NF from the last custom filter of the application.

Table B-4 oc_egressgateway_connection_failure_total

Field	Details
Available Tags	• Host • Port • InstanceIdentifier • Direction • error_reason
Pegging Instance	This metric will be pegged in the customized Jetty Client as soon as it fails to connect to the destination service. Here in case of Egress gateway, the destination service will be Producer NF. This will also be pegged when the request to Producer NF fails in Jetty request Listener with direction as egressOut

Table B-5 oc_egressgateway_notification_ratelimit_total

Field	Details
Available Tags	• Method • Scheme • InstanceIdentifier
Pegging Instance	This metric is pegged in the custom filter implemented to check the notification rate limit conditions.

Table B-6 oc_egressgateway_request_processing_latency_seconds

Field	Details
Available Tags	• quantile • InstanceIdentifier

Table B-6 (Cont.) oc_egressgateway_request_processing_latency_seconds

Field	Details
Pegging Instance	This metric is pegged in the last custom filter of the Egress Gateway while the response is sent back to the consumer NF. This metric tracks the amount of time taken for processing the request only within Egress Gateway. It starts as soon as the request reaches the first custom filter of the application and lasts till the request is forwarded to the destination.

Table B-7 oc_egressgateway_jetty_request_stat_metrics_total

Field	Details
Available Tags	• event • client_type • InstanceIdentifier
Pegging Instance	This metric is pegged for every event occurred when a request is sent to EGW

Table B-8 oc_egressgateway_jetty_response_stat_metrics_total

Field	Details
Available Tags	• event • client_type • InstanceIdentifier
Pegging Instance	This metric is pegged for every event occurred when a response is received by EGW

Table B-9 oc_egressgateway_jetty_latency_seconds

Field	Details
Available Tags	• quantile • InstanceIdentifier
Pegging Instance	This metric is pegged in Jetty response listener that captures the amount of time taken for processing of the request by jetty client

Table B-10 oc_egressgateway_netty_latency_seconds

Field	Details
Available Tags	• quantile • InstanceIdentifier
Pegging Instance	This metric is pegged in Netty outbound handler that captures the amount of time taken for processing of the request by netty server

Table B-11 oc_egressgateway_request_content_metrics_total

Field	Details
Available Tags	• method • content_available • InstanceIdentifier
Pegging Instance	This metric is pegged by default filter RequestContentMetrics. It pegs whether request has request body or not and the method.

Table B-12 oc_egressgateway_blacklisted_producer_total

Field	Details
Available Tags	• NFType • NFServiceType • InstanceIdentifier • Host • Route_path
Pegging Instance	This metric is a counter. Track number of times producer is blacklisted.

Table B-13 oc_configclient_request_total

Field	Details
Available Tags	• Release version • Config version
Pegging Instance	This metric will be pegged whenever config client is polling for configuration update from common configuration server

Table B-14 oc_configclient_response_total

Field	Details
Available Tags	• Release version • Config version • Updated
Pegging Instance	This metrics will be pegged whenever config client receives response from common configuration server

Table B-15 oc_egressgateway_sbiRouting_http_responses_total

Field	Details
Available Tags	• Sbi_Fqdn • Reroute_Path • Attempt • HttpVersion • Scheme • InstanceIdentifier

Table B-15 (Cont.) oc_egressgateway_sbiRouting_http_responses_total

Field	Details
Pegging Instance	This metric is pegged in the SBIRoutingFilter only when SBIRouting feature is enabled for a route to which request is sent to Egress Gateway.

Table B-16 oc_egressgateway_sbiRouting_http_requests_total

Field	Details
Available Tags	• Sbi_Fqdn • Reroute_Path • Attempt • HttpVersion • Scheme • InstanceIdentifier • ErrorOriginator
Pegging Instance	This metric is pegged in the SBIRoutingFilter only when SBIRouting feature is enabled for a route to which request is sent to Egress Gateway and when sbiRerouteEnabled is set to true and reroute mechanism is executed.

Table B-17 oc_egressgateway_outgoing_tls_connections

Field	Details
Description	Number of TLS Connections received on the Egress Gateway and their negotiated TLS versions. The versions can be TLSv1.3 or TLSv1.2.
Type	Gauge
Dimension	• NegotiatedTLSVersion • Host • Direction • InstanceIdentifier

Table B-18 security_cert_x509_expiration_seconds

Field	Details
Description	Indicates the time to certificate expiry in epoch seconds.
Type	Histogram
Dimension	• NegotiatedTLSVersion • Host • Direction • InstanceIdentifier

Egress Gateway Metrics Common Tags

Metric Type	Available Tags	Possible Values
Method	Http method	GET, PUT, POST, DELETE, PATCH

