Oracle® Communications

Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide

Release 25.1.202
G33127-03
October 2025

Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide, Release 25.1.202

G33127-03

Contents

3 Customizing SEPP

Preface

Documentation Accessibility

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

Access to Oracle Support

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

Diversity and Inclusion

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

Conventions

The following text conventions are used in this document:

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

My Oracle Support

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

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

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

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

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

Acronyms

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

Table Acronyms and Terminologies

Acronym	Description
Cat-0	Category 0 SBI Message Schema Validation Feature
Cat-1	Category 1 Service API Validation Feature
Cat-2	Category 2 Network ID Validation Feature
Cat-3	Category 3 Previous Location Check/ Category 3 Time location check
CNC Console	Oracle Communications Cloud Native Configuration Console
CRD	Custom Resource Definition
CNE	Oracle Communications Cloud Native Environment
cSEPP/C-SEPP	Consumer Security Edge Protection Proxy
DB	Database
DNS	Domain Name System
DRL	Drools Rule Language
EGW	Egress Gateway
FQDN	Fully Qualified Domain Name
GSMA	Groupe Speciale Mobile Association (GSMA). Represents the interests of mobile operators and the broader mobile industry worldwide.
Hosted SEPP	Hosted SEPP functionality provides selective routing in Roaming Hub Mode
IGW	Ingress Gateway
IPX	Internetwork Packet Exchange
K8s	Kubernetes
Local PLMN	PLMN managed by Local SEPP
Local SEPP	SEPP in Local PLMN
MNO	Mobile Network Operator
NDB	Network Database
NF	Network Function
Network Function	A functional building block within a network infrastructure, which has well defined external interfaces and well defined functional behavior. In practical terms, a network function is often a network node or physical appliance.
NF Consumer	A generic way to refer to an NF which consumes services provided by another NF. Example: An AMF acts as a Consumer NF that consumes AMPolicy services provided by the PCF.
NF Instance	A specific instance of a network function type.
NF Producer or NF Provider	A generic way to refer to an NF which provides services that can be consumed by another NF. Example: A PCF acts as a Producer NF that provides AMPolicy Services to the AMF.
NRF	Oracle Communications Cloud Native Core, Network Repository Function
OHC	Oracle Help Center
OSDC	Oracle Software Delivery Cloud
PDB	PodDisruptionBudget

Table (Cont.) Acronyms and Terminologies

Acronym	Description
PLMN	Public Land Mobile Network
pSEPP/P-SEPP	Producer Security Edge Protection Proxy
Remote PLMN	PLMN managed by Remote SEPP
Remote SEPP	SEPP in Remote PLMN
Remote SEPP Set	Set of Remote SEPPs to allow alternate routing across Remote SEPPs
REST API	Representational State Transfer Application Programming Interface
Roaming Hub	Roaming Hub is the deployment mode of SEPP. Roaming Hub is used as an intermediate proxy. Each SEPP connects to the Roaming Hub which further connect to another SEPP. All the Remote SEPPs can communicate with each other through roaming hub.
Scaling	Ability to dynamically extend or reduce resources granted to the Virtual Network Function (VNF) as needed. This includes scaling out and in or scaling up and down.
SCM	Security Coutermeasure
SEPP	Oracle Communications Cloud Native Core, Security Edge Protection Proxy
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SVC	Service
TLS	Transport Layer Security
TH	Topology Hiding
TUH	Topology Unhiding
TPS	Transactions Per Second
UE	User Equipment
UDR	Oracle Communications Cloud Native Core, Unified Data Repository

What's New in This Guide

This section introduces the documentation updates for Release 25.1.2xx.

Release 25.1.202- G33127-03, October 2025

General Updates:

- Updated the release number to 25.1.202 in the entire document.
- Updated the SEPP images in the Pushing the SEPP Images to Customer Docker Registry, Pushing the Roaming Hub or Hosted SEPP Images to Customer Docker Registry, and Pushing the SEPP Images to OCI Docker Registry sections to mention the compatible docker image versions for various microservices.
- Updated the following sections to provide information about Oracle's error correction policy and open source support policies:
  - Oracle Error Correction Policy
  - Oracle Open Source Support Policies

Installation Updates

- Added the following parameters in the perf_info section:
  - `capacityConfig.overall`
  - `capacityConfig.serviceLevel`
  - `capacityConfig.default`

Upgrade, Rollback, and Uninstall Updates:

- Updated the supported upgrade paths in the Upgrading SEPP section.
- Updated the supported rollback paths in the Rolling Back SEPP section.

Release 25.1.201- G33127-02, August 2025

General Updates:

- Updated the release number to 25.1.201 in the entire document.
- Updated the SEPP images in the Pushing the SEPP Images to Customer Docker Registry, Pushing the Roaming Hub or Hosted SEPP Images to Customer Docker Registry, and Pushing the SEPP Images to OCI Docker Registry sections to mention the compatible docker image versions for various microservices.
- Updated the following sections to provide information about Oracle's error correction policy and open source support policies:
  - Oracle Error Correction Policy
  - Oracle Open Source Support Policies

Upgrade, Rollback, and Uninstall Updates:

- Updated the supported upgrade paths in the Upgrading SEPP section.
- Updated the supported rollback paths in the Rolling Back SEPP section.

Release 25.1.200- G33127-01, July 2025

General Updates:

- Updated the release number to 25.1.200 in the entire document.
- Updated the SEPP images in the Pushing the SEPP Images to Customer Docker Registry, Pushing the Roaming Hub or Hosted SEPP Images to Customer Docker Registry, and Pushing the SEPP Images to OCI Docker Registry sections to mention the compatible docker image versions for various microservices.
- Updated the following sections to provide information about Oracle's error correction policy and open source support policies:
  - Oracle Error Correction Policy
  - Oracle Open Source Support Policies
- Updated the Software Requirements section.

Installation Updates:

- Added the following parameters in the n32-ingress-gateway and plmn-ingress-gateway sections for configuring the LCI and OCI Headers feature:
  - `global.lciHeaderConfig.enabled`
  - `global.lciHeaderConfig.loadThreshold`
  - `global.lciHeaderConfig.localLciHeaderValidity`
  - `global.ociHeaderConfig.enabled`
  - `global.ociHeaderConfig.validityPeriod`
  - `global.ociHeaderConfig.overloadConfigRange.minor`
  - `global.ociHeaderConfig.overloadConfigRange.major`
  - `global.ociHeaderConfig.overloadConfigRange.critical`
  - `global.ociHeaderConfig.reductionMetrics.minor`
  - `global.ociHeaderConfig.reductionMetrics.major`
  - `global.ociHeaderConfig.reductionMetrics.critical`
  - `global.nfInstanceId`
  - `global.nfType`
  - `global.nfFqdn`
  - `global.svcToSvcInstanceIdMapping.svcName`
  - `global.svcToSvcInstanceIdMapping.serviceInstanceId`
  - `global.perfInfoConfig.pollingInterval`
  - `global.perfInfoConfig.serviceName`
  - `global.perfInfoConfig.host`
  - `global.perfInfoConfig.port`
  - `global.perfInfoConfig.perfInfoRequestMap`
  - `tlsVersionSupportForKubeApiServer.enabled`
  - `tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`
  - `tlsVersionSupportForKubeApiServer.cipherSuites`
  - `tlsVersionSupportForKubeApiServer.featureSecrets`
  - `overloadControlLocalDiscardEnabled`

- Added the following parameters in the n32-egress-gateway and plmn-egress-gateway sections for configuring the LCI and OCI Headers feature:
  - `dnsSrv.backoffDelay`
  - `dnsSrv.fqdnSchemesForProbing`
  - `tlsVersionSupportForKubeApiServer.enabled`
  - `tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`
  - `tlsVersionSupportForKubeApiServer.cipherSuites`
  - `tlsVersionSupportForKubeApiServer.featureSecrets`
- Added the `traffic.sidecar.istio.io/excludeInboundPorts: "8081"` annotations for the `db-monitor-svc.podAnnotations` cnDBTier service in the Service Mesh Sidecar section.
- Updated the default value of `overloadManager.enabled` parameter to false in the perf_info section.
- Added the `payloadSizeLimit` parameter in the cn32f-svc and pn32f-svc sections to increase the maximum pay load size.
- Added the `egwPeerMonitoringThreshold` parameter in the Global Parameters section.
- Added the note to the `jettyIdleTimeout` parameter in the Timer Parameters section.
- Updated the default value of `coherence-svc.log.root` and `coherence-svc.log.sepp` parameters to ERROR in the coherence section.
- Removed the step for false Helm message observed during SEPP uninstall from the Uninstalling SEPP Using Helm.

Upgrade, Rollback, and Uninstall Updates:

- Updated the supported upgrade paths in the Upgrading SEPP section.
- Updated the supported rollback paths in the Rolling Back SEPP section.

1 Introduction

This guide describes how to install or upgrade Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) in a cloud native environment (OCCNE), Oracle Cloud Infrastructure (OCI), and general Kubernetes environment. It also includes information on performing fault recovery for SEPP.

Note

- This guide covers the installation instructions when Podman is the container platform with Helm as the Packaging Manager. For any other container platform, the operator must use the commands based on their deployed container runtime environment.
- `kubectl` commands can vary based on the platform deployment. Replace `kubectl` with Kubernetes environment-specific command line tool to configure Kubernetes resources through kube-api server. The instructions provided in this document are as per the CNE version of kube-api server.

Caution

User, computer and applications, and character encoding settings may cause an issue when copy-pasting commands or any content from PDF. PDF reader version also affects the copy-pasting functionality. It is recommended to verify the pasted content especially when the hyphens or any special characters are part of the copied content.

1.1 Overview

The Security Edge Protection Proxy (SEPP) is a critical network function in the 5G network designed to secure communication between different 5G network elements, particularly between the 5G core and external networks, such as in roaming scenarios. It is the key component of 5G Service Based Architecture (SBA). SEPP acts as a security gateway, enforcing security policies, performing traffic filtering, encryption, and ensuring that only authorized network functions can exchange sensitive information. It ensures the confidentiality, integrity, and availability of communication, mitigating threats like unauthorized access and data breaches.

SEPP supports the following functions:

- It provide an HTTP2 based RESTful interface and APIs to provision other Network Functions (NFs) data.
- Provides TLS protection for traffic between 5G networks, particularly for inter-PLMN (Public Land Mobile Network) communications.
- Acts as a proxy to ensure secure interactions between different Network Functions (NFs) across operators.

- Supports logging, monitoring, and alerting of security-related events.
- Facilitates secure roaming and inter-network communication by securing the edge.

SEPP:

- leverages a common Oracle Communications Cloud Native Framework.
- uses MySQL NDB Cluster as the backend database in the Data Tier.
- registers with NRF in the 5G network, so the other NFs in the network can discover SEPP through NRF.
- has tiered architecture providing separation between the connectivity, business logic and data layers.

> **Note**
>
> The performance and capacity of the SEPP system may vary based on the call model, Feature/Interface configuration, and underlying platform and hardware environment including but not limited to, the size of the json payload and traffic model.

For more information about the SEPP architecture, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.

1.2 References

Refer to the following documents while deploying :

- *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, cnDBTier User Guide*
- *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*
- *Oracle Communications Cloud Native Core, Data Collector User Guide*
- *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*
- *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide*
- *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide*
- *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Network Impact Report*
- *Oracle Communications Cloud Native Configuration Console User Guide*
- *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Automated Test Suite User Guide*
- *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*

- *Oracle Communications Cloud Native Core, Certificate Management User Guide*
- *Oracle Communications Cloud Native Core, OCI Deployment Guide*
- *Oracle Communications Cloud Native Core, OCI Adaptor User Guide*
- *Oracle Communications Network Analytics Data Director Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core Release Notes*
- *Oracle Communications Cloud Native Core Licensing Information User Guide*
- *Oracle Communications Cloud Native Core Solution Upgrade Guide*
- *Oracle Communications Cloud Native Core Security Guide*

1.3 Supported Deployment Models

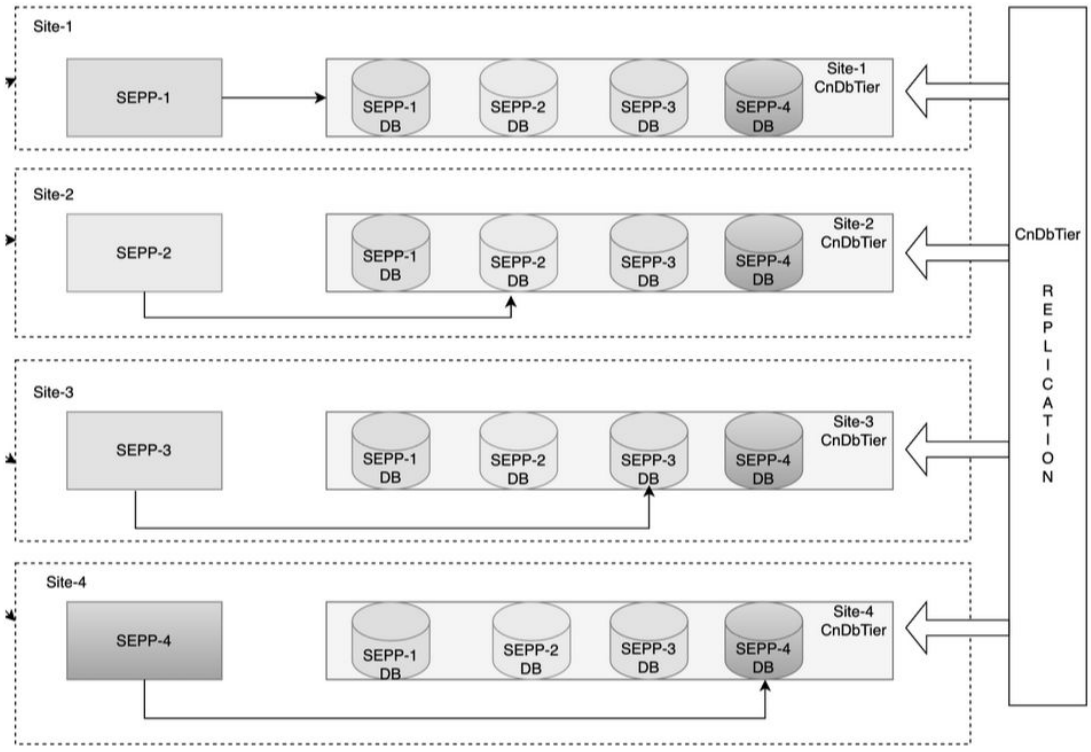
The following deployment models are supported by SEPP:

- Single Cluster, Single Instance (Single SEPP instance on dedicated cnDBTier instance)
- Single Cluster, Multiple Instances (Multiple SEPP instances on shared cnDBTier instance)

1.3.1 Single Cluster, Single Instance (Single SEPP Instance on Dedicated cnDBTier Instance)

This deployment model has dedicated cnDBTier for each SEPP in a cluster.