Metric Type	Available Tags	Possible Values
NFType	Name of the NF Type	"UNKNOWN" (Updates are available when Ingress is 5G aware)
NFServiceType	Name of the Service within the NF	"UNKNOWN" (Updates are available when Ingress is 5G aware)
Host	(IP or fqdn): port of ingress gateway	Not Applicable
HttpVersion	Http protocol version (http1.1/ http2)	HTTP1.1, HTTP2.0
Scheme	Http protocol scheme (http/https)	HTTP, HTTPS, UNKNOWN
Proxy	Value received for "x-custom-egress-proxy-header".	Unknown or value of "x-custom-egress-proxy-header".
oc_egressgateway_connection_failure_Host	destination ip/fqdn	Not Applicable
oc_egressgateway_connection_failure_Port	destination port	Not Applicable
BlacklistedFqdn	Blacklisted Producer Fqdn	Unknown or Blacklisted Producer Fqdn
oc_configclient_request_total_**releaseVersion**	This tag indicates the current release version of egress gateway	Picked from helm chart{{ .Chart.Version }}
oc_configclient_request_total_**configVersion**	This tag indicates the configuration version that egress gateway is currently maintaining	Initial value is 0. Incremental value received from config server whenever there is an update from config server (0, 1, 2...)
oc_configclient_response_total_**releaseVersion**	This tag indicates the current release version of egress gateway	Picked from helm chart{{ .Chart.Version }}
oc_configclient_response_total_**configVersion**	This tag indicates the configuration version that egress gateway is currently maintaining	Value received from config server (1, 2...)
oc_configclient_response_total_**updated**	This tag indicates whether the configuration was updated or not	true/false

Oauth Metrics

Table B-19 oc_oauth_nrf_request_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope • NrfFqdn
Pegging Instance	This metric is pegged in the OAuth client implementation if the request is sent to NRF for requesting the OAuth token. OAuth client implementation will be used in Egress gateway.

Table B-20 oc_oauth_token_cache_total

Field	Details
Available Tags	• ConsumerNFInstanceId • ConsumerNFType • TargetNFType • TargetNFInstanceId • scope
Pegging Instance	This metric is pegged in the OAuth Client Implementation if the OAuth token is found in the cache.

Table B-21 oc_oauth_validation_successful_total

Field	Details
Available Tags	• issuer • subject • scope
Pegging Instance	This metric is pegged in OAuth validator implementation if the received OAuth token is validated successfully. OAuth validator implementation is used in Ingress Gateway.

Table B-22 oc_oauth_validation_failure_total

Field	Details
Available Tags	• issuer • subject • scope • reason
Pegging Instance	This metric is pegged in OAuth validator implementation if the validation of the the received OAuth token is failed. OAuth validator implementation is used in Ingress gateway.

OAuth Metrics common tags

Common Tags	Description	Possible Values
ConsumerNFInstanceId	NF instance id of the NF service consumer	Not Applicable
ConsumerNFType	The NF type of the NF service consumer	NRF, UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC,5G_EIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF
TargetNFType	The NF type of the NF service producer	NRF, UDM, AMF, SMF, AUSF, NEF, PCF, SMSF, NSSF, UDR, LMF, GMLC,5G_EIR, SEPP, UPF, N3IWF, AF, UDSF, BSF, CHF, NWDAF

Common Tags	Description	Possible Values
TargetNFInstanceId	NF instance id of the NF service producer	Not Applicable
scope	NF service name(s) of the NF service producer(s), separated by whitespaces	Not Applicable
StatusCode	Status code of NRF access token request	Bad Request, Internal Server Error, and so on (HttpStatus.*)
ErrorOriginator	from where the error is originated (nrf or egress)	Nrf, EgressGW
issuer	NF instance id of NRF	Not Applicable
subject	NF instance id of service consumer	Not Applicable
reason	reason contains the human readable msg for OAuth validation failure	Not Applicable
NrfFqdn	NrfFqdn tag determines the corresponding fqdn of NRF where the request has been forwarded to.	Nrf-Fqdn (dynamic value based on Fqdn), NA
NrfClientUrl	This tag determines the url of NRF-Client Mgmt Svc where subscription requests are sent from OAuth Client module in EGW.	URL of NRF-Client Mgmt Svc (Dynamic value)
EgwNotificationUrl	This tag determines the notification URL mapped in OAuth Client module of EGW where NRF-Client Mgmt Svc will send notifications requests.	Notification URL (Dynamic value)
ConfigurationType	This tag determines the type of configuration in place for OAuth Client in Egress Gateway. If nrfClientQueryEnabled Helm parameter in oauthClient Helm configurations at Egress Gateway is false then the ConfigurationType is STATIC, else DYNAMIC.	STATIC, DYNAMIC

Table B-23 oc_egressgateway_msgcopy_requests_total

Field	Details
Description	This is incremented whenever egress request message is sent or acknowledged from Kafka.
Type	Counter
Dimension	

Table B-24 oc_egressgateway_msgcopy_responses_total

Field	Details
Description	This is incremented whenever egress response message is sent or acknowledged from Kafka.
Type	Counter
Dimension	

C

HTTP Status Codes Supported on SBI

Table C-1 HTTP Status Codes Supported on Service Based Interface (SBI)

HTTP Status Code	Description
204	There is no PCF session binding information matching the query parameters.
400	• The HTTP request contains an unsupported API name or API version in the URI. • The HTTP request has an invalid format. • The HTTP request contains an unsupported query parameter in the URI. • The HTTP request contains an invalid value for a mandatory parameter. • The HTTP request contains a semantically incorrect value for an optional parameter. • A mandatory query parameter is missing in the HTTP request. • The HTTP request contains a semantically incorrect value for a mandatory IE. • The HTTP request contains a semantically incorrect value for an optional IE. • A mandatory IE for an HTTP method is not included in the payload body of the request. • The request is rejected due to a malformed request. • The BSF found more than one binding resource. Therefore, the selected PCF cannot be provided.
401	Unauthorized With Header "WWW-Authenticate"
403	Request is forbidden.
404	The request for modification or deletion of a subscription is rejected because the subscription is not found in the NF.
405	The HTTP request is rejected as the performed operation is not allowed.
406	The request is not acceptable.
408	The request is rejected is segmented and all parts of the message are not received within the expected timeframe.
409	The request is rejected due to schema errors and conflicts in versions.
410	This requested resource has been permanently deleted.
411	The request is rejected due to the incorrect value of a Content-length header field.
412	The request is rejected due to incorrect conditions in the GET request.
413	The payload is larger than the limit.
414	The request URI is longer than the limit.
415	The HTTP request contains an unsupported payload type.
429	The request is rejected due to excessive traffic, which if continued over time, may lead to (or may increase) an overload situation.
500	• The request is rejected due to insufficient resources. • The request is rejected due to unspecified reasons at the NF. • The request is rejected due to a generic error condition in the NF.
503	The NF experiences congestion and performs overload control that does not allow the request to be processed.
504	This error code is generated in case of timeout due to inactivity.

D
Error Code Dictionary

Table D-1 Error Code Dictionary for BSF Management

App Error Id	Description	Cause	Action

EC-OBSF-BSF_MGMT-REQVLD-EI-05-01-400-00005-NA-02	The
	
	`GET`
	
	request to BSF failed with a 400 status code and cause
	
	`MANDATORY_QUERY_PARAM_INCORRECT`
	
	.
		The previous error appears whenever the Binding Request Query contains multiple UE Addresses (e.g. a MAC-48 Address and an IPv4 Address), or the mandatory query parameters have an incorrect format.	NA

EC-OBSF-BSF_MGMT-REQVLD-EI-05-01-400-00006-NA-02	The
	
	`GET`
	
	request to BSF failed with a 400 status code and cause
	
	`OPTIONAL_QUERY_PARAM_INCORRECT`
	
	.
		The previous error appears whenever the Binding Request optional query parameters has an incorrect format or value.	NA

EC-OBSF-BSF_MGMT-REQVLD-EI-05-01-400-00007-NA-02	The GET request to BSF failed with a 400 status code and cause `MANDATORY_QUERY_PARAM_MISSING` .	The previous error appears whenever the Binding Request Query does not contain a mandatory parameter. Mandatory parameters are the following: • UE Direction – IPv4 Address and/or Ipv6 Prefix – MAC-48 Address	NA

Table D-1 (Cont.) Error Code Dictionary for BSF Management

App Error Id	Description	Cause	Action
EC-OBSF-BSF_MGMT-INTRNL-EI-05-02-500-00000-01-02	The POST request to BSF failed with a 500 status code and cause INTERNAL_SERVER_ERROR .	The previous error appears whenever an internal error occurs on BSF Management Service while trying to register.	NA
EC-OBSF-BSF_MGMT-REQVLD-EI-05-02-400-00003-01-02	The POST request to BSF failed with a 400 status code and cause INVALID_MSG_FORMAT .	The previous error appears whenever the Binding Data from the Binding Request contains multiple UE Addresses (e.g. a MAC-48 Address and an IPv4 Address), or the IP Address is missing its IPv4 Address.	NA
EC-OBSF-BSF_MGMT-REQVLD-EI-05-02-400-00008-01-02	The POST register request to BSF failed with a 400 status code and cause MANDATORY_IE_INCORRECT .	The previous error appears whenever a mandatory IE in the Binding Data from the Binding Request has an incorrect format.	NA
EC-OBSF-BSF_MGMT-REQVLD-EI-05-02-400-00009-01-02	The POST request to BSF failed with a 400 status code and cause OPTIONAL_IE_INCORRECT	The previous error appears whenever the Binding Request optional query parameters has an incorrect format or value.	NA

Table D-1 (Cont.) Error Code Dictionary for BSF Management

App Error Id	Description	Cause	Action
EC-OBSF-BSF_MGMT-REQVLD-EI-05-02-400-00010-01-02	The POST register request to BSF failed with a 400 status code and cause MANDATORY_IE_MISSING .	The previous error appears whenever a mandatory IE is missing in the Binding Data from the Binding Request. Mandatory IE are the following: • UE Direction – IPv4 Address and/or Ipv6 Prefix – MAC-48 Address • SNSSAI – SST – SD	NA
EC-OBSF-BSF_MGMT-INTRNL-EI-05-04-500-00056-01-02	The DELETE deregister request to BSF failed with a 500 status code and cause INTERNAL_SERVER_ERROR	The previous error appears whenever an internal error occurs on BSF Management Service while trying to deregister.	NA

Table D-2 Error Code Dictionary for Egress Gateway

App Error Code	Error Type	Description	Cause	Action
E001	CONNECTION_TIMEOUT	This error code indicates that egress-gateway is unable to establish the connection with peer NF in the configured connectionTimeout period.	The server is down or it takes too long to respond.	Increase the timeout value or check if the server is up and running
E002	REQUEST_TIMEOUT	This error code indicates that request processing takes more time than the configured request timeout at egress-gateway.	A successful TCP connection was established but no response was received within the expected time frame.	Consider increasing the request timeout setting on the gateway or optimizing the backend services to handle the request faster.