Figure 1-1 Single Cluster, Single Instance (Single SEPP Instance on Dedicated cnDBTier Instance)



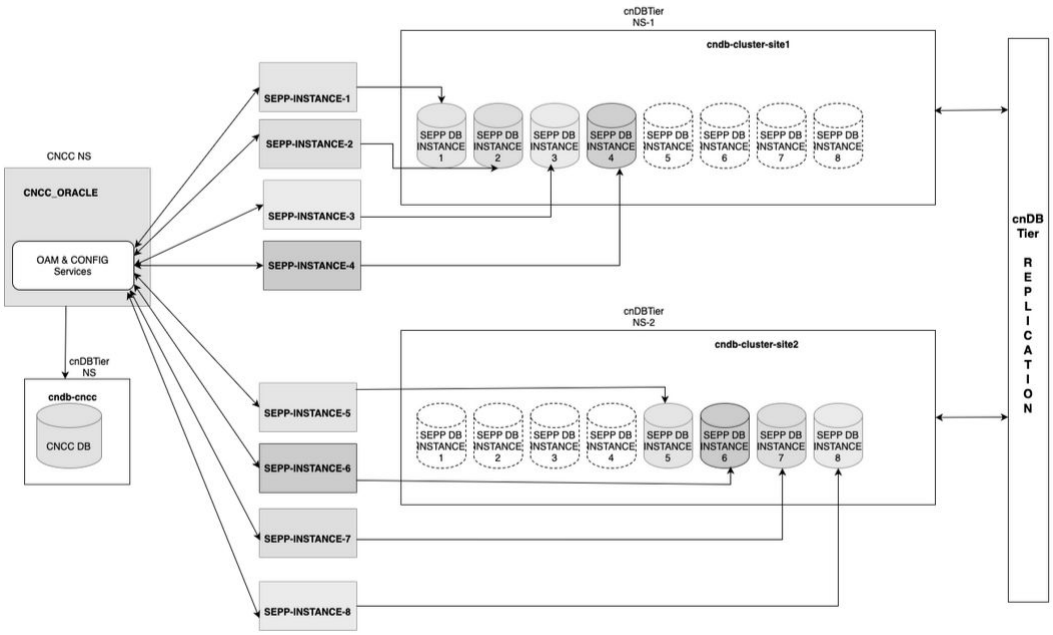
The deployment model has the following characteristics:

- Dedicated SEPP and cnDBTier. Only single instance of NF is supported.
- CNC Console shares the cnDBTier with NF.
- Any failure in cnDBTier impacts only that SEPP.
- SEPP and cnDBTier upgrade and rollback are seamless and easy to maintain.

1.3.2 Single Cluster, Multiple Instances (Multiple SEPP Instances on Shared cnDBTier Instance)

This deployment model allows multiple SEPP instances to be deployed on a shared cnDBTier instance.

Figure 1-2 Single Cluster, Multiple Instance (multiple SEPP instances on shared cnDBTier instance)



The deployment model has the following characteristics:

- This approach optimizes resource utilization and can lead to considerable resource efficiency.
- Data access for each SEPP instance is restricted through the use of distinct logins and credentials during deployment.
- 1+1 GR redundancy only is supported with not more than 4 SEPP instances in one cluster.
- This deployment model can only be used for SEPP instances deployed on the same CNE cluster.

1.4 Oracle Error Correction Policy

The table below outlines the key details for the current and past releases, their General Availability (GA) dates, and the end dates for the Error Correction Grace Period.

Table 1-1 Oracle Error Correction Policy

Cloud Native Core Release Number	General Availability (GA) Date	Error Correction Grace Period End Date
3.25.1.200.0	July 2025	July 2026
3.25.1.100.0	April 2025	April 2026
3.24.3	October 2024	October 2025
3.24.2	July 2024	July 2025

Note

- For the latest patch releases, see their corresponding *Oracle Communications Cloud Native Core Release Notes.*
- For a release, Sev1 and Critical Patch Update (CPU) patches are supported for 12 months. For more information, see Oracle Communications Cloud Native Core and Network Analytics Error Correction Policy.

1.5 Oracle Open Source Support Policies

Oracle Communications Cloud Native Core uses open source technology governed by the Oracle Open Source Support Policies. For more information, see Oracle Open Source Support Policies.

2
Installing SEPP

This chapter provides information about installing SEPP using Command Line Interface (CLI) procedures. CLI provides an interface to run various commands required for SEPP deployment processes.

The SEPP installation is supported over the following platforms:

- Oracle Communications Cloud Native Core, Cloud Native Environment (CNE). For more information about CNE, see *Oracle Communications Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- Oracle Cloud Infrastructure (OCI). For more information, see *Oracle Communications Cloud Native Core, OCI Deployment Guide*.
- General Kubernetes environment.

> **Note**
>
> SEPP supports fresh installation, and it can also be upgraded. For more information on how to upgrade SEPP, see Upgrading SEPP section.

The user can install either SEPP or Roaming Hub/Hosted SEPP. The installation procedure comprises of prerequisites, predeployment configuration, installation, and postinstallation tasks. You must perform the installation tasks in the same sequence as outlined in the following table:

Table 2-1 SEPP or Roaming Hub/Hosted SEPP Installation Sequence

Task	Sub tasks	Applicable for SEPP Installation (CNE Deployment)	Applicable for Roaming Hub or Hosted SEPP Installation (CNE Deployment)	Applicable for OCI Deployment
Prerequisites: This section describes how to set up the installation environment.	Prerequisites	Yes	Yes	Yes
-	Software Requirements	Yes	Yes	Yes
-	Environment Setup Requirements	Yes	Yes	Yes
-	Resource Requirements	SEPP Resource Requirements	Roaming Hub or Hosted SEPP Resource Requirements	SEPP Resource Requirements

Table 2-1 (Cont.) SEPP or Roaming Hub/Hosted SEPP Installation Sequence

Task	Sub tasks	Applicable for SEPP Installation (CNE Deployment)	Applicable for Roaming Hub or Hosted SEPP Installation (CNE Deployment)	Applicable for OCI Deployment
Preinstallation Tasks: This section describes how to create namespace and database and configure Kubernetes secrets.	Preinstallation Tasks	Yes	Yes	Yes
-	Downloading SEPP package	Yes	Yes	Yes
-	Pushing the SEPP Images to Customer Docker Registry	Yes	No	No
-	Pushing the Roaming Hub or Hosted SEPP Images to Customer Docker Registry	No	Yes	Yes
-	Pushing the SEPP Images to OCI Docker Registry	No	No	Yes
-	Verifying and Creating SEPP Namespace	Yes	Yes	Yes
-	Configuring Database, Creating Users, and Granting Permissions	Yes	Yes	Yes
-	Configuring Kubernetes Secrets for Accessing SEPP Database	Yes	Yes	Yes
-	Configuring Kubernetes Secret for Enabling HTTPS/ HTTP over TLS	Yes	Yes	Yes
Installation Tasks: This section describes how to download the SEPP package, install SEPP, and verify the installation.	Installation Tasks			

Table 2-1 (Cont.) SEPP or Roaming Hub/Hosted SEPP Installation Sequence

Task	Sub tasks	Applicable for SEPP Installation (CNE Deployment)	Applicable for Roaming Hub or Hosted SEPP Installation (CNE Deployment)	Applicable for OCI Deployment
Installing SEPP / Roaming Hub	Installing SEPP/ Roaming Hub/ Hosted SEPP	Installing SEPP	Installing Roaming Hub or Hosted SEPP	Installing SEPP
Verifying SEPP Installation	Verifying SEPP Installation	Yes	Yes	Yes
PodDisruptionBudget Kubernetes Resource	PodDisruptionBudget Kubernetes Resource	Yes	Yes	Yes
Customizing SEPP	Customizing SEPP	Yes	Yes	Yes
Upgrading SEPP	Upgrading SEPP	Yes	Yes	Yes
Rollback SEPP deployment	Rollback SEPP deployment	Yes	Yes	Yes
Uninstalling SEPP	Uninstalling SEPP	Yes	Yes	Yes
Fault Recovery	Fault Recovery	Yes	Yes	Yes

2.1 Prerequisites

Before installing and configuring SEPP, ensure that the following prerequisites are met.

2.1.1 Software Requirements

This section lists the software that must be installed before installing SEPP:

> **Note**
>
> Table 2-2 and Table 2-3 offer a comprehensive list of software necessary for the proper functioning of BSF during deployment. However, these tables are indicative, and the software used can vary based on the customer's specific requirements and solution.
>
> The **Software Requirement** column in Table 2-2 and Table 2-3 indicates one of the following:
>
> - Mandatory: Absolutely essential; the software cannot function without it.
> - Recommended: Suggested for optimal performance or best practices but not strictly necessary.
> - Conditional: Required only under specific conditions or configurations.
> - Optional: Not essential; can be included based on specific use cases or preferences.

Table 2-2 Preinstalled Software Versions

Software	25.1.2xx	25.1.1xx	24.3.x	Software Requirement	Usage Description
Kubernetes	1.32.0	1.31.1	1.30.0	Mandatory	Kubernetes orchestrates scalable, automated NF deployments for high availability and efficient resource utilization. **Impact**: Preinstallation is required. Without orchestration capabilities, deploying and managing network functions (NFs) can become complex, leading to inefficient resource utilization and potential downtime.
Helm	3.17.1	3.16.2	3.15.2	Mandatory	Helm, a package manager, simplifies deploying and managing NFs on Kubernetes with reusable, versioned charts for easy automation and scaling. **Impact**: Preinstallation is required. Without this capability, management of NF versions and configurations becomes time-consuming and error-prone, impacting deployment consistency.
Podman	4.9.4	4.9.4	4.6.1	Recommended	Podman is a part of Oracle Linux. It manages and runs containerized NFs without requiring a daemon, offering flexibility and compatibility with Kubernetes. **Impact**: Preinstallation is required. Without efficient container management, the development and deployment of NFs could become cumbersome, impacting agility.

To check the current CNE, Helm, Kubernetes, or Podman version installed, run the following commands:

```
echo $OCCNE_VERSION
```

```
helm version
```

```
kubectl version
```

```
podman version
```

> **Note**
>
> This guide covers the installation instructions for SEPP when Podman is the container platform with Helm as the Packaging Manager. For non-CNE, the operator can use commands based on their deployed Container Runtime Environment, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

> **Note**
>
> Podman version or docker version based on the container engine installed.

If you are deploying SEPP in a cloud native environment, these following additional software are to be installed before installing SEPP.

Table 2-3 Additional Software Versions

Software	25.1.2xx	25.1.1xx	24.3.x	Software Requirement	Usage Description
AlertManager	0.28.0	0.27.0	0.27.0	Recommended	Alertmanager is a component that works in conjunction with Prometheus to manage and dispatch alerts. It handles the routing and notification of alerts to various receivers. **Impact**: Not implementing alerting mechanisms can lead to delayed responses to critical issues, potentially resulting in service outages or degraded performance.
Calico	3.29.1	3.28.1	3.27.3	Recommended	Calico provides networking and security for NFs in Kubernetes, ensuring scalable, policy-driven connectivity. **Impact**: Calico is a popular Container Network Interface (CNI) and CNI is mandatory for the functioning of 5G NFs. Without a CNI plugin, the network could witness security vulnerabilities and inadequate traffic management, impacting the reliability of NF communications.
cinder-csi-plugin	1.32.0	1.31.1	1.30.0	Mandatory	Cinder CSI (Container Storage Interface) plugin is used for provisioning and managing block storage in Kubernetes. It is often used in OpenStack environments to provide persistent storage for containerized applications **Impact**: Without the CSI plugin, provisioning block storage for NFs would be manual and inefficient, complicating storage management.

Table 2-3 (Cont.) Additional Software Versions

Software	25.1.2xx	25.1.1xx	24.3.x	Software Requirement	Usage Description
containerd	1.7.24	1.7.22	1.7.16	Recommended	Containerd manages container lifecycles to run NFs efficiently in Kubernetes. **Impact**: A lack of a reliable container runtime could lead to performance issues and instability in NF operations.
CoreDNS	1.11.13	1.11.1	1.11.1	Recommended	CoreDNS is the DNS server in Kubernetes, which provides DNS resolution services within the cluster. **Impact**: DNS is an essential part of deployment. Without proper service discovery, NFs would struggle to communicate with each other, leading to connectivity issues and operational failures.
Fluentd	1.17.1	1.17.1	1.16.2	Recommended	Fluentd is an open source data collector that streamlines data collection and consumption, ensuring improved data utilization and comprehension. **Impact**: Not utilizing centralized logging can hinder the ability to track NF activity and troubleshoot issues effectively, complicating maintenance and support.
Grafana	9.5.3	9.5.3	9.5.3	Recommended	Grafana is a popular open source platform for monitoring and observability. It provides a user-friendly interface for creating and viewing dashboards based on various data sources. **Impact**: Without visualization tools, interpreting complex metrics and gaining insights into NF performance would be cumbersome, affecting effective management.
Jaeger	1.65.0	1.60.0	1.60.0	Recommended	Jaeger provides distributed tracing for 5G NFs, enabling performance monitoring and troubleshooting across microservices. **Impact**: Not utilizing distributed tracing may hinder the ability to diagnose performance bottlenecks, making it challenging to optimize NF interactions and user experience.
Kyverno	1.13.4	1.12.5	1.12.5	Recommended	Kyverno is a Kubernetes policy engine that allows to manage and enforce policies for resource configurations within a Kubernetes cluster. **Impact**: Without the policy enforcement, there could be misconfigurations, resulting in security risks and instability in NF operations, affecting reliability.

Table 2-3 (Cont.) Additional Software Versions

Software	25.1.2xx	25.1.1xx	24.3.x	Software Requirement	Usage Description
MetalLB	0.14.4	0.14.4	0.14.4	Recommended	MetalLB is used as a load balancing solution in CNE, which is mandatory for the solution to work. MetalLB provides load balancing and external IP management for 5G NFs in Kubernetes environments. **Impact**: Without load balancing, traffic distribution among NFs may be inefficient, leading to potential bottlenecks and service degradation.
metrics-server	0.7.2	0.7.2	0.7.1	Recommended	Metrics server is used in Kubernetes for collecting resource usage data from pods and nodes. **Impact**: Without resource metrics, auto-scaling and resource optimization would be limited, potentially leading to resource contention or underutilization.
Multus	4.1.3	3.8.0	3.8.0	Recommended	Multus enables multiple network interfaces in Kubernetes pods, allowing custom configurations and isolated paths for advanced use cases such as NF deployments, ultimately supporting traffic segregation. **Impact**: Without this capability, connecting NFs to multiple networks could be limited, impacting network performance and isolation.
OpenSearch	2.15.0	2.11.0	2.11.0	Recommended	OpenSearch provides scalable search and analytics for 5G NFs, enabling efficient data exploration and visualization. **Impact**: Without a robust analytics solution, there would be difficulties in identifying performance issues and optimizing NF operations, affecting overall service quality.
OpenSearch Dashboard	2.15.0	2.11.0	2.11.0	Recommended	OpenSearch dashboard visualizes and analyzes data for 5G NFs, offering interactive insights and custom reporting. **Impact**: Without visualization capabilities, understanding NF performance metrics and trends would be difficult, limiting informed decision making.