Table D-2 (Cont.) Error Code Dictionary for Egress Gateway

App Error Code	Error Type	Description	Cause	Action
E003	UNKNOWN_HOST_EXCEPTION	This error code indicates that egress-gateway is unable to resolve the peer NF service host name.	The error message indicates that the ingress gateway is unable to resolve the configured backend service hostname. This could be due to several reasons such as incorrect DNS settings, network issues, or misconfigured hostnames.	Ensure that the hostname provided in the configuration file matches the actual hostname of the backend service. If necessary, update the DNS records or configure the gateway to use alternative routing service.
E004	CONNECT_EXCEPTION	This error code indicates that egress-gateway is unable to establish the connection with peer NF service.	Peer/NF Service is refused due to incorrect network configuration, inactive service	Verify Peer/NF service availability, network routing, and ensuring the correct IP address and port are being used
E005	INVALID_HTTP_REQUEST_EXCEPTION	This error code indicates exception occurred because HTTP1.1 is disabled but oc-http-version header has value http1.	enableOutgoingHttp1 flag of Egress Gateway is set to false.	Set enableOutgoingHTTP1 flag in EGW config to true.
E006	CLOSED_CHANNEL_EXCEPTION	This error code indicates that closed channel exception has occurred as incoming TCP connection was abruptly terminated before egress gateway had send back the response.	Unexpected Behaviour within the Network	Capture network traces to identify the root cause of the abrubt connection termination .
E007	SSL_HANDSHAKE_EXCEPTION	This error code indicates the ssl hand shake exception occurred in egress gateway.	Incorrect Certificates used for establishing the connection. Use of incorrect certificates or cipher suites mismatch or TLS Version incompatibility.	Cross Check Certificates used, Cipher suites and TLS Version match between the client and server.

Table D-2 (Cont.) Error Code Dictionary for Egress Gateway

App Error Code	Error Type	Description	Cause	Action
E051	REJECTED_EXECUTION_EXCEPTION	This error code indicates that RejectedExecutionException has occurred at egress-gateway as the incoming no. of requests are more than the queueCapacity configured in applicationThreadPoolConfig.	Value set for applicationThreadPoolConfig in configuration of EGW is low for incoming traffic	Increase the value of applicationThreadPoolConfig in EGW Configuration or reduce the number of requests flowing to EGW for incoming traffic
E052	NOT_FOUND_EXCEPTION	This error code indicates that egress-gateway received request path with an endpoint that is not implemented in the peer NF service.	URI/Path of the request is incorrect or required path is not configured on Peers/NFs side.	Configure the required URI in routesConfig or correct the URI of the request
E054	INTERNAL_ERROR	This error code indicates that some unknown internal error occurred in egress-gateway while processing the request.	NA	NA
E102	LATE_ARRIVAL_EXCEPTION	This error code indicates that late arrival exception occurred at egress-gateway as the request has already expired as part of SbiTimer feature.	Timezone mismatch (or) 12H/24H time format mismatch leading to some time in the past in SBI Timer Header for SBI Timer Feature (or) Header of MaxRspTime might have been configured with the wrong value (or) the calculated request timeout value based on SBI Timer Headers is less than the configured requiredTime value at route level	Make sure the timestamp and max response time attached in the header, are of the correct time with respect to the time zone and not a time in the past. Verify if the requiredTime is accomodating to the calculated timeout value from SBI Timer Header values.
E112	NOTIFICATION_RATE_LIMIT	This error code indicates that requests are being rejected after exceeding the bucketCapacity when notificationRateLimit feature is enabled.	Request Count is higher than the configured bucketCapacity at notificationRateLimit in EGW Configurations	Either increase the bucketCapacity or reduce the number requests

Table D-2 (Cont.) Error Code Dictionary for Egress Gateway

App Error Code	Error Type	Description	Cause	Action
E122	RETRY_AFTER_ERROR	This error code indicates that retry-after feature is enabled and producer fqdn is blacklisted and hence the request cannot be fulfilled.	RetryAfter Feature is enabled, and the blackListPeriod is completed for the peer. But when we access the peer while it is still blacklisted, we see this error.	If not the intended behaviour, disable RetryAfter Feature
E127	GRACEFUL_SHUTDOWN	This error code indicates that the service shutdown is in progress.	During Normal Flow of requests, if the IP changes and DNS refresh occurs	Wait for the IP reset and DNS refresh to complete. After establishing connection to the service, then try sending the request again
E132	VIRTUAL_HOST_RESOLUTION_ERROR	This error code indicates that the DNS resolution of virtual fqdn failed.	The vFQDN provided for the virtual host cannot be resolved by the DNS servers.	Verify that the vFQDN is correctly spelled and formatted (or) ensure that the DNS server is operational (or) confirm that the FQDN exists in the DNS records.
E152	INVALID_OAUTH_TOKEN_REQUEST	This error code indicates the exception occurred because of bad AccessToken request received.	OAuth Token received might be of wrong format/ value.	Check for the correct format/ value on the basis of the configurations at EGW
E153	OAUTH_INTERNAL_ERROR	This error code indicates that egress gateway is unable to send AccessToken request to NRF.	InternalServerError because of error while processing/ sending the request to NRF	NA
E154	OAUTH_TOKEN_RETRIEVAL_FAILURE	This error code indicates error in retrieving token from NRF.	Error while retrieving the token from Response received from NRF	NA
E155	OAUTH_NRF_RESPONSE_FAILURE	This error code indicates response failure from NRF(invalid/bad response) while trying to fetch oauth token.	Error while processing the Response received from NRF	NA

Table D-2 (Cont.) Error Code Dictionary for Egress Gateway

App Error Code	Error Type	Description	Cause	Action
E172	EGRESS_RATE_LIMITING	This error code indicates that requests are being rejected after exceeding the bucketCapacity when egressRateLimiting feature is enabled.	Number of requests are exceeding the bucket size set in the configurations for EGW.	Edit bucket size in EGW configurations, or reduce the rate of request.
E182	EGW_CUSTOM_EXCEPTION	This error code indicates custom exception occurred in some feature at egress gateway because some conditions failed to fulfill at runtime namely SbiRouting, SeppProxyFilter, PeerBlackListHelper, EgressGatewayFilter	NA	Identify the Error from the Response received, and cross verify with the respective documentaiton
E183	RESPONSE_STATUS_EXCEPTION	This error code indicates that ResponseStatusException was created by Spring boot as egress gateway exception handler was not able to handle a exception.	NA	NA
E192	PARTIAL_SHUTDOWN	This error code indicates that requests are being discarded partially at egress-gateway when Control shutdown feature enabled.	Behaviour is observed when ControlledShutdown is enabled	Disable ControlledShutdown
E193	COMPLETE_SHUTDOWN	This error code indicates that requests are being discarded completely at egress-gateway when Control shutdown feature enabled.	Behaviour is observed when ControlledShutdown is enabled	Disable ControlledShutdown
E202	INVALID_ROUTE_EXCEPTION	This error code indicates invalid route exception has occurred as invalidRouteFilter was configured in the routesConfiguration.	Invalid Route Exception is a filter enabled at route level in routesConfig.	If this is unexpected behaviour, check the path if that is the expected path that was supposed to be marked as an invalid route.
E206	IP_TYPE_MISMATCH_EXCEPTION	This error code indicates that there is a mismatch in the configured EgressRoutingMode IP type and the DNS resolved IP type.	The type of IP resolved by DNS is differing from the IP Type configured at the EGW.	Verify if gateway is deployed in dual stack IP setup

Table D-3 Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E001	CONNECTION_TIMEOUT	This error code indicates that ingress-gateway is unable to establish the connection with backend service in the configured connectionTimeout period.	The server is down or it takes too long to respond.	Increase the timeout value or check if the server is up and running
E002	REQUEST_TIMEOUT	This error code indicates that request processing takes more time than the configured request timeout at ingress-gateway.	A successful TCP connection was established but no response was received within the expected time frame.	To resolve this issue, consider increasing the request timeout setting on the ingress gateway or optimizing the backend services to handle the request faster.
E003	UNKNOWN_HOST_EXCEPTION	This error code indicates that ingress-gateway is unable to resolve the configured backend service host name.	The error message indicates that the ingress gateway is unable to resolve the configured backend service hostname. This could be due to several reasons such as incorrect DNS settings, network issues, or misconfigured hostnames.	Check if the FQDN of the backend service is correctly resolved from the ingress gateway's perspective. If necessary, update the DNS records or configure the ingress gateway to use alternative routing servers. Additionally, ensure that the hostname provided in the configuration file matches the actual hostname of the backend service.
E004	CONNECT_EXCEPTION	This error code indicates that ingress-gateway is unable to establish the connection with backend service.	Peer/NF Service is refused due to incorrect network configuration, inactive service	Verify Peer/NF service availability, network routing, and ensuring the correct IP address and port are being used

Table D-3 (Cont.) Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E005	BLACKLIST_IP_EXCEPTION	This error code indicates that BlackList IP exception has occurred while establishing new connection with blacklisted IP at ingress-gateway. IP would be blacklisted if TCP connection to this IP failed for more than 10 times.	Gateway is not able to establish TCP connection for more than 10 times	Verify why the IP is not accepting TCP Conneciton
E006	CLOSED_CHANNEL_EXCEPTION	This error code indicates that closed channel exception has occurred as incoming TCP connection was abruptly terminated before ingress gateway had send back the response.	Unexpected Behaviour within the Network	Capture Network Traces to identify the root cause of why the connection terminated abrubtly
E051	REJECTED_EXECUTION_EXCEPTION	This error code indicates that RejectedExecutionException has occurred at ingress-gateway as the incoming no. of requests are more than the queueCapacity configured in applicationThreadPoolConfig.	Value set for applicationThreadPoolConfig in configuration of IGW is low for incoming traffic	Increase the value of applicationThreadPoolConfig in IGW Configuration or reduce the number of requests flowing to IGW for incoming traffic
E052	NOT_FOUND_EXCEPTION	This error code indicates that ingress-gateway received request path with an endpoint that is not implemented in the backend service.	URI of the Request has not been configured in the routesConfig for IGW.	Configure the required URI in routesConfig or correct the URI of the request
E053	SOCKET_EXCEPTION	This error indicates that SocketException has occurred as ingress-gateway was unable to create TCP connection.	Network connectivity issues, network restrictions, or misconfigured endpoints	Verify if there are any network policies blocking the communication between the ingress gateway and the backend service. Confirm that the endpoint URL provided in the configuration file is correct and reachable from the ingress gateway