Table 2-3 (Cont.) Additional Software Versions

Software	25.1.2xx	25.1.1xx	24.3.x	Software Requirement	Usage Description
Prometheus	3.2.0	2.52.0	2.52.0	Mandatory	Prometheus is a popular open source monitoring and alerting toolkit. It collects and stores metrics from various sources and allows for alerting and querying. **Impact**: Not employing this monitoring solution could result in a lack of visibility into NF performance, making it difficult to troubleshoot issues and optimize resource usage.
prometheus-kube-state-metric	2.15.0	2.13.0	2.13.0	Recommended	Kube-state-metrics is a service that generates metrics about the state of various resources in a Kubernetes cluster. It's commonly used for monitoring and alerting purposes. **Impact**: Without these metrics, monitoring the health and performance of NFs could be challenging, making it harder to proactively address issues.
prometheus-node-exporter	1.8.2	1.8.2	1.8.2	Recommended	Prometheus Node Exporter collects hardware and OS-level metrics from Linux hosts. **Impact**: Without node-level metrics, visibility into infrastructure performance would be limited, complicating the identification of resource bottlenecks.
Prometheus Operator	0.80.1	0.76.0	0.76.0	Recommended	The Prometheus Operator is used for managing Prometheus monitoring systems in Kubernetes. Prometheus Operator simplifies the configuration and management of Prometheus instances. **Impact**: Not using this operator could complicate the setup and management of monitoring solutions, increasing the risk of missed performance insights.
rook	1.16.6	1.15.2	1.13.3	Mandatory	Rook is the Ceph orchestrator for Kubernetes that provides storage solutions. It is used in BareMetal CNE solution. **Impact**: Not utilizing rook could increase the complexity of deploying and managing ceph, making it difficult to scale storage solutions in a Kubernetes environment.
snmp-notifier	1.6.1	1.5.0	1.4.0	Recommended	snmp-notifier sends SNMP alerts for 5G NFs, providing real-time notifications for network events. **Impact**: Without SNMP notifications, proactive monitoring of NF health and performance could be compromised, delaying response to critical issues.

Table 2-3 (Cont.) Additional Software Versions

Software	25.1.2xx	25.1.1xx	24.3.x	Software Requirement	Usage Description
Velero	1.13.2	1.13.2	1.12.0	Recommended	Velero backs up and restores Kubernetes clusters for 5G NFs, ensuring data protection and disaster recovery. **Impact**: Without backup and recovery capabilities, customers would witness a risk of data loss and extended downtime, requiring a full cluster reinstall in case of failure or upgrade.

Important

If you are using NRF with SEPP, install it before proceeding with the SEPP installation. SEPP 25.1.2xx supports NRF 25.1.2xx.

2.1.2 Environment Setup Requirements

This section describes the environment setup requirements for installing SEPP.

2.1.2.1 Client Machine Requirements

This section describes the requirements for client machine, that is, the machine used by the user to run deployment commands.

The client machine should have:

- Helm repository configured.
  - To add a Helm repository, run the following command:

    ```
    helm repo add <helm-repo-name> <helm-repo-address>
    ```

    Where, `<helm-repo-name>` is the name of the Helm repository and `<helm-repo-address>` is the URL of the Helm repository.
  - To verify that Helm repository has been added successfully, run the following command:

    ```
    helm repo list
    ```

    The output must show the added Helm repository in the list.
- network access to the Helm repository and Docker image registry.
- network access to the Kubernetes cluster.
- required environment settings to run the `kubectl`, `podman`, or `docker` commands. The environment should have privileges to create namespace in the Kubernetes cluster.

- Helm client installed with the push plugin. Configure the environment in such a manner that the `helm install` command deploys the software in the Kubernetes cluster.

2.1.2.2 Network Access Requirement

The Kubernetes cluster hosts must have network access to the following repositories:

- Local Helm repository: It contains the SEPP helm charts.
  To check if the Kubernetes cluster hosts have network access to the local helm repository, run the following command:

  ```
  helm repo update
  ```

- Local Docker image registry: It contains the SEPP Docker images.
  To check if the Kubernetes cluster hosts can access the local docker image registry, pull any image with an image-tag using either of the following commands:

  ```
  docker pull <docker-repo>/<image-name>:<image-tag>
  ```

  ```
  podman pull <podman-repo>/<image-name>:<image-tag>
  ```

  Where:

  - `<docker-repo>` is the IP address or host name of the Docker registry.
  - `<image-name>` is the Docker image name.
  - `<image-tag>` is the tag assigned to the Docker image used for the SEPP pod.

  Example:

  ```
  docker pull CUSTOMER_REPO/oc-app-info:25.1.200
  ```

  ```
  podman pull occne-repo-host:5000/occnp/oc-app-info:25.1.200
  ```

2.1.2.3 Server or Space Requirement

For information about server or space requirements, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation Upgrade, and Fault Recovery Guide*.

2.1.2.4 CNE Requirement

This section is applicable only if you are installing SEPP on Cloud Native Environment (CNE).

SEPP supports CNE 25.1.2xx, 25.1.1xx, and 24.3.x.

To check the CNE version, run the following command:

```
echo $OCCNE_VERSION
```

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

2.1.2.5 cnDBTier Requirement

SEPP supports cnDBTier 25.1.2xx, 25.1.1xx, and 24.3.x. cnDBTier must be configured and running before installing SEPP. For more information about cnDBTier installation, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

For more information about the cnDBTier customizations required for SEPP, see the `ocsepp_dbtier_cnDBTier_version_custom_values_SEPP_version.yaml` file.

If you have already installed a version of cnDBTier, run the following command to upgrade your current cnDBTier installation using the `ocsepp_dbtier_<version>_custom_values_<version>.yaml` file:

```
helm upgrade <release-name> <chart-path> -f <cndb-custom-values.yaml> -n
<namespace>
```

For example:

```
helm upgrade mysql-cluster occndbtier/ -f
ocsepp_dbtier_25.1.200_custom_values_25.1.201.yaml -n ocsepp-cndb
```

For more information about cnDBTier installation and upgrade procedure, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

> **Note**
>
> In georedundant deployment, a dedicated cnDBTier must be installed and configured for each SEPP site.

> **Note**
>
> Starting from 25.1.100 onwards, the `ndb_allow_copying_alter_table` in cnDBTier should be set to OFF.

2.1.2.6 OSO Requirement

SEPP supports Operations Services Overlay (OSO) 25.1.2xx for common operation services (Prometheus and components such as alertmanager, pushgateway) on a Kubernetes cluster, which does not have these common services. For more information about OSO installation, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide.*

2.1.2.7 CNC Console Requirements

SEPP supports CNC Console 25.1.2xx to configure and manage Network Functions. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide.*

2.1.2.8 OCCM Requirements

SEPP supports OCCM 25.1.2xx. To support automated certificate lifecycle management, SEPP integrates with Oracle Communications Cloud Native Core, Certificate Management (OCCM) in compliance with 3GPP security recommendations. For more information about OCCM in SEPP, see the "Support for Automated Certificate Lifecycle Management" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.

For more information about OCCM, see the following guides:

- *Oracle Communications Cloud Native Core, Certificate Manager Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Certificate Manager User Guide*

2.1.2.9 OCI Requirements

SEPP can be deployed on OCI.

For more information about OCI deployment, see *Oracle Communications Cloud Native Core, OCI Adaptor Deployment Guide*.

2.1.3 SEPP Resource Requirements

This section lists the resource requirements to install and run SEPP.

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

2.1.3.1 SEPP Services

The following table lists resource requirement for SEPP Services:

Table 2-4 SEPP Services

Service Name	CPU	CPU	Memory(GB)	Memory(GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Gi)**	**Max(Gi)**
Helm Test	1	1	1	1	1	1	70Mi	1
Helm Hook	1	1	1	1	1	1	0	1
<helm-release-name>-n32-ingress-gateway	6	6	5	5	7	7	1	1

Table 2-4 (Cont.) SEPP Services

Service Name	CPU	CPU	Memory(GB)	Memory(GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	Min	Max	Min	Max	Min	Max	Min(Gi)	Max(Gi)
<helm-release-name>-n32-egress-gateway	5	5	5	5	7	7	1	1
<helm-release-name>-plmn-ingress-gateway	5	5	5	5	7	7	1	1
<helm-release-name>-plmn-egress-gateway	5	5	5	5	7	7	1	1
<helm-release-name>-pn32f-svc	5	5	8	8	7	7	2	2
<helm-release-name>-cn32f-svc	5	5	8	8	7	7	2	2
<helm-release-name>-cn32c-svc	2	2	2	2	2	2	1	1
<helm-release-name>-pn32c-svc	2	2	2	2	2	2	1	1
<helm-release-name>-config-mgr-svc	2	2	2	2	1	1	1	1
<helm-release-name>-sepp-nrf-client-nfdiscovery	1	1	2	2	2	2	1	1

Table 2-4 (Cont.) SEPP Services

Service Name	CPU	CPU	Memory(GB)	Memory(GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Gi)**	**Max(Gi)**
<helm-release-name>-sepp-nrf-client-nfmanagement	1	1	1	1	1	1	1	1
<helm-release-name>-ocpm-config	1	1	1	1	2	2	1	1
<helm-release-name>-appinfo	1	1	1	2	2	2	1	1
<helm-release-name>-perf-info	2	2	200Mi	4	2	2	1	1
<helm-release-name>-nf-mediation	8	8	8	8	2	2	NA	NA
<helm-release-name>-coherence-svc	1	1	2	2	1	1	NA	NA
<helm-release-name>-alternate-route	2	2	4	4	2	2	NA	NA
Total	56	56	63.200	68	63	63	16.7 Gi	18

Where,

- #: <helm-release-name> will be prefixed in each microservice name. Example: if Helm release name is "ocsepp-release", then cn32f-svc microservice name will be "ocsepp-release-cn32f-svc".
- Init-service container's and Common Configuration Client Hook's resources are not counted because the container gets terminated after initialization completes.
- **Helm Hooks Jobs:** These are pre and post jobs that are invoked during installation, upgrade, rollback, and uninstallation of the deployment. These are short span jobs that get terminated after the deployment completion.

- **Helm Test Job:** This job is run on demand when the Helm test command is initiated. This job runs the helm test and stops after completion. These are short-lived jobs that get terminated after the deployment is done. They are not part of active deployment resource, but are considered only during helm test procedures.
- If you enable Message Feed feature at Ingress Gateway and Egress Gateway, approximately 33% pod capacity is impacted.

> **Note**
>
> If you enable Message Feed feature at Ingress Gateway and Egress Gateway, approximately 33% pod capacity is impacted.

2.1.3.2 Upgrade

Following is the resource requirement for upgrading SEPP:

Table 2-5 Upgrade

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Gi)**	**Max(Gi)**
Helm test	0	0	0	0	0	0	0	0
Helm Hook	0	0	0	0	0	0	0	0
<helm-release-name>-n32-ingress-gateway	6	6	5	5	0	0	1	1
<helm-release-name>-n32-egress-gateway	5	5	5	5	0	0	1	1
<helm-release-name>-plmn-ingress-gateway	5	5	5	5	0	0	1	1
<helm-release-name>-plmn-egress-gateway	5	5	5	5	0	0	1	1
<helm-release-name>-pn32f-svc	5	5	8	8	0	0	2	2

Table 2-5 (Cont.) Upgrade

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	Min	Max	Min	Max	Min	Max	Min(Gi)	Max(Gi)
<helm-release-name>-cn32f-svc	5	5	8	8	0	0	2	2
<helm-release-name>-cn32c-svc	2	2	2	2	0	0	1	1
<helm-release-name>-pn32c-svc	2	2	2	2	0	0	1	1
<helm-release-name>-config-mgr-svc	2	2	2	2	0	0	1	1
<helm-release-name>-sepp-nrf-client-nfdiscovery	1	1	2	2	0	0	1	1
<helm-release-name>-sepp-nrf-client-nfmanagement	1	1	1	1	0	0	1	1
<helm-release-name>-ocpm-config	1	1	1	1	0	0	1	1
<helm-release-name>-appinfo	1	1	1	2	0	0	1	1
<helm-release-name>-perf-info	2	2	200Mi	4	0	0	1	1
<helm-release-name>-nf-mediation	8	8	8	8	0	0	1	1

Table 2-5 (Cont.) Upgrade

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Gi)**	**Max(Gi)**
<helm-release-name>-coherence-svc	1	1	2	2	0	0	NA	NA
<helm-release-name>-alternate-route	2	2	4	4	0	0	NA	NA
Total	54	54	61.2	66	0	0	17	17 Gi

Note

- `MaxSurge` is set to 0.
- <helm-release-name> is the Helm release name. For example, if Helm release name is "ocsepp-release", then cn32f-svc microservice name will be "ocsepp-release-cn32f-svc".

2.1.3.3 Common Services Container

Following is the resource requirement for Common Services Container:

Table 2-6 Common Services Container

Container Name	CPU	Memory (GB)	Kubernetes Init Container
init-service	1	1	Y
common_config_hook	1	1	N
mediation_hook	2	2	N

- **Init Container service:** Ingress or Egress Gateway services use this container to get OCSEPP Private Key or Certificate and CA Root Certificate for TLS during start up.
- **Common Configuration Hook:** It is used for creating database for common service configuration.

2.1.3.4 Service Mesh Sidecar

SEPP leverages the Platform Service Mesh (for example, Aspen Service Mesh) for all internal and external TLS communication. If ASM Sidecar injection is enabled during SEPP deployment or upgrade, this container is injected to each pod (or selected pod, depending on the option chosen during deployment or upgrade). These containers stay till pod or deployment exist.

Table 2-7 Service Mesh Sidecar

Service Name	CPU	CPU	Memory (GB	Memory (GB)	Ephemeral Storage	Ephemeral Storage
Min/Max	Min	Max	Min	Max	Min(Mi)	Max(Gi)
<helm-release-name>-n32-ingress-gateway	2	2	1	1	70	1
<helm-release-name>-n32-egress-gateway	2	2	1	1	70	1
<helm-release-name>-plmn-ingress-gateway	2	2	1	1	70	1
<helm-release-name>-plmn-egress-gateway	2	2	1	1	70	1
<helm-release-name>-pn32f-svc	2	2	1	1	70	1
<helm-release-name>-cn32f-svc	2	2	1	1	70	1
<helm-release-name>-cn32c-svc	2	2	1	1	70	1
<helm-release-name>-pn32c-svc	2	2	1	1	70	1
<helm-release-name>-config-mgr-svc	2	2	1	1	70	1
<helm-release-name>-sepp-nrf-client-nfdiscovery	2	2	1	1	70	1

Table 2-7 (Cont.) Service Mesh Sidecar

Service Name	CPU	CPU	Memory (GB	Memory (GB)	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min(Mi)**	**Max(Gi)**
<helm-release-name>-sepp-nrf-client-nfmanagement	2	2	1	1	70	1
<helm-release-name>-ocpm-config	2	2	1	1	70	1
<helm-release-name>-appinfo	2	2	1	1	70	1
<helm-release-name>-perf-info	2	2	1	1	70	1
<helm-release-name>-nf-mediation	2	2	1	1	70	1
<helm-release-name>-coherence-svc	2	2	1	1	NA	NA
<helm-release-name>-alternate-route	2	2	1	1	NA	NA
Total	34	34	17	17	1050 Mi	15 Gi

> **Note**
>
> <helm-release-name> is the Helm release name. For example, if Helm release name is "ocsepp-release", then cn32f-svc microservice name will be "ocsepp-release-cn32f-svc".