Table D-3 (Cont.) Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E054	INTERNAL_ERROR	This error code indicates that some unknown internal error occurred in ingress-gateway while processing the request.	Internal Errors, occur when there's an issue with improper configurations, mismatch in helm charts and versions.	Identify the cause from the error message sent back in the response and refer to the documentation for the specific feature that is being used and re verify all the configurations. Helm Charts and respective versions can also be checked
E102	LATE_ARRIVAL_EXCEPTION	This error code indicates that late arrival exception occurred at ingress-gateway as the request has already expired as part of SbiTimer feature.	Timezone mismatch (or) 12H/24H time format mismatch leading to some time in the past in SBI Timer Header for SBI Timer Feature (or) Header of MaxRspTime might have been configured with the wrong value (or) the calculated request timeout value based on SBI Timer Headers is less than the configured requiredTime value at route level	Make sure the timestamp and max response time attached in the header, are of the correct time with respect to the time zone and not a time in the past. Verify if the requiredTime is accommodating to the calculated timeout value from SBI Timer Header values.
E112	USERAGENT_VALIDATION_FAILURE_EXCEPTION	This error code indicates that validation of user-agent header failed at ingress-gateway.	The NF configured in the user-agent header of the request does not match with the configured NFs in the IGW	Either verify if the request has the correct NF Value configured, or if the intended NF as been added into the list of acceptable NFs at the IGW end.
E122	GRACEFUL_SHUTDOWN	This error code indicates that requests received at ingress-gateway rejected gracefully during the ingress-gateway shutdown.	This indicates that the service/pod is shutting down and responses sent include this Error Response	(Re) Deploy IGW, or prevent shutdown

Table D-3 (Cont.) Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E132	GLOBAL_RATELIMIT	This error code indicates that requests are being rejected after exceeding the burstCapacity when global ratelimit feature enabled.	Number of requests are exceeding the bucket size set in the configurations for IGW, which is calculated on the basis of maxTokenRequest and burstCapacity.	Modify the globalIngressRateLimiting parameter of Gateway configurations to accommodate incoming requests.
E152	RSS_BASED_RATELIMIT	This error code indicates that requests are being rejected after exceeding the burstCapacity when rss ratelimit feature enabled.	When egressrateLimiting ConfigMap is configured with burstCapacity and ratelimiting enabled, this exception is thrown when the requests count exceeds this burstCapacity and it is also based on the MNC and MCC values.	If this is unexpected behaviour, change the values/ attributes in egressrateLimiting ConfigMap.
E162	XFCC_HEADER_VALIDATION_FAILURE	This error code indicates that validation of XFCC header failed at ingress-gateway.	Indicates that the XFCC Header in the request is in the correct format but is not validated as it is the wrong value for the request.	Verify if the right value is updated in the XFCC Header based on the IGW Deployment configuration.
E163	XFCC_HEADER_NOT_PRESENT_OR_EMPTY	This error code indicates that request received at ingress gateway with no XFCC header or empty XFCC header.	XFCC Header is not present	Include the XFCC Header in the Request
E164	XFCC_MATCHCERTCOUNT_GREATER_THAN_CERTS_IN_HEADER	This error code indicates that XFCC header validation failed due to XFCC certificate count miss match in ingress-gateway.	IGW Configuration requires more certs than the number of certs sent in the request	Check the number of certificates in the request sent and attach the certificates matching the configuration set for IGW
E165	XFCC_HEADER_INVALID	This error code indicates that invalid XFCC header received at ingress-gateway.	XFCC Header present in request is not of the right format.	Fix the XFCC Header of the request and send.

Table D-3 (Cont.) Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E171	OAUTH_TOKEN_VALIDATION_FAILURE	This error code indicates that validation of OAuth token failed at ingress-gateway.	Oauth token passed with the request is enclosed with values which are incorrect with respect to the configuration present at the gateway.	Verify and include the Oauth Token with the correct set of values related to the deployed IGW config.
E172	OAUTH_CERT_EXPIRED	This error code indicates that OAuth cert expired received at ingress-gateway.	Indicates that all the attributes are present and in the correct format, but the token has expired with respect to IGW's configuration	Attach an Oauth Token in the Request which hasn't expired
E173	OAUTH_MISMATCH_IN_KID	This error code indicates that OAuth miss match in KID at ingress-gateway.	Incorrect issuer and incorrect KID Value is included in the request.	Check the issuer attribute and KID Value passsed in the request.
E173	OAUTH_MISMATCH_IN_ALGORITHM_FOR_KID	This error code indicates that algorithm used while generating token is not matching with the configured algorithm when the oauthValidationMode is "KID_ONLY"	Algorithm used while generating token is not matching with the configured algorithm.	Correct the algorithm used.
E174	OAUTH_PRODUCER_SCOPE_NOT_PRESENT	This error code indicates that producer scope not present in the OAuth token received at ingress-gateway.	Producer Scope is not present in the token of the request	Check for Producer Scope value in the token used in the request
E175	OAUTH_PRODUCER_SCOPE_MISMATCH	This error code indicates that producer scope present in the OAuth token miss match with producer scope configured in ingress gateway.	Producer Scope sent through the token either has wrong format, has been used incorrectly, or incorrect value is present.	Verify the Producer Scope Attribute of the token sent through the request
E176	OAUTH_MISMATCH_IN_NRF_INSTANCEID	This error code indicates that nrf instance id present in the OAuth token miss match with nrf instance id configured in ingress gateway.	Wrong issuer attribute is passed along with the access token.	Check the issue attribute attached along with the request

Table D-3 (Cont.) Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E176	OAUTH_MISMATCH_IN_ALGORITHM	This error code indicates that algorithm used while generating token is not matching with the configured algorithm when the oauthValidationMode is "KID_PREFERRED" or "INSTANCEID_ONLY"	Algorithm used while generating token is not matching with the configured algorithm.	Correct the algorithm used.
E177	OAUTH_PRODUCER_PLMNID_MISMATCH	This error code indicates that the received OAuth token miss match with producer plmn configured in ingress gateway.	Configured PLMN ID in IGW, is not matching with the PLMN ID received through the OAuth Token	Correct the PLMN ID in the configuration for IGW or correct the ID in the OAuth Token itself.
E178	OAUTH_AUDIENCE_NOT_PRESENT_OR_INVALID	This error code indicates that the received OAuth token does not contain an audiance or invalid audiance at ingress gateway.	Token is passed with Audience parameter containing only correct nfType but in a different Case. An Audience Parameter with missing or wrong values for NfType and NfInstanceId can also raise this error	Verify and include the correct NfType or/and NfInstanceID in the request.
E179	OAUTH_TOKEN_INVALID	This error code indicates that invalid OAuth token received at ingress-gateway.	Indicates that the OAuth Token received at IGW is not valid, i.e., not in the correct format.	Verify if the OAuth Token is in the right format and configured with the right set of values with respect to the configuration at the gateway.
E180	OAUTH_TOKEN_ABSENCE	This error code indicates that request received at ingress gateway with no OAuth token or empty OAuth token	OAuth Token is missing in the request	Include the OAuth Token in the request
E182	IGW_OVERLOAD_CONTROL_EXCEPTION	This error code indicates that overload control exception occurred at ingress-gateway.	Occurs when the feature OverloadControl is enabled and configured at the requests/second being sent.	Modify the Configuration for acceptable requests/second.

Table D-3 (Cont.) Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E183	RESPONSE_STATUS_EXCEPTION	This error code indicates that ResponseStatusException was created by Spring boot as ingress gateway exception handler was not able to handle a exception.	NA	NA
E191	CCA_HEADER_VALIDATION_FAILURE	This error code indicates that validation of CCA header failed at ingress-gateway.	CCA Header sent through the request, failed while validation.	Include the correct value for CCA Header in the request
E192	PARTIAL_SHUTDOWN	This error code indicates that requests are being discarded partially at ingress-gateway when Control shutdown feature enabled.	Behaviour is observed when ControlledShutdown is enabled	Disable ControlledShutdown
E193	COMPLETE_SHUTDOWN	This error code indicates that requests are being discarded completely at ingress-gateway when Control shutdown feature enabled.	Behaviour is observed when ControlledShutdown is enabled	Disable ControlledShutdown
E200	IGW_TRAFFIC_REJECTION	This error code indicates all requests will rejected at ingress-gateway when traffic reject feature enabled.	trafficrejectmode has been enabled through REST configuration for IGW	Disbale trafficrejectmode through REST configuration for IGW
E201	IGW_OVERLOAD_CONTROL_PERCENTAGE_DISCARD	This error code indicates that requests are being rejected when load level matches with configured percentage in discard policy mapping of overload control feature.	The number of requests have reached the configured percentage for OverloadControl. When this value has reached, the respective Error Code is displayed	Change the percentage value to accommodate more requests and not to display the error code.
E202	IGW_OVERLOAD_CONTROL_PRIORITY_DISCARD	This error code indicates that requests with sbi-priority header with value greater than configured number of discarded load level matches in discard policy mapping of overload control feature.	The number of requests have reached the configured priority for OverloadControl. When this value has reached, the respective Error Code is displayed	Change the priority value to accommodate more requests and not to display the error code.