2.1.3.5 Debug Tool Container

The Debug Tool provides third-party troubleshooting tools for debugging the runtime issues in a lab environment. If Debug Tool Container injection is enabled during SEPP deployment or upgrade, this container is injected to each SEPP pod (or selected pod, depending on the option chosen during deployment or upgrade). These containers stay till pod or deployment exist. For more information about configuring Debug Tool, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide*.

Table 2-8 Debug Tool Container

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	Ephemeral Storage	Ephemeral Storage
Min/Max	Min	Max	Min(Gi)	Max(Gi)	Min(Mi)	Max(Mi)
<helm-release-name>-n32-ingress-gateway	0.5	1	4	4	512	512
<helm-release-name>-n32-egress-gateway	0.5	1	4	4	512	512
<helm-release-name>-plmn-ingress-gateway	0.5	1	4	4	512	512
<helm-release-name>-plmn-egress-gateway	0.5	1	4	4	512	512
<helm-release-name>-pn32f-svc	0.5	1	4	4	512	512
<helm-release-name>-cn32f-svc	0.5	1	4	4	512	512
<helm-release-name>-cn32c-svc	0.5	1	4	4	512	512
<helm-release-name>-pn32c-svc	0.5	1	4	4	512	512
<helm-release-name>-config-mgr-svc	0.5	1	4	4	512	512
<helm-release-name>-sepp-nrf-client-nfdiscovery	0.5	1	4	4	512	512

Table 2-8 (Cont.) Debug Tool Container

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min(Gi)**	**Max(Gi)**	**Min(Mi)**	**Max(Mi)**
<helm-release-name>-sepp-nrf-client-nfmanagement	0.5	1	4	4	512	512
<helm-release-name>-ocpm-config	0.5	1	4	4	512	512
<helm-release-name>-appinfo	0.5	1	4	4	512	512
<helm-release-name>-perf-info	0.5	1	4	4	512	512
<helm-release-name>-nf-mediation	0.5	1	4	4	512	512
<helm-release-name>-coherence-svc	NA	NA	NA	NA	NA	NA
<helm-release-name>-alternate-route	0.5	1	4	4	NA	NA
Total	8	16	64	64	7680 Mi	7680 Mi

> **Note**
>
> <helm_release_name> is the Helm release name. For example, if Helm release name is "ocsepp-release", then plmn-egress-gateway microservice name will be "ocsepp-release-plmn-egress-gateway".

2.1.3.6 SEPP Hooks

Following is the resource requirement for SEPP Hooks:

Table 2-9 SEPP Hooks

Hook Name	CPU		Memory (GB)	
Min/Max	Min	Max	Min	Max
<helm-release-name>-update-db-pre-install	1	1	1	1
<helm-release-name>-update-db-<post-install>	1	1	1	1
<helm-release-name>-update-db-<pre-upgrade>	1	1	1	1
<helm-release-name>-update-db-<post-upgrade>	1	1	1	1
<helm-release-name>-update-db-<pre-rollback>	1	1	1	1
<helm-release-name>-update-db-<post-rollback>	1	1	1	1
<helm-release-name>-pn32f-svc-pre-install	1	1	1	1
<helm-release-name>-pn32f-svc-post-install	1	1	1	1
<helm-release-name>-pn32f-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-pn32f-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-pn32f-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-pn32f-svc-<post-rollback>	1	1	1	1
<helm-release-name>-cn32f-svc-pre-install	1	1	1	1
<helm-release-name>-cn32f-svc-<post-install>	1	1	1	1
<helm-release-name>-cn32f-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-cn32f-svc-<post-upgrade>	1	1	1	1

Table 2-9 (Cont.) SEPP Hooks

Hook Name	CPU		Memory (GB)	
<helm-release-name>-cn32f-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-cn32f-svc-<post-rollback>	1	1	1	1
<helm-release-name>-cn32c-svc-pre-install	1	1	1	1
<helm-release-name>-cn32c-svc-<post-install>	1	1	1	1
<helm-release-name>-cn32c-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-cn32c-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-cn32c-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-cn32c-svc-<post-rollback>	1	1	1	1
<helm-release-name>-pn32c-svc-pre-install	1	1	1	1
<helm-release-name>-pn32c-svc-<post-install>	1	1	1	1
<helm-release-name>-pn32c-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-pn32c-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-pn32c-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-pn32c-svc-<post-rollback>	1	1	1	1
<helm-release-name>-config-mgr-svc-pre-install	1	1	1	1
<helm-release-name>-config-mgr-svc-<post-install>	1	1	1	1
<helm-release-name>-config-mgr-svc-<pre-upgrade>	1	1	1	1

Table 2-9 (Cont.) SEPP Hooks

Hook Name	CPU		Memory (GB)	
<helm-release-name>-config-mgr-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-config-mgr-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-config-mgr-svc-<post-rollback>	1	1	1	1

> **Note**
>
> <helm-release-name> is the Helm release name.

2.1.3.7 CNC Console

CNC Console Oracle Communications Cloud Native Configuration Console (CNC Console) is a Graphical User Interface (GUI) for NFs and Oracle Communications Cloud Native Core, Cloud Native Environment (CNE) common services.

For information about CNC Console resources required by SEPP, see "CNC Console Resource Requirement" section in *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide*.

2.1.3.8 cnDBTier

cnDBTier is the geodiverse database layer provided as part of the Cloud Native Environment. It provides persistent storage for the state data and subscriber data in a cloud environment. Any Kubernetes environment with dynamic Kubernetes storage supports cnDBTier installation.

Table 2-10 cnDBTier

Detailed DBTier Resources	vCPU	Memory (GB)	Max Replicas	Total vCPU	Total Memory (GB)	PVC Storage (GB)	Ephemeral Storage (GB)
SQL - Replication (ndbmysqld) StatefulSet	3	4	4	12	16	60	0.1
MGMT (ndbmgmd) StatefulSet	3	4	2	6	8	15	0.1
DB (ndbmtd) StatefulSet	4	12	4	16	48	60	0.1

Table 2-10 (Cont.) cnDBTier

Detailed DBTier Resources	vCPU	Memory (GB)	Max Replicas	Total vCPU	Total Memory (GB)	PVC Storage (GB)	Ephemeral Storage (GB)
db-backup-manager-svc	1	1	1	1	1	0	0.1
db-replication-svc	1	2	1	1	2	60	0.1
db-monitor-svc	4	4	1	4	4	0	0.1
db-connectivity-service	0	0	0	0	0	0	0
SQL - Access (ndbappmysqld) StatefulSet	5	10	2	10	20	20	0.1
grrecoveryresources	2	12	2	4	24	0	0
Total			17	54	123	215	0.7

Note

- Node profiles in the above tables are for two-site replication cnDBTier clusters. Modify the `ndbmysqld` and `Replication Service` pods based on the number of georeplication sites.
- In case, any of the service requires a vertical scaling of any of their PVC, see the respective sub-section in "Vertical Scaling" section in *Oracle Communications Cloud Native Core, cnDBTier User Guide*.
- PVC shrinking (downsizing) is not supported. It is recommended to retain the existing vertically scaled up PVC sizes, eventhough cnDBTier is rolledback to previous releases.

For information about cnDBTier resources required by SEPP, see "Resource Requirement" section in *Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

2.1.3.8.1 cnDBTier Sidecars

The following table indicates the sidecars for cnDBTier services.

Table 2-11 Sidecars per cnDBTier Service

Service Name	init-sidecar	db-executor-svc	init-discover-sql-ips	db-infra-monitor-svc
MGMT (ndbmgmd)	No	No	No	Yes

Table 2-11 (Cont.) Sidecars per cnDBTier Service

Service Name	init-sidecar	db-executor-svc	init-discover-sql-ips	db-infra-monitor-svc
DB (ndbmtd)	No	Yes	No	Yes
SQL (ndbmysqld)	Yes	No	No	Yes
SQL (ndbappmysqld)	Yes	No	No	Yes
Monitor Service (db-monitor-svc)	No	No	No	No
Backup Manager Service (db-backup-manager-svc)	No	No	No	No
Replication Service	No	No	Yes	No

Table 2-12 cnDBTier Additional Containers

Sidecar	CPU/Pod		Memory/Pod (in Gi)		PVC Size (in Gi)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (Mi)	Max(Gi)Min (Mi)
db-executor-svc	1	1	2	2	NA	NA	90	1
init-sidecar	0.1	0.1	025	0.25	NA	NA	90	1
init-discover-sql-ips	0.2	0.2	0.5	0.5	NA	NA	90	1
db-infra-monitor-svc	0.1	0.1	0.25	0.25	NA	NA	90	1

2.1.3.8.2 Service Mesh Sidecar

If SEPP is deployed with ASM, the user must add the following annotation in the `ocsepp_dbtier_CNDBTIER_VERSION_custom_values_SEPP_VERSION.yaml` file.

\

Table 2-13 Default Values for Service Mesh Specific Annotations

Parameter Name	Annotations
`db-monitor-svc.podAnnotations`	traffic.sidecar.istio.io/excludeInboundPorts: "8081,8080"

Example:

```
db-monitor-svc:
  podAnnotations:
    traffic.sidecar.istio.io/excludeInboundPorts: "8081,8080"
```

2.1.4 Roaming Hub or Hosted SEPP Resource Requirements

This section lists the resource requirements to install and run Roaming Hub or Hosted SEPP.

2.1.4.1 Roaming Hub or Hosted SEPP Services

The following table lists resource requirement for SEPP Services for Roaming Hub or Hosted SEPP:

Table 2-14 SEPP Services for Roaming Hub or Hosted SEPP

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Mi)**	**Max(Gi)**
Helm Test	1	1	1	1	1	1	70	1
Helm Hook	1	1	1	1	1	1	0	1
<helm-release-name>-n32-ingress-gateway	6	6	5	5	2	2	70	1
<helm-release-name>-n32-egress-gateway	5	5	5	5	2	2	70	1
<helm-release-name>-plmn-ingress-gateway	5	5	5	5	2	2	70	1
<helm-release-name>-plmn-egress-gateway	5	5	5	5	2	2	70	1
<helm-release-name>-pn32f-svc	5	5	8	8	2	2	70	1
<helm-release-name>-cn32f-svc	5	5	8	8	2	2	70	1
<helm-release-name>-cn32c-svc	2	2	2	2	2	2	70	1

Table 2-14 (Cont.) SEPP Services for Roaming Hub or Hosted SEPP

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Mi)**	**Max(Gi)**
<helm-release-name>-pn32c-svc	2	2	2	2	2	2	70	1
<helm-release-name>-config-mgr-svc	2	2	2	2	1	1	70	1
<helm-release-name>-perf-info	2	2	200Mi	4	2	2	1	1
<helm-release-name>-nf-mediation	8	8	8	8	2	2	NA	NA
Total	49	49	52.2	56	23	23	701 Mi	12 Gi

Note

- #: <helm-release-name> will be prefixed in each microservice name. Example: if Helm release name is "ocsepp-release", then cn32f-svc microservice name will be "ocsepp-release-cn32f-svc"
- Init-service container's and Common Configuration Client Hook's resources are not counted because the container gets terminated after initialization completes.
- **Helm Hooks Jobs:** These are pre and post jobs that are invoked during installation, upgrade, rollback, and uninstallation of the deployment. These are short span jobs that get terminated after the deployment completion.
- **Helm Test Job:** This job is run on demand when the helm test command is initiated. This job runs the helm test and stops after completion. These are short-lived jobs that get terminated after the deployment is done. They are not part of active deployment resource, but are considered only during helm test procedures.

2.1.4.2 Upgrade

Following is the resource requirement for upgrading Roaming Hub or Hosted SEPP:

Table 2-15 Upgrade

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Mi)**	**Max(Gi)**
Helm test	0	0	0	0	0	0	0	0
Helm Hook	0	0	0	0	0	0	0	0
<helm-release-name>-n32-ingress-gateway	6	6	5	5	1	2	70	1
<helm-release-name>-n32-egress-gateway	5	5	5	5	1	2	70	1
<helm-release-name>-plmn-ingress-gateway	5	5	5	5	1	2	70	1
<helm-release-name>-plmn-egress-gateway	5	5	5	5	1	2	70	1
<helm-release-name>-pn32f-svc	5	5	8	8	1	2	70	1
<helm-release-name>-cn32f-svc	5	5	8	8	1	3	70	1
<helm-release-name>-cn32c-svc	2	2	2	2	1	1	70	1
<helm-release-name>-pn32c-svc	2	2	2	2	1	1	70	1
<helm-release-name>-config-mgr-svc	2	2	2	2	1	1	70	1

Table 2-15 (Cont.) Upgrade

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	POD	POD	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min**	**Max**	**Min**	**Max**	**Min(Mi)**	**Max(Gi)**
<helm-release-name>-perf-info	2	2	200Mi	4	1	1	70	1
<helm-release-name>-nf-mediation	8	8	8	8	1	1	70	1
Total	47	47	50.2	54	11	18	770 Mi	11 Gi

> **Note**
>
> <helm-release-name> is the Helm release name. For example, if Helm release name is "ocsepp-release", then cn32f-svc microservice name will be "ocsepp-release-cn32f-svc"

2.1.4.3 Common Services Container

Following is the resource requirement for Common Services Container:

Table 2-16 Common Services Container

Container Name	CPU	Memory (GB)	Kubernetes Init Container
init-service	1	1	Y
common_config_hook	1	1	N

> **Note**
>
> - **Init Container service:** Ingress or Egress Gateway services use this container to get SEPP Private Key or Certificate and CA Root Certificate for TLS during start up.
> - **Common Configuration Hook:** It is used for creating database for common service configuration.

2.1.4.4 ASM Sidecar

> **Note**
>
> In Roaming Hub or Hosted SEPP mode, ASM is not supported.

2.1.4.5 Debug Tool Container

The Debug Tool provides third-party troubleshooting tools for debugging the runtime issues in a lab environment. If Debug Tool Container injection is enabled during Roaming Hub/Hosted SEPP deployment or upgrade, this container is injected to each Roaming Hub/Hosted SEPP pod (or selected pod, depending on the option chosen during deployment or upgrade). These containers stay till pod or deployment exist. For more information about configuring the Debug Tool, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide*.