Table D-3 (Cont.) Error Code Dictionary for Ingress Gateway

App Error Code	Error Type	Description	Cause	Action
E211	IGW_ROUTE_RATELIMITER_PRIORITY_DISCARD	This error code indicates that requests are being rejected when priority level matches with configured priority in discard policy mapping of route level ratelimiting feature.	Request is rejected because priority level set in the SBI header is greater than the configured priority in the route level rate limiting, discard policy mapping.	Increase the Priority in discard policy mapping for route level rate limiting, so requests with higher priority are accepted.
E220	IGW_PLMN_EGRESS_RATELIMIT	This error code indicates that requests are being rejected after exceeding the burstCapacity when plmn egress ratelimit feature enabled	When egressrateLimiting ConfigMap is configured with burstCapacity and ratelimiting enabled, this exception is thrown when the requests count exceeds this burstCapacity and it is also based on the MNC and MCC values.	If this is unexpected behaviour, change the values/ attributes in egressrateLimiting ConfigMap.
E221	INVALID_ROUTE_EXCEPTION	This error code indicates invalid route exception has occurred as invalidRouteFilter was configured in the routesConfiguration.	Invalid Route Exception is a filter enabled at route level in routesConfig.	If this is unexpected behaviour, check the path if that is the expected path that was supposed to be marked as an invalid route.
E223	OAUTH_ALGORITHM_INVALID	This error code indicates that the algorithm used while generating the token is not a valid algorithm.	Algorithm used while generating token is not a valid algorithm.	Provide the valid algorithm while generating the token.

Table D-4 Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
E001	This is error code indicates that gateway is unable	The server is down or it takes too long to respond.	Increase the timeout value or check if the server is up and running

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
	etoestablishtheconnectionwithpeerNFintheconfigu	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
	redconnection_timeoutperiod.	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NCMGMT-E001	$NF_CONGESTION erviceUnavailableerrorresponse	Cannot send NRF request since all NRFs are down

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NfType-EGW-E002	Timeout for discovery to NRF client	Request Timeout at EGW	Request Timeout

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NC_MGMT-E002	NO_AVAILABLE_NRF when error when no NRF are available for service	No NRFs available for service

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NC_MGMT-E007	UUNKNOWN_HOST_EXCEPTION ninstallorscalegressgetaway	UnknownHostException when communicating with NRF

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NCMGMT-E512	RSYSTEM_FAILURE equesticannotableetocompleteareqiestitoNRF	Invalid patch operation

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NC_MGMT-E101	Send a discovery request with header OC-Force-Rediscovery	MANDATORY_QUERY_PARAM_INCORRECT	Invalid custom discovery header value for OC-Force-Rediscovery

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
	verywithavaluedifferentthanOor1.	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NC_MGMT-E102	Send a discovery Request with header OC-Retention-Per	MANDATORY_QUERY_PARAM_INCORRECT	Invalid custom discovery header value for OC-Retention-Period

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
	iodwithafoobarasvalue.	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NC_MGMT-E109	Send a discovery request with missed parameter value	MANDATORY_QUERY_PARAM_INCORRECT	Missing name or value of a discovery parameter

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NCMGMT-E110	When sending a discovery request with missed parameter value	MANDATORY_QUERY_PARAM_INCORRECT	One or more discovery parameters are not valid

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
	ueandusing'&		
NCMGMT-E202	Whenthenotificationurlcouldbenull	MANDATORY_IE_MISSING	Missing parameter notificationUri in subscription request

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NCMGMT-E202	RMANDATORY_IE_MISSING equestionNrfRouteListSubscriptionwithemptyURI	Missing parameter notificationUri in subscription request

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NCMGMT-E203	MANDATORY_IE_INCORRECT henthenotificationUricouldbeinvalid	Invalid notificationUri for subscription request

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NCMGMT-E203	RMANDATORY_IE_INCORRECT equestionNrfRouteListSubscriptionwithwrongURI	Invalid notificationUri for subscription request

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NC_MGMT-E209	POST request to /notifications/nrfRouteList "with an	MISSING_PARAMETER	The entire request body is missing

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
	empty body	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NC_MGMT-E301	MISSING_PARAMETER when missed or not valid NFInstance profile	Missing parameter 'nfInstanceID' (uuid)

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NC_MGMT-E302	PUT request to "/nf-instances/{uuid}" with an invalid	MISSING_PARAMETER	Missing parameter 'nfProfile'

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
	ue for the profile in the request body	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NC_MGMT-E302	PMISSING_PARAMETER U - request to /nf-instances/{uuid}" with empty body	Missing parameter 'nfProfile'

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NCMGMT-E309	RMANDATORY_IE_INCORRECT egistrationwithoutNFinstanceIDwithinvalidservi	Semantic validation failed for received NfProfile

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
		cestatus	
NC_MGMT-E033		MANDATORY_IE_INCORRECT	Invalid attributes in request body
		hembindingResultcontainserror	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NC_MGMT-E033	When Request goes with an empty body	INVALID_REQUEST_BODY	Invalid attributes in request body

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NC_MGMT-E033	PINVALID_REQUEST_BODY U+request to "/nf-instances/{uuid}" with an invalid	Invalid attributes in request body

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
	value		
NC_MGMT-E402	invalid null SubscriptionId.	MISSING_PARAMETER	Missing parameter 'subscriptionID'
NC_MGMT-E403	investigating		

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
NC_MGMT-E411	FAILED_CFG_ITEM_CREATION	Failed config item creation for subscriptionData	

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	DCause escription	Action
NC_MGMT-E502	PINVALID_PROFILE OS+request to "/nnrf-client/v1/notify" with an empt	Invalid attributes in notified NfProfile

Table D-4 (Cont.) Error Code Dictionary for NRF Client

App Error Code	Description	Cause	Action
	body		
NC_MGMT-E510	invalid config item creation for profile.	FAILED_CFG_ITEM_CREATION	Failed config item creation for profile from notificationData