Table 2-17 Debug Tool Container

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	Ephemeral Storage	Ephemeral Storage
Min/Max	**Min**	**Max**	**Min(Gi)**	**Max(Gi)**	**Min(Mi)**	**Max(Mi)**
Helm Test	0	0	0	0	512	512
Helm Test	0	0	0	0	512	512
<helm-release-name>-n32-ingress-gateway	0.5	1	4	4	512	512
<helm-release-name>-n32-egress-gateway	0.5	1	4	4	512	512
<helm-release-name>-plmn-ingress-gateway	0.5	1	4	4	512	512
<helm-release-name>-plmn-egress-gateway	0.5	1	4	4	512	512
<helm-release-name>-pn32f-svc	0.5	1	4	4	512	512
<helm-release-name>-cn32f-svc	0.5	1	4	4	512	512

Table 2-17 (Cont.) Debug Tool Container

Service Name	CPU	CPU	Memory (GB)	Memory (GB)	Ephemeral Storage	Ephemeral Storage
Min/Max	Min	Max	Min(Gi)	Max(Gi)	Min(Mi)	Max(Mi)
<helm-release-name>-cn32c-svc	0.5	1	4	4	512	512
<helm-release-name>-pn32c-svc	0.5	1	4	4	512	512
<helm-release-name>-config-mgr-svc	0.5	1	4	4	512	512
<helm-release-name>-perf-info	0.5	1	4	4	512	512
<helm-release-name>-nf-mediation	0.5	1	4	4	512	512
Total	5.5	11	44	44	6656 Mi	6656 Mi

> **Note**
>
> <helm-release-name> is the Helm release name. Example: if helm release name is "ocsepp", then cn32f-svc microservice name will be "ocsepp-cn32f-svc"

2.1.4.6 SEPP Hooks

Following is the resource requirement for SEPP Hooks.

Table 2-18 SEPP Hooks

Hook Name	CPU	CPU	Memory (GB)	Memory (GB)
Min/Max	Min	Max	Min	Max
<helm-release-name>-update-db-pre-install	1	1	1	1
<helm-release-name>-update-db-<post-install>	1	1	1	1
<helm-release-name>-update-db-<pre-upgrade>	1	1	1	1

Table 2-18 (Cont.) SEPP Hooks

Hook Name	CPU	CPU	Memory (GB)	Memory (GB)
<helm-release-name>-update-db-<post-upgrade>	1	1	1	1
<helm-release-name>-update-db-<pre-rollback>	1	1	1	1
<helm-release-name>-update-db-<post-rollback>	1	1	1	1
<helm-release-name>-pn32f-svc-pre-install	1	1	1	1
<helm-release-name>-pn32f-svc-post-install	1	1	1	1
<helm-release-name>-pn32f-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-pn32f-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-pn32f-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-pn32f-svc-<post-rollback>	1	1	1	1
<helm-release-name>-cn32f-svc-pre-install	1	1	1	1
<helm-release-name>-cn32f-svc-<post-install>	1	1	1	1
<helm-release-name>-cn32f-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-cn32f-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-cn32f-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-cn32f-svc-<post-rollback>	1	1	1	1
<helm-release-name>-cn32c-svc-pre-install	1	1	1	1
<helm-release-name>-cn32c-svc-<post-install>	1	1	1	1

Table 2-18 (Cont.) SEPP Hooks

Hook Name	CPU	CPU	Memory (GB)	Memory (GB)
<helm-release-name>-cn32c-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-cn32c-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-cn32c-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-cn32c-svc-<post-rollback>	1	1	1	1
<helm-release-name>-pn32c-svc-pre-install	1	1	1	1
<helm-release-name>-pn32c-svc-<post-install>	1	1	1	1
<helm-release-name>-pn32c-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-pn32c-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-pn32c-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-pn32c-svc-<post-rollback>	1	1	1	1
<helm-release-name>-config-mgr-svc-pre-install	1	1	1	1
<helm-release-name>-config-mgr-svc-<post-install>	1	1	1	1
<helm-release-name>-config-mgr-svc-<pre-upgrade>	1	1	1	1
<helm-release-name>-config-mgr-svc-<post-upgrade>	1	1	1	1
<helm-release-name>-config-mgr-svc-<pre-rollback>	1	1	1	1
<helm-release-name>-config-mgr-svc-<post-rollback>	1	1	1	1

> **Note**
>
> <helm-release-name> is the Helm release name.

2.2 Installation Sequence

This section describes preinstallation, installation, and postinstallation tasks for SEPP (SEPP, Roaming Hub, or Hosted SEPP).

2.2.1 Preinstallation Tasks

Before installing SEPP, perform the tasks described in this section.

2.2.1.1 Downloading SEPP package

Perform the following procedure to download the Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) release package from My Oracle Support:

1. Log in to My Oracle Support using the appropriate credentials.
2. Click the **Patches & Updates** tab to locate the patch.
3. In **Patch Search** console, click the **Product or Family (Advanced)** tab.
4. Enter `Oracle Communications Cloud Native Core - 5G` in **Product** field and select the product from the Product drop-down list.
5. From the **Release** drop-down, select **"Oracle Communications Cloud Native Core Security Edge Protection Proxy <release_number>".**

   Where, <release-number> indicates the required release number of Cloud Native Core, Security Edge Protection Proxy.
6. Click **Search.** The Patch Advanced Search Results list appears.
7. Select the required patch from the list. The **Patch Details** window appears.
8. Click **Download**. File Download window appears.
9. Click the `<p********_<release_number>_Tekelec>.zip` file to download the package. Where, <p********> is the MOS patch number and <release_number> is the release number of SEPP.

2.2.1.2 Pushing the SEPP Images to Customer Docker Registry

SEPP deployment package includes ready-to-use images and Helm charts to orchestrate containers in Kubernetes.

The following table lists the docker images for SEPP:

Table 2-19 SEPP Images

Services	Image	Tag
<helm-release-name>-alternate_route	alternate_route	25.1.206
<helm-release-name>-common_config_hook	common_config_hook	25.1.202

Table 2-19 (Cont.) SEPP Images

Services	Image	Tag
<helm-release-name>-configurationinit	configurationinit	25.1.202
<helm-release-name>-mediation/ocmed-nfmediation	mediation/ocmed-nfmediation	25.1.107
<helm-release-name>-nf_test	nf_test	25.1.202
<helm-release-name>-nrf-client	nrf-client	25.1.204
<helm-release-name>-occnp/oc-app-info	occnp/oc-app-info	25.1.204
<helm-release-name>-occnp/oc-config-server	occnp/oc-config-server	25.1.204
<helm-release-name>-performance	occnp/oc-perf-info	25.1.204
<helm-release-name>-ocdebugtool/ocdebug-tools	ocdebugtool/ocdebug-tools	25.1.203
<helm-release-name>-ocegress_gateway	ocegress_gateway	25.1.206
<helm-release-name>-ocingress_gateway	ocingress_gateway	25.1.206
<helm-release-name>-oocsepp-cn32c-svc	ocsepp-cn32c-svc	25.1.202
<helm-release-name>- ocsepp-cn32f-svc	ocsepp-cn32f-svc	25.1.202
<helm-release-name>-ocsepp-coherence-svc	ocsepp-coherence-svc	25.1.202
<helm-release-name>-ocsepp-config-mgr-svc	ocsepp-config-mgr-svc	25.1.202
<helm-release-name>-ocsepp-pn32c-svc	ocsepp-pn32c-svc	25.1.202
<helm-release-name>-ocsepp-pn32f-svc	ocsepp-pn32f-svc	25.1.202
<helm-release-name>-ocsepp-pre-install-hook	ocsepp-pre-install-hook	25.1.202
<helm-release-name>-ocsepp-update-db	ocsepp-update-db	25.1.202
<helm-release-name>-ocsepp-configurationupdate	configurationupdate	25.1.202

To push the images to the registry:

1. Navigate to the location where you want to install SEPP. Unzip the SEPP release package to retrieve the following CSAR package.
   The SEPP package is as follows:

   ```
   ReleaseName_csar_Releasenumber.zip
   ```

   Where:

   - ReleaseName is a name that is used to track this installation instance.
   - Releasenumber is the release number.

     For example:

   ```
   ocsepp_csar_25_1_202_0_0.zip
   ```

2. Unzip the SEPP package file to get SEPP docker image tar file:

   ```
   unzip ocsepp_csar_Releasenumber.zip
   ```

For example:

```
unzip ocsepp_csar_25_1_202_0_0.zip
```

3. The directory `ocsepp_csar_25_1_202_0_0.zip` consists of the following:

```
├─── Definitions
│    ├─── ocsepp_cne_compatibility.yaml
│    └─── ocsepp.yaml
├─── Files
│    ├─── alternate_route-25.1.206.tar
│    ├─── ChangeLog.txt
│    ├─── common_config_hook-25.1.202.tar
│    ├─── configurationinit-25.1.202.tar
│    ├─── Helm
│    │    ├─── ocsepp-25.1.202.tgz
│    │    ├─── ocsepp-network-policy-25.1.202.tgz
│    │    └─── ocsepp-servicemesh-config-25.1.202.tgz
│    ├─── Licenses
│    ├─── mediation-ocmed-nfmediation-25.1.107.tar
│    ├─── nf_test-25.1.202.tar
│    ├─── nrf-client-25.1.204.tar
│    ├─── occnp-oc-app-info-25.1.204.tar
│    ├─── occnp-oc-config-server-25.1.204.tar
│    ├─── occnp-oc-perf-info-25.1.204.tar
│    ├─── ocdebugtool-ocdebug-tools-25.1.203.tar
│    ├─── ocegress_gateway-25.1.206.tar
│    ├─── ocingress_gateway-25.1.206.tar
│    ├─── ocsepp-cn32c-svc-25.1.202.tar
│    ├─── ocsepp-cn32f-svc-25.1.202.tar
│    ├─── ocsepp-coherence-svc-25.1.202.tar
│    ├─── ocsepp-config-mgr-svc-25.1.202.tar
│    ├─── ocsepp-pn32c-svc-25.1.202.tar
│    ├─── ocsepp-pn32f-svc-25.1.202.tar
│    ├─── ocsepp-pre-install-hook-25.1.202.tar
│    ├─── ocsepp-update-db-25.1.202.tar
│    ├─── Oracle.cert
│    └─── Tests
├─── ocsepp.mf
├─── Scripts
│    ├─── ocsepp_alertrules_promha_25.1.202.yaml
│    ├─── ocsepp_configuration_openapi_25.1.202.yaml
│    ├─── ocsepp_custom_values_25.1.202.yaml
│    ├─── ocsepp_custom_values_roaming_hub_25.1.202.yaml
│    ├─── ocsepp_dashboard_25.1.202.json
│    ├─── ocsepp_dashboard_promha_25.1.202.json
│    ├─── ocsepp_network_policies_custom_values_25.1.202.yaml
│    ├─── ocsepp-servicemesh-config-25.1.202.tgz
│    ├─── ocsepp_alertrules_25.1.202.yaml
│    ├─── ocsepp_mib_25.1.202.mib
│    ├─── ocsepp_mib_tc_25.1.202.mib
│    └─── toplevel.mib
│    └─── ocsepp_oci_alertrules_25.1.202.zip
│    └─── ocsepp_oci_dashboard_25.1.202.json
│    └─── ocsepp_rollback_schema_25.1.202.sql
│    └─── ocsepp_dbtier_25.1.200_custom_values_25.1.202.yaml
│    └─── ocsepp_single_service_account_config_25.1.202.yaml
└─── TOSCA-Metadata
     └─── TOSCA.meta
```

4. Open the `Files` folder and based on the container engine installed, run one of the following command to load the SEPP images. Load all the images that are listed in SEPP Images (2-18) Table:

   ```
   podman load --input /IMAGE_PATH/<microservicename-releasenumber>.tar

   docker load --input /IMAGE_PATH/<microservicename-releasenumber>.tar
   ```

   Where, IMAGE_PATH is the location where the SEPP docker image tar file is archived.

   Sample command:

   ```
   podman load --input /IMAGE_PATH/ocsepp-pn32c-svc-25.1.202.tar
   ```

   > **Note**
   >
   > The docker/podman load command needs to be executed seperately for each tar file/docker image.

5. Run one of the following commands to verify that the image is loaded:

   ```
   docker images | grep ocsepp


   podman images | grep ocsepp
   ```

   > **Note**
   >
   > Verify the list of images shown in the output with the list of images shown in the table SEPP Images. If the list does not match, reload the image tar file.

6. Run one of the following commands to tag the images to the registry:

   ```
   docker tag <image-name>:<image-tag> <docker-repo>/<image-name>:<image-tag>


   podman tag <image-name>:<image-tag> <docker-repo>/<image-name>:<image-tag>
   ```

   Sample Tag commands:

   ```


   podman tag alternate_route:25.1.206 <customer repo>/
   alternate_route:25.1.206
   podman tag common_config_hook:25.1.202 <customer repo>/
   common_config_hook:25.1.202
   podman tag configurationinit:25.1.200 <customer repo>/
   configurationinit:25.1.200
   podman tag configurationupdate:25.1.200 <customer repo>/
   configurationupdate:25.1.200
   podman tag mediation/ocmed-nfmediation:25.1.107 <customer repo>/mediation/
   ocmed-nfmediation:25.1.107
   podman tag nf_test:25.1.202 <customer repo>/nf_test:25.1.202
   podman tag nrf-client:25.1.204 <customer repo>/nrf-client:25.1.204
   podman tag occnp/oc-app-info:25.1.204 <customer repo>/occnp/oc-app-
   ```

```
info:25.1.204
podman tag occnp/oc-config-server:25.1.204 <customer repo>/occnp/oc-config-
server:25.1.204
podman tag occnp/oc-perf-info:25.1.204 <customer repo>/occnp/oc-perf-
info:25.1.204
podman tag ocdebugtool/ocdebug-tools:25.1.203 <customer repo>/ocdebugtool/
ocdebug-tools:25.1.203
podman tag ocegress_gateway:25.1.206 <customer repo>/
ocegress_gateway:25.1.206
podman tag ocingress_gateway:25.1.206 <customer repo>/
ocingress_gateway:25.1.206
podman tag ocsepp-cn32c-svc:25.1.200 <customer repo>/ocsepp-cn32c-
svc:25.1.200
podman tag ocsepp-cn32f-svc:25.1.200 <customer repo>/ocsepp-cn32f-
svc:25.1.200
podman tag ocsepp-coherence-svc:25.1.200 <customer repo>/ocsepp-coherence-
svc:25.1.200
podman tag ocsepp-config-mgr-svc:25.1.200 <customer repo>/ocsepp-config-
mgr-svc:25.1.200
podman tag ocsepp-pn32c-svc:25.1.200 <customer repo>/ocsepp-pn32c-
svc:25.1.200
podman tag ocsepp-pn32f-svc:25.1.200 <customer repo>/ocsepp-pn32f-
svc:25.1.200
podman tag ocsepp-pre-install-hook:25.1.200 <customer repo>/ocsepp-pre-
install-hook:25.1.200
podman tag ocsepp-update-db:25.1.200 <customer repo>/ocsepp-update-
db:25.1.200
```

7. Run one of the following commands to push the image to the registry:

```
docker push <docker-repo>/<image-name>:<image-tag>

podman push <docker-repo>/<image-name>:<image-tag>
```

Sample push commands:

```
podman push occne-repo-host:5000/alternate_route:25.1.206
podman push occne-repo-host:5000/common_config_hook:25.1.202
podman push occne-repo-host:5000/configurationinit:25.1.200
podman push occne-repo-host:5000/configurationupdate:25.1.200
podman push occne-repo-host:5000/mediation/ocmed-nfmediation:25.1.107
podman push occne-repo-host:5000/nf_test:25.1.202
podman push occne-repo-host:5000/nrf-client:25.1.204
podman push occne-repo-host:5000/occnp/oc-app-info:25.1.204
podman push occne-repo-host:5000/occnp/oc-config-server:25.1.204
podman push occne-repo-host:5000/occnp/oc-perf-info:25.1.204
podman push occne-repo-host:5000/ocdebugtool/ocdebug-tools:25.1.203
podman push occne-repo-host:5000/ocegress_gateway:25.1.206
podman push occne-repo-host:5000/ocingress_gateway:25.1.206
podman push occne-repo-host:5000/ocsepp-cn32c-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-cn32f-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-coherence-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-config-mgr-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-pn32c-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-pn32f-svc:25.1.200
```

```
podman push occne-repo-host:5000/ocsepp-pre-install-hook:25.1.200
podman push occne-repo-host:5000/ocsepp-update-db:25.1.200
```

> **Note**
>
> It is recommended to configure the Docker certificate before running the push command to access customer registry through HTTPS, otherwise docker push command may fail.

2.2.1.3 Pushing the Roaming Hub or Hosted SEPP Images to Customer Docker Registry

Roaming Hub or Hosted SEPP deployment package includes ready-to-use images and Helm charts to orchestrate containers in Kubernetes.

The following table lists the docker images for Roaming Hub or Hosted SEPP:

Table 2-20 Roaming Hub or Hosted SEPP

Services	Image	Tag
<helm-release-name>-alternate_route	alternate_route	25.1.206
<helm-release-name>-common_config_hook	common_config_hook	25.1.202
<helm-release-name>-configurationinit	configurationinit	25.1.202
<helm-release-name>-mediation/ocmed-nfmediation	mediation/ocmed-nfmediation	25.1.107
<helm-release-name>-nf_test	nf_test	25.1.202
<helm-release-name>-performance	occnp/oc-perf-info	25.1.204
<helm-release-name>-ocdebugtool/ocdebug-tools	ocdebugtool/ocdebug-tools	25.1.203
<helm-release-name>-ocegress_gateway	ocegress_gateway	25.1.206
<helm-release-name>-ocingress_gateway	ocingress_gateway	25.1.206
<helm-release-name>-oocsepp-cn32c-svc	ocsepp-cn32c-svc	25.1.202
<helm-release-name>- ocsepp-cn32f-svc	ocsepp-cn32f-svc	25.1.202
<helm-release-name>-ocsepp-coherence-svc	ocsepp-coherence-svc	25.1.202
<helm-release-name>-ocsepp-config-mgr-svc	ocsepp-config-mgr-svc	25.1.202
<helm-release-name>-ocsepp-pn32c-svc	ocsepp-pn32c-svc	25.1.202
<helm-release-name>-ocsepp-pn32f-svc	ocsepp-pn32f-svc	25.1.202
<helm-release-name>-ocsepp-pre-install-hook	ocsepp-pre-install-hook	25.1.202
<helm-release-name>-ocsepp-update-db	ocsepp-update-db	25.1.202
<helm-release-name>-ocsepp-configurationupdate	configurationupdate	25.1.202

> **Note**
>
> <helm-release-name> will be prefixed in each microservice name. Example: if Helm release name is "ocsepp", then cn32f-svc microservice name will be "ocsepp-cn32f-svc".

To push the images to the registry:

1. Navigate to the location where you want to install SEPP. Unzip the SEPP release package (<p********>_<release_number>_Tekelec.zip) to retrieve the following CSAR package. The SEPP package is as follows:

   ```
   ReleaseName_csar_Releasenumber.zip
   ```

   Where:

   - ReleaseName is a name that is used to track this installation instance.
   - Releasenumber is the release number.

     For example:

   ```
   ocsepp_csar_25_1_202_0_0.zip
   ```

2. Unzip the SEPP package file to get SEPP docker image tar file:

   ```
   unzip ReleaseName_csar_Releasenumber.zip
   ```

   For example:

   ```
   unzip ocsepp_csar_25_1_202_0_0.zip
   ```

3. The directory `ocsepp_csar_25_1_202_0_0.zip` consists of the following:

   ```
   ├── Definitions
   │   ├── ocsepp_cne_compatibility.yaml
   │   └── ocsepp.yaml
   ├── Files
   │   ├── alternate_route-25.1.206.tar
   │   ├── ChangeLog.txt
   │   ├── common_config_hook-25.1.202.tar
   │   ├── configurationinit-25.1.202.tar
   │   ├── Helm
   │   │   ├── ocsepp-25.1.202.tgz
   │   │   ├── ocsepp-network-policy-25.1.202.tgz
   │   │   └── ocsepp-servicemesh-config-25.1.202.tgz
   │   ├── Licenses
   │   ├── mediation-ocmed-nfmediation-25.1.107.tar
   │   ├── nf_test-25.1.202.tar
   │   ├── nrf-client-25.1.204.tar
   │   ├── occnp-oc-app-info-25.1.204.tar
   │   ├── occnp-oc-config-server-25.1.204.tar
   │   ├── occnp-oc-perf-info-25.1.204.tar
   │   ├── ocdebugtool-ocdebug-tools-25.1.203.tar
   │   ├── ocegress_gateway-25.1.206.tar
   │   ├── ocingress_gateway-25.1.206.tar
   │   ├── ocsepp-cn32c-svc-25.1.202.tar
   │   ├── ocsepp-cn32f-svc-25.1.202.tar
   ```

```
│   ├── ocsepp-coherence-svc-25.1.202.tar
│   ├── ocsepp-config-mgr-svc-25.1.202.tar
│   ├── ocsepp-pn32c-svc-25.1.202.tar
│   ├── ocsepp-pn32f-svc-25.1.202.tar
│   ├── ocsepp-pre-install-hook-25.1.202.tar
│   ├── ocsepp-update-db-25.1.202.tar
│   ├── Oracle.cert
│   └── Tests
├── ocsepp.mf
├── Scripts
│   ├── ocsepp_alertrules_promha_25.1.202.yaml
│   ├── ocsepp_configuration_openapi_25.1.202.yaml
│   ├── ocsepp_custom_values_25.1.202.yaml
│   ├── ocsepp_custom_values_roaming_hub_25.1.202.yaml
│   ├── ocsepp_dashboard_25.1.202.json
│   ├── ocsepp_dashboard_promha_25.1.202.json
│   ├── ocsepp_network_policies_custom_values_25.1.202.yaml
│   ├── ocsepp-servicemesh-config-25.1.202.tgz
│   ├── ocsepp_alertrules_25.1.202.yaml
│   ├── ocsepp_mib_25.1.202.mib
│   ├── ocsepp_mib_tc_25.1.202.mib
│   ├── toplevel.mib
│   ├── ocsepp_oci_alertrules_25.1.202.zip
│   ├── ocsepp_oci_dashboard_25.1.202.json
│   ├── ocsepp_rollback_schema_25.1.202.sql
│   ├── ocsepp_dbtier_25.1.202_custom_values_25.1.202.yaml
│   └── ocsepp_single_service_account_config_25.1.202.yaml
└── TOSCA-Metadata
    └── TOSCA.meta
```

4. Open the `Files` folder based on the container engine installed, run one of the following command to load the SEPP images. Load all the images that are listed in Roaming Hub or Hosted SEPP(2-19) Table:

   ```
   podman load --input /IMAGE_PATH/<microservicename-releasenumber>.tar

   docker load --input /IMAGE_PATH/<microservicename-releasenumber>.tar
   ```

   Where, IMAGE_PATH is the location where the SEPP docker image tar file is archived.

   Sample command:

   ```
   podman load --input /IMAGE_PATH/ocsepp-pn32c-svc-25.1.202.tar
   ```

   > **Note**
   >
   > The docker/ podman load command needs to be executed seperately for each tar file/ docker image.

5. Run one of the following commands to verify that the image is loaded:

   ```
   docker images | grep ocsepp


   podman images | grep ocsepp
   ```

> **Note**
>
> Verify the list of images shown in the output with the list of images shown in the table SEPP Images. If the list does not match, reload the image tar file.

6. Run one of the following commands to tag the images to the registry:

```
docker tag <image-name>:<image-tag> <docker-repo>/<image-name>:<image-tag>
```

```
podman tag <image-name>:<image-tag> <docker-repo>/<image-name>:<image-tag>
```

Sample Tag commands:

```
podman tag alternate_route:25.1.206 <customer repo>/
alternate_route:25.1.206
podman tag common_config_hook:25.1.202 <customer repo>/
common_config_hook:25.1.202
podman tag configurationinit:25.1.202 <customer repo>/
configurationinit:25.1.202
podman tag configurationupdate:25.1.202 <customer repo>/
configurationupdate:25.1.202
podman tag mediation/ocmed-nfmediation:25.1.107 <customer repo>/mediation/
ocmed-nfmediation:25.1.107
podman tag nf_test:25.1.202 <customer repo>/nf_test:25.1.202
podman tag nrf-client:25.1.204 <customer repo>/nrf-client:25.1.204
podman tag occnp/oc-app-info:25.1.204 <customer repo>/occnp/oc-app-
info:25.1.202
podman tag occnp/oc-config-server:25.1.204 <customer repo>/occnp/oc-config-
server:25.1.204
podman tag occnp/oc-perf-info:25.1.204 <customer repo>/occnp/oc-perf-
info:25.1.204
podman tag ocdebugtool/ocdebug-tools:25.1.203 <customer repo>/ocdebugtool/
ocdebug-tools:25.1.203
podman tag ocegress_gateway:25.1.206 <customer repo>/
ocegress_gateway:25.1.206
podman tag ocingress_gateway:25.1.206 <customer repo>/
ocingress_gateway:25.1.206
podman tag ocsepp-cn32c-svc:25.1.202 <customer repo>/ocsepp-cn32c-
svc:25.1.202
podman tag ocsepp-cn32f-svc:25.1.202 <customer repo>/ocsepp-cn32f-
svc:25.1.202
podman tag ocsepp-coherence-svc:25.1.202 <customer repo>/ocsepp-coherence-
svc:25.1.202
podman tag ocsepp-config-mgr-svc:25.1.202 <customer repo>/ocsepp-config-
mgr-svc:25.1.202
podman tag ocsepp-pn32c-svc:25.1.202 <customer repo>/ocsepp-pn32c-
svc:25.1.202
podman tag ocsepp-pn32f-svc:25.1.202 <customer repo>/ocsepp-pn32f-
svc:25.1.202
podman tag ocsepp-pre-install-hook:25.1.202 <customer repo>/ocsepp-pre-
install-hook:25.1.202
```

```
podman tag ocsepp-update-db:25.1.202 <customer repo>/ocsepp-update-
db:25.1.202
```

7. Run one of the following commands to push the image to the registry:

```
docker push <docker-repo>/<image-name>:<image-tag>

podman push <docker-repo>/<image-name>:<image-tag>
```

Sample push commands:

```
podman push occne-repo-host:5000/alternate_route:25.1.206
podman push occne-repo-host:5000/common_config_hook:25.1.202
podman push occne-repo-host:5000/configurationinit:25.1.202
podman push occne-repo-host:5000/configurationupdate:25.1.202
podman push occne-repo-host:5000/mediation/ocmed-nfmediation:25.1.107
podman push occne-repo-host:5000/nf_test:25.1.202
podman push occne-repo-host:5000/nrf-client:25.1.204
podman push occne-repo-host:5000/occnp/oc-app-info:25.1.204
podman push occne-repo-host:5000/occnp/oc-config-server:25.1.204
podman push occne-repo-host:5000/occnp/oc-perf-info:25.1.204
podman push occne-repo-host:5000/ocdebugtool/ocdebug-tools:25.1.203
podman push occne-repo-host:5000/ocegress_gateway:25.1.206
podman push occne-repo-host:5000/ocingress_gateway:25.1.206
podman push occne-repo-host:5000/ocsepp-cn32c-svc:25.1.202
podman push occne-repo-host:5000/ocsepp-cn32f-svc:25.1.202
podman push occne-repo-host:5000/ocsepp-coherence-svc:25.1.202
podman push occne-repo-host:5000/ocsepp-config-mgr-svc:25.1.202
podman push occne-repo-host:5000/ocsepp-pn32c-svc:25.1.202
podman push occne-repo-host:5000/ocsepp-pn32f-svc:25.1.202
podman push occne-repo-host:5000/ocsepp-pre-install-hook:25.1.202
podman push occne-repo-host:5000/ocsepp-update-db:25.1.202
```

> **Note**
>
> - It is recommended to configure the Docker certificate before running the push command to access customer registry through HTTPS, otherwise, docker push command may fail.

2.2.1.4 Pushing the SEPP Images to OCI Docker Registry

SEPP deployment package includes ready-to-use images and Helm charts to orchestrate containers in Kubernetes.

The following table lists the docker images for SEPP:

Table 2-21 SEPP Images

Services	Image	Tag
<helm-release-name>-alternate_route	alternate_route	25.1.206
<helm-release-name>-common_config_hook	common_config_hook	25.1.202

Table 2-21 (Cont.) SEPP Images

Services	Image	Tag
<helm-release-name>-configurationinit	configurationinit	25.1.200
<helm-release-name>-mediation/ocmed-nfmediation	mediation/ocmed-nfmediation	25.1.107
<helm-release-name>-nf_test	nf_test	25.1.202
<helm-release-name>-nrf-client	nrf-client	25.1.204
<helm-release-name>-occnp/oc-app-info	occnp/oc-app-info	25.1.204
<helm-release-name>-occnp/oc-config-server	occnp/oc-config-server	25.1.204
<helm-release-name>-performance	occnp/oc-perf-info	25.1.204
<helm-release-name>-ocdebugtool/ocdebug-tools	ocdebugtool/ocdebug-tools	25.1.203
<helm-release-name>-ocegress_gateway	ocegress_gateway	25.1.206
<helm-release-name>-ocingress_gateway	ocingress_gateway	25.1.206
<helm-release-name>-oocsepp-cn32c-svc	ocsepp-cn32c-svc	25.1.200
<helm-release-name>- ocsepp-cn32f-svc	ocsepp-cn32f-svc	25.1.200
<helm-release-name>-ocsepp-coherence-svc	ocsepp-coherence-svc	25.1.200
<helm-release-name>-ocsepp-config-mgr-svc	ocsepp-config-mgr-svc	25.1.200
<helm-release-name>-ocsepp-pn32c-svc	ocsepp-pn32c-svc	25.1.200
<helm-release-name>-ocsepp-pn32f-svc	ocsepp-pn32f-svc	25.1.200
<helm-release-name>-ocsepp-pre-install-hook	ocsepp-pre-install-hook	25.1.200
<helm-release-name>-ocsepp-update-db	ocsepp-update-db	25.1.200
<helm-release-name>-ocsepp-configurationupdate	configurationupdate	25.1.200

To push the images to the registry:

1. Navigate to the location where you want to install SEPP. Unzip the SEPP release package (<p********>_<release_number>_Tekelec.zip) to retrieve the following CSAR package. The SEPP package is as follows:

   ```
   ReleaseName_csar_Releasenumber.zip
   ```

   Where,

   - ReleaseName is a name that is used to track this installation instance.
   - Releasenumber is the release number.

     For example:

   ```
   ocsepp_csar_25_1_202_0_0.zip
   ```

2. Unzip the SEPP package file to get SEPP docker image tar file:

   ```
   unzip ocsepp_csar_Releasenumber.zip
   ```

   For example:

   ```
   unzip ocsepp_csar_25_1_202_0_0.zip
   ```

3. The directory `ocsepp_csar_25_1_202_0_0.zip` consists of the following:

```
├─── Definitions
│    ├─── ocsepp_cne_compatibility.yaml
│    └─── ocsepp.yaml
├─── Files
│    ├─── alternate_route-25.1.206.tar
│    ├─── ChangeLog.txt
│    ├─── common_config_hook-25.1.202.tar
│    ├─── configurationinit-25.1.202.tar
│    ├─── Helm
│    │    ├─── ocsepp-25.1.202.tgz
│    │    ├─── ocsepp-network-policy-25.1.202.tgz
│    │    └─── ocsepp-servicemesh-config-25.1.202.tgz
│    ├─── Licenses
│    ├─── mediation-ocmed-nfmediation-25.1.107.tar
│    ├─── nf_test-25.1.202.tar
│    ├─── nrf-client-25.1.204.tar
│    ├─── occnp-oc-app-info-25.1.204.tar
│    ├─── occnp-oc-config-server-25.1.204.tar
│    ├─── occnp-oc-perf-info-25.1.204.tar
│    ├─── ocdebugtool-ocdebug-tools-25.1.203.tar
│    ├─── ocegress_gateway-25.1.206.tar
│    ├─── ocingress_gateway-25.1.206.tar
│    ├─── ocsepp-cn32c-svc-25.1.202.tar
│    ├─── ocsepp-cn32f-svc-25.1.202.tar
│    ├─── ocsepp-coherence-svc-25.1.202.tar
│    ├─── ocsepp-config-mgr-svc-25.1.202.tar
│    ├─── ocsepp-pn32c-svc-25.1.202.tar
│    ├─── ocsepp-pn32f-svc-25.1.202.tar
│    ├─── ocsepp-pre-install-hook-25.1.202.tar
│    ├─── ocsepp-update-db-25.1.202.tar
│    ├─── Oracle.cert
│    └─── Tests
├─── ocsepp.mf

├─── Scripts
│    ├─── ocsepp_alertrules_promha_25.1.202.yaml
│    ├─── ocsepp_configuration_openapi_25.1.202.yaml
│    ├─── ocsepp_custom_values_25.1.202.yaml
│    ├─── ocsepp_custom_values_roaming_hub_25.1.202.yaml
│    ├─── ocsepp_dashboard_25.1.202.json
│    ├─── ocsepp_dashboard_promha_25.1.202.json
│    ├─── ocsepp_network_policies_custom_values_25.1.202.yaml
│    ├─── ocsepp-servicemesh-config-25.1.202.tgz
│    ├─── ocsepp_alertrules_25.1.202.yaml
│    ├─── ocsepp_mib_25.1.202.mib
│    ├─── ocsepp_mib_tc_25.1.202.mib
│    └─── toplevel.mib
│    └─── ocsepp_oci_alertrules_25.1.202.zip
│    └─── ocsepp_oci_dashboard_25.1.202.json
│    └─── ocsepp_rollback_schema_25.1.202.sql
│    └─── ocsepp_dbtier_25.1.200_custom_values_25.1.202.yaml
│    └─── ocsepp_single_service_account_config_25.1.202.yaml
└─── TOSCA-Metadata
     └─── TOSCA.meta
```

4. Open the `Files` folder and based on the container engine installed, run one of the following command to load the SEPP images. Load all the images that are listed in SEPP Images Table:

```
podman load --input /IMAGE_PATH/<microservicename-releasenumber>.tar
```

```
docker load --input /IMAGE_PATH/<microservicename-releasenumber>.tar
```

Where, IMAGE_PATH is the location where the SEPP docker image tar file is archived.

Sample command:

```
podman load --input /IMAGE_PATH/ocsepp-pn32c-svc-25.1.202.tar
```

> **Note**
>
> The docker/podman load command needs to be executed seperately for each tar file/docker image.

5. Run one of the following commands to verify that the image is loaded:

```
docker images | grep ocsepp
```

```
podman images | grep ocsepp
```

> **Note**
>
> Verify the list of images shown in the output with the list of images shown in the table SEPP Images. If the list does not match, reload the image tar file.

6. Run the following commands to log in to the OCI Docker registry:

```
podman login -u <REGISTRY_USERNAME> -p <REGISTRY_PASSWORD> <REGISTRY_NAME>
```

```
docker login -u <REGISTRY_USERNAME> -p <REGISTRY_PASSWORD> <REGISTRY_NAME>
```

where,

- REGISTRY_NAME is `<Region_Key>.ocir.io`
- REGISTRY_USERNAME is `<Object Storage Namespace>/<identity_domain>/email_id`
- REGISTRY_PASSWORD is the Auth token generated by the user.

For more information about OCIR configuration and creating auth token, see *Cloud Native Core OCI Adaptor, NF Deployment in OCI Guide*.

- `<Object Storage Namespace>` is configured in OCI Console. To access it, navigate to **OCI Console> Governanace & Administration> Account Management> Tenenancy Details> Object Storage Namespace**.
- `<Identity Domain>` is the domain where the user currently is present.
- In OCI, each region is associated with a key. For the details about the `<Region_Key>`, refer to Regions and Availability Domains.

7. Run one of the following commands to tag the images to the registry:

```
docker tag <image-name>:<image-tag> <REGISTRY_NAME>/<Object Storage
Namespace>/<image-name>:<image-tag>
```

```
podman tag <image-name>:<image-tag> <REGISTRY_NAME>/<Object Storage
Namespace>/<image-name>:<image-tag>
```

Sample Tag commands:

```
podman tag alternate_route:25.1.206 <customer repo>/
alternate_route:25.1.206
podman tag common_config_hook:25.1.202 <customer repo>/
common_config_hook:25.1.202
podman tag configurationinit:25.1.200 <customer repo>/
configurationinit:25.1.200
podman tag configurationupdate:25.1.200 <customer repo>/
configurationupdate:25.1.200
podman tag mediation/ocmed-nfmediation:25.1.107 <customer repo>/mediation/
ocmed-nfmediation:25.1.107
podman tag nf_test:25.1.202 <customer repo>/nf_test:25.1.202
podman tag nrf-client:25.1.204 <customer repo>/nrf-client:25.1.204
podman tag occnp/oc-app-info:25.1.204 <customer repo>/occnp/oc-app-
info:25.1.204
podman tag occnp/oc-config-server:25.1.204 <customer repo>/occnp/oc-config-
server:25.1.204
podman tag occnp/oc-perf-info:25.1.204 <customer repo>/occnp/oc-perf-
info:25.1.204
podman tag ocdebugtool/ocdebug-tools:25.1.203 <customer repo>/ocdebugtool/
ocdebug-tools:25.1.203
podman tag ocegress_gateway:25.1.206 <customer repo>/
ocegress_gateway:25.1.206
podman tag ocingress_gateway:25.1.206 <customer repo>/
ocingress_gateway:25.1.206
podman tag ocsepp-cn32c-svc:25.1.200 <customer repo>/ocsepp-cn32c-
svc:25.1.200
podman tag ocsepp-cn32f-svc:25.1.200 <customer repo>/ocsepp-cn32f-
svc:25.1.200
podman tag ocsepp-coherence-svc:25.1.200 <customer repo>/ocsepp-coherence-
svc:25.1.200
podman tag ocsepp-config-mgr-svc:25.1.200 <customer repo>/ocsepp-config-
mgr-svc:25.1.200
podman tag ocsepp-pn32c-svc:25.1.200 <customer repo>/ocsepp-pn32c-
svc:25.1.200
podman tag ocsepp-pn32f-svc:25.1.200 <customer repo>/ocsepp-pn32f-
svc:25.1.200
podman tag ocsepp-pre-install-hook:25.1.200 <customer repo>/ocsepp-pre-
install-hook:25.1.200
podman tag ocsepp-update-db:25.1.200 <customer repo>/ocsepp-update-
db:25.1.200
```

8. Run one of the following commands to push the image to the registry:

```
docker push <REGISTRY_NAME>/<Object Storage Namespace>/<image-name>:<image-tag>
```

```
podman push <REGISTRY_NAME>/<Object Storage Namespace>/<image-name>:<image-tag
```

Sample push commands:

```
podman push occne-repo-host:5000/alternate_route:25.1.206
podman push occne-repo-host:5000/common_config_hook:25.1.202
podman push occne-repo-host:5000/configurationinit:25.1.200
podman push occne-repo-host:5000/configurationupdate:25.1.200
podman push occne-repo-host:5000/mediation/ocmed-nfmediation:25.1.107
podman push occne-repo-host:5000/nf_test:25.1.202
podman push occne-repo-host:5000/nrf-client:25.1.204
podman push occne-repo-host:5000/occnp/oc-app-info:25.1.204
podman push occne-repo-host:5000/occnp/oc-config-server:25.1.204
podman push occne-repo-host:5000/occnp/oc-perf-info:25.1.204
podman push occne-repo-host:5000/ocdebugtool/ocdebug-tools:25.1.203
podman push occne-repo-host:5000/ocegress_gateway:25.1.206
podman push occne-repo-host:5000/ocingress_gateway:25.1.206
podman push occne-repo-host:5000/ocsepp-cn32c-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-cn32f-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-coherence-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-config-mgr-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-pn32c-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-pn32f-svc:25.1.200
podman push occne-repo-host:5000/ocsepp-pre-install-hook:25.1.200
podman push occne-repo-host:5000/ocsepp-update-db:25.1.200
```

9. All the image repositories must be public. Run the following steps to make all image repositories public:
   a. Log in to OCI Console. Navigate to **OCI Console> Developer Services > Containers & Artifacts> Container Registry.**
   b. Select the root Compartment.
   c. In the **Repositories and Images** Seach option, the images will be listed. Select each image and click **Change to Public.** This step must be performed for all the images sequentially.

2.2.1.5 Verifying and Creating Namespace

This section explains how to verify and create a namespace in the system.

> **Note**
>
> This is a mandatory procedure, run this before proceeding further with the installation. The namespace created or verified in this procedure is an input for the next procedures.

To verify and create a namespace:

1. Run the following command to verify if the required namespace already exists in system:

```
kubectl get namespaces
```

In the output of the above command, if the namespace exists, continue with the Creating Service Account, Role and RoleBinding section.

2. If the required namespace is not available, create the namespace using the following command:

   ```
   kubectl create namespace <required namespace>
   ```

   Example:

   ```
   kubectl create namespace seppsvc
   ```

   Sample output:

   ```
   namespace/seppsvc created
   ```

3. Update the namespace in the `ocsepp custom-values.yaml` file with the namespace created in the previous step.

   Example:

   Run the following kubectl command create the namespace seppsvc:

   ```
   kubectl create namespace seppsvc
   ```

   update the parameters : global: nameSpace: seppsvc # NameSpace where secret is deployed nameSpace: seppsvc

Naming Convention for Namespace

The namespace should:

- start and end with an alphanumeric character.
- contain 63 characters or less.
- contain only alphanumeric characters or '-'.

> **Note**
>
> It is recommended to avoid using the prefix `kube-` when creating a namespace. The prefix is reserved for Kubernetes system namespaces.

2.2.1.6 Creating Service Account, Role, and RoleBinding

This section explains how to create and use a single service account, role, and rolebinding resources which can be used by all the microservices of SEPP. This is an optional procedure and is only needed, if the user wants to use a single service account, role,and rolebinding by all the microservices of SEPP.

1. Create a OCSEPP resource file:

   ```
   vi <ocsepp-resource-file>
   ```

Example:

```
vi ocsepp_single_service_account_config_<version>.yaml
```

2. Update the `ocsepp_single_service_account_config_<version>.yaml` file with the correct namespace by replacing seppsvc with the user defined SEPP's namespace:

> **Note**
>
> The user have an option to update the name of service account, role, and rolebinding.

> **Note**
>
> If SEPP is deployed with ASM, the user must add the following annotation in the single service account: `certificate.aspenmesh.io/customFields: '{ "SAN": { "DNS": [<SEPP inter PLMN FQDN>, <SEPP intra PLMN FQDN>], "URI": [<SEPP inter PLMN FQDN>, <SEPP intra PLMN FQDN>] } }`
> Example:
>
> ```
> apiVersion: v1
> kind: ServiceAccount
> metadata:
>   annotations:
>     certificate.aspenmesh.io/customFields: '{ "SAN": { "DNS":
> [sepp1.inter.oracle.com, sepp1.intra.oracle.com], "URI":
> [sepp1.inter.oracle.com, sepp1.intra.oracle.com] } }'
>   name: sepp-sa
>   namespace: seppsvc
> ```

```
#sa-role-rolebinding.yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  annotations: {}
  labels: {}
  name: sepp-sa
  namespace: seppsvc

---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  annotations: {}
  labels: {}
  name: sepp-role
  namespace: seppsvc
rules:
```

```
- apiGroups:
  - ""
  resources:
  - services
  - configmaps
  - pods
  - secrets
  - endpoints
  - persistentvolumeclaims
  - pods/exec
  - serviceaccounts
  verbs:
  - get
  - watch
  - list
  - update
  - delete
  - deletecollection
  - create
  - patch
# for cnDBtier
- apiGroups:
  - apps
  resources:
  - deployments
  - statefulsets
  - replicasets
  verbs:
  - get
  - watch
  - list
  - update
  - delete
  - create
  - patch
- apiGroups:
  - autoscaling
  resources:
  - horizontalpodautoscalers
  verbs:
  - get
  - watch
  - list
  - update
# for job deletion
- apiGroups:
  - batch
  resources:
  - jobs
  verbs:
  - get
  - delete
- apiGroups:
  - ""
  resources:
  - events
```

```
  - pods/log
  verbs:
  - get
  - watch
  - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  annotations: {}
  labels: {}
  name: sepp-rolebinding
  namespace: seppsvc
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: sepp-role
subjects:
- kind: ServiceAccount
  name: sepp-sa
  namespace: seppsvc
```

3. Run the following command to create service account, role, and role binding:

   ```
   $ kubectl -n <SEPP namespace> create -f
   ocsepp_single_service_account_config_<version>.yaml
   ```

   For example:

   ```
   $ kubectl -n seppsvc create -f
   ocsepp_single_service_account_config_<version>.yaml
   ```

4. Update the `serviceAccountName` parameter in the `ocsepp_custom_values_<version>.yaml` file.

2.2.1.7 Configuring Database, Creating Users, and Granting Permissions

This section explains how database administrators can create users and database in a single and multisite deployment.

SEPP supports single database (provisional Database) and single type of user.

> **Note**
>
> - Before running the procedure for georedundant sites, ensure that the cnDBTier for georedundant sites is up and replication channels are enabled.
> - While performing a fresh installation, if SEPP is already deployed, purge the deployment and remove the database and users that were used for the previous deployment. For uninstallation procedure, see Uninstalling SEPP.
> - To install cnDBTier, refer *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

cnDBTier Parameter Values

For Single Cluster, Single Instance (Single SEPP Instances on Dedicated cnDBTier Cluster) deployment model, the cnDBTier resources can be taken from `ocsepp_dbtier_<cnDBTier_version>_custom_values_<SEPP_version>.yaml` file.

Example: `ocsepp_dbtier_25.1.200_custom_values_25.1.201.yaml`

For Single Cluster, Multiple Instance (multiple SEPP instances on shared cnDBTier cluster), the cnDBTier parameters from cnDBTier Parameter Values Table should be updated in `ocsepp_dbtier_<cnDBTier_version>_custom_values_<SEPP_version>.yaml` file.

> **Note**
>
> Verify the value of the following parameters before deploying SEPP in 1+1 site GR with single cluster, multiple instance.

Table 2-22 cnDBTier Parameter Values

Parameter	Default Values (in CV file)	New Values (to be Updated in CV file)
MaxNoOfTables	1024	3000
MaxNoOfAttributes	5000	24000
MaxNoOfOrderedIndexes	1024	3700

SEPP Users

SEPP supports a single type of user:

This user has a complete set of permissions. This user can perform create, alter, or drop operations on tables to perform install, upgrade, rollback, or delete operations.

SEPP Database

SEPP Database contains configuration information. The same configuration must be done on each site by the operator. In case of multisite georedundant setups, each site must have a unique SEPP Database, which is replicated to other sites. SEPP sites can access only the information in their unique provisional database.

For example:

- For Site 1: seppdb_site_1

- For Site 2: seppdb_site_1
- For Site 3: seppdb_site_1

2.2.1.7.1 Single Site

This section explains how database administrator can create the database, users, and grant permissions to the users for single SEPP site.

Follow the below steps to manually create SEPP Database and MySQL user required for the deployment:

1. Log in to the machine that has permission to access the SQL nodes of NDB cluster.
2. Run the following command to log in to one of the `ndbappmysqld` node pods of the primary NDB cluster:

   Connect to the SQL nodes.

   ```
   kubectl exec -it ndbappmysqld-0 -n <cndb-namespace> -- bash
   ```

   where, `cndb-namespace` is the namespace in which cnDBTier is installed.
3. Log in to the MySQL prompt using root permission or user, which has permission to create users with conditions as mentioned (in the next step):

   Example:

   ```
   mysql -h127.0.0.1 -uroot -p<rootPassword>
   ```

   > **Note**
   >
   > This command varies between systems, path for MySQL binary, root user, and root password. After running this command, enter the password specific to the user mentioned in the command.

4. Check whether OCSEPP database user already exists. If the user does not exist, create an OCSEPP database user by running the following queries:
   a. Run the following command to to list the users:

      ```
      $ SELECT User FROM mysql.user;
      ```

   b. If the SEPP user does not exist, run the following command to create the new user :

      ```
      $ CREATE USER IF NOT EXISTS '<OCSEPP User Name>'@'%' IDENTIFIED BY
      '<OCSEPP User Password>';
      ```

      Example:

      ```
      $ CREATE USER IF NOT EXISTS 'seppusr'@'%' IDENTIFIED BY 'sepppasswd';
      ```

> **Note**
>
> You must create the user on all the SQL nodes for all georedundant sites.

5. Check if OCSEPP database already exists. If it does not exist, run the following commands to create an OCSEPP database and provide permissions to OCSEPP username created in the previous step:

> **Note**
>
> **Naming Convention for SEPP Database**
>
> As the SEPP instances cannot share the same database, user must provide a unique name to the SEPP database in the cnDBTier. The recommended format for SEPP database and SEPP-backup database name is as follows:
>
> `<database-name>_<site-name>_<NF_INSTANCE_ID>` where "-" in NF_INSTANCE_ID is replaced by "_".
>
> Example: seppdb_site1_9faf1bbc_6e4a_4454_a507_aef01a101a06
>
> The name of the database must:
>
> - starts and ends with an alphanumeric character
> - contains a maximum of 63 characters
> - contains only alphanumeric characters or '_'

   a. Run the following command to check if database exists:

      ```
      $ show databases;
      ```

   b. If database does not exist, run the following command for database creation:

      ```
      $ CREATE DATABASE IF NOT EXISTS <OCSEPP Database>;
      ```

      Example:

      ```
      $ CREATE DATABASE IF NOT EXISTS seppdb;
      ```

   c. If backup database does not exist, run the following command for database creation:

      ```
      $ CREATE DATABASE IF NOT EXISTS <OCSEPP Backup Database>;
      ```

      Example:

      ```
      CREATE DATABASE IF NOT EXISTS seppbackupdb;
      ```

> **Note**
>
> Ensure that you use the same database names while creating database that you have used in the global parameters of `ocsepp_custom_values_<version>.yaml` file. Following is an example of what are the database names configured in the `ocsepp_custom_values_<version>.yaml` file:
>
> ```
> global:seppDbName: "seppdb"
> global:leaderPodDbName: "seppdb"
> global:networkDbName: "seppdb"
> global:nrfClientDbName: "seppdb"
>
> Backup Database
>   global:seppBackupDbName: "seppbackupdb"
> ```

6. a. Run the following command to grant permission to user to SEPP Database:

   ```
   $ GRANT SELECT,INSERT,CREATE,ALTER,DROP,LOCK TABLES,CREATE TEMPORARY
   TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON <OCSEPP Database>.* TO
   '<OCSEPP User Name>'@'%';
   ```

   Example:

   ```
   GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE
   TEMPORARY TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON seppdb.* TO
   'seppusr'@'%';
   ```

   b. Run the following command to grant permission to user for SEPP backup db:

   ```
   $ GRANT SELECT,INSERT,CREATE,ALTER,DROP,LOCK TABLES,CREATE TEMPORARY
   TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON <OCSEPP backup Database>.*
   TO '<OCSEPP User Name>'@'%';
   ```

   Example:

   ```
   GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE
   TEMPORARY TABLES, DELETE, UPDATE, REFERENCES, EXECUTE ON seppbackupdb.*
   TO 'seppusr'@'%';
   ```

   c. Run the following command to grant permission for MySQL db:

   ```
   $ GRANT SELECT,INSERT,CREATE,ALTER,DROP,LOCK TABLES,CREATE TEMPORARY
   TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON mysql.* TO '<OCSEPP User
   Name>'@'%';
   ```

Example:

```
GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE
TEMPORARY TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON mysql.* TO
'seppusr'@'%';
```

7. Run the following command to grand the permission to NDB_STORED_USER:

   ```
   GRANT NDB_STORED_USER ON *.* TO '<OCSEPP User Name>'@'%' WITH GRANT OPTION;
   ```

   Example:

   ```
   GRANT NDB_STORED_USER ON *.* TO 'seppusr'@'%' WITH GRANT OPTION;
   ```

8. Run the following command to flush the privileges:

   ```
   flush privileges;
   ```

9. Run the following command to verify SEPP database grants were correctly created:

   ```
   show grants for '<sepp user>'@'%';
   ```

   Example:

   ```
   show grants for 'seppusr'@'%';

   +-----------------------------------------------------------------------------
   ------------------------------------------------------------------------------
   ------+
   | Grants for seppusr@% |
   +-----------------------------------------------------------------------------
   ------------------------------------------------------------------------------
   ------+
   | GRANT USAGE ON *.* TO `seppusr`@`%` |
   | GRANT NDB_STORED_USER ON *.* TO `seppusr`@`%` WITH GRANT OPTION |
   | GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
   CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE ON `mysql`.* TO
   `seppusr`@`%` |
   | GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
   CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE ON `seppbackupdb`.* TO
   `seppusr`@`%` |
   | GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
   CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE ON `seppdb`.* TO
   `seppusr`@`%` |
   +-----------------------------------------------------------------------------
   ------------------------------------------------------------------------------
   ------+
   ```

10. Exit from MySQL prompt and SQL nodes.

2.2.1.7.2 Multisite

This section explains how database administrator can create the database, users, and grant permissions to the users for multisite deployment.

Follow the below steps to manually create SEPP Database and MySQL user required for the deployment:

1. Log in to the machine that has permission to access the SQL nodes of NDB cluster.
2. Run the following command to log in to one of the `ndbappmysqld` node pods of the primary NDB cluster:

   Connect to the SQL nodes.

   ```
   kubectl exec -it ndbappmysqld-0 -n <cndb-namespace> -- bash
   ```

   where, `cndb-namespace` is the namespace in which CNDB is installed.
3. Log in to the MySQL prompt using root permission or user, which has permission to create users with conditions as mentioned (in the next step):

   Example:

   ```
   mysql -h127.0.0.1 -uroot -p<rootPassword>
   ```

   > **Note**
   >
   > This command varies between systems, path for MySQL binary, root user, and root password. After running this command, enter the password specific to the user mentioned in the command.

4. Check whether SEPP database user already exists. If the user does not exist, create an SEPP database user by running the following queries:
   a. Run the following command to to list the users:

      ```
      $ SELECT User FROM mysql.user;
      ```

   b. If the SEPP user does not exist, run the following command to create the new user :

      ```
      $ CREATE USER IF NOT EXISTS '<OCSEPP User Name>'@'%' IDENTIFIED BY
      '<OCSEPP User Password>';
      ```

      Example:

      ```
      $ CREATE USER IF NOT EXISTS 'seppusr'@'%' IDENTIFIED BY 'sepppasswd';
      ```

   > **Note**
   >
   > You must create the user on all the SQL nodes for all georedundant sites.

5. Check if SEPP database already exists. If it does not exist, run the following commands to create an SEPP database and provide permissions to SEPP username created in the previous step:

> **Note**
>
> **Naming Convention for SEPP Database**
>
> As the SEPP instances cannot share the same database, user must provide a unique name to the SEPP database in the cnDBTier. The recommended format for SEPP database and SEPP-backup database name is as follows:
>
> `<database-name>_<site-name>_<NF_INSTANCE_ID>` where "-" in NF_INSTANCE_ID is replaced by "_".
>
> Example: seppdb_site1_9faf1bbc_6e4a_4454_a507_aef01a101a06
>
> The name of the database must:
>
> - starts and ends with an alphanumeric character
> - contains a maximum of 63 characters
> - contains only alphanumeric characters or '_'

> **Note**
>
> Create database for each site. For Site-2 or Site-3, ensure that the database name is different from the previous site names.

a. Run the following command to check if database exists:

```
$ show databases;
```

b. If database does not exist, run the following command for database creation:

```
$ CREATE DATABASE IF NOT EXISTS <OCSEPP Database>;
```

Example:

```
$ CREATE DATABASE IF NOT EXISTS seppdb;
```

c. If backup database does not exist, run the following command for database creation:

```
$ CREATE DATABASE IF NOT EXISTS <SEPP Backup Database>;
```

Example:

```
CREATE DATABASE IF NOT EXISTS seppbackupdb;
```

> **Note**
>
> Ensure that you use the same database names while creating database that you have used in the global parameters of `ocsepp_custom_values_<version>.yaml` file. Following is an example of what are the database names configured in the `ocsepp_custom_values_<version>.yaml` file:
>
> ```
> global:seppDbName: "seppdb"
> global:leaderPodDbName: "seppdb"
> global:networkDbName: "seppdb"
> global:nrfClientDbName: "seppdb"
>
> Backup Database
>   global:seppBackupDbName: "seppbackupdb"
> ```

6. a. Run the following command to grant permission to user to SEPP DB:

   ```
   $ GRANT SELECT,INSERT,CREATE,ALTER,DROP,LOCK TABLES,CREATE TEMPORARY
   TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON <OCSEPP Database>.* TO
   '<OCSEPP User Name>'@'%';
   ```

   Example:

   ```
   GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE
   TEMPORARY TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON seppdb.* TO
   'seppusr'@'%';
   ```

   b. Run the following command to grant permission to user for backup db:

   ```
   $ GRANT SELECT,INSERT,CREATE,ALTER,DROP,LOCK TABLES,CREATE TEMPORARY
   TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON <OCSEPP backup Database>.*
   TO '<OCSEPP User Name>'@'%';
   ```

   Example:

   ```
   GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE
   TEMPORARY TABLES, DELETE, UPDATE, REFERENCES, EXECUTE ON seppbackupdb.*
   TO 'seppusr'@'%';
   ```

   c. Run the following command to grant permission for MySQL db:

   ```
   $ GRANT SELECT,INSERT,CREATE,ALTER,DROP,LOCK TABLES,CREATE TEMPORARY
   TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON mysql.* TO '<OCSEPP User
   Name>'@'%';
   ```

Example:

```
GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE
TEMPORARY TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON mysql.* TO
'seppusr'@'%';
```

7. Run the following command to grand the permission to NDB_STORED_USER:

   ```
   GRANT NDB_STORED_USER ON *.* TO '<OCSEPP User Name>'@'%' WITH GRANT OPTION;
   ```

   Example:

   ```
   GRANT NDB_STORED_USER ON *.* TO 'seppusr'@'%' WITH GRANT OPTION;
   ```

8. Run the following command to flush the privileges:

   ```
   flush privileges;
   ```

9. Run the following command to verify SEPP database grants were correctly created:

   ```
   show grants for '<sepp user>'@'%';
   ```

   Example:

   ```
   show grants for 'seppusr'@'%';

   +-----------------------------------------------------------------------------
   ------------------------------------------------------------------------------
   ------+
   | Grants for seppusr@% |
   +-----------------------------------------------------------------------------
   ------------------------------------------------------------------------------
   ------+
   | GRANT USAGE ON *.* TO `seppusr`@`%` |
   | GRANT NDB_STORED_USER ON *.* TO `seppusr`@`%` WITH GRANT OPTION |
   | GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
   CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE ON `mysql`.* TO
   `seppusr`@`%` |
   | GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
   CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE ON `seppbackupdb`.* TO
   `seppusr`@`%` |
   | GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, ALTER,
   CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE ON `seppdb`.* TO
   `seppusr`@`%` |
   +-----------------------------------------------------------------------------
   ------------------------------------------------------------------------------
   ------+
   ```

10. Exit from MySQL prompt and SQL nodes.

2.2.1.8 Configuring Kubernetes Secrets for Accessing Database

This section explains how to configure Kubernetes secrets for accessing SEPP database.

1. Run the following command to create a Kubernetes secret for the SEPP users:

   ```
   kubectl create secret generic <OCSEPP User secret name> --from-
   literal=mysql-username=<OCSEPP MySQL Database User Name> --from-
   literal=mysql-password=<OCSEPP Mysql User Password > -n <Namespace>
   ```

   Where,

   - <OCSEPP User secret name> is the secret name of the user.
   - <OCSEPP MySQL Database User Name> is the username of the ocsepp MySQL user.
   - <OCSEPP MySQL User Password> is the password of the ocsepp MySQL user.
   - <Namespace> is the namespace of SEPP deployment.

   > **Note**
   >
   > Note down the command used during the creation of Kubernetes secret. This command is used for updating the secrets in future.

   Example:

   ```
   $ kubectl create secret generic ocsepp-mysql-cred  --from-literal=mysql-
   username=seppusr --from-literal=mysql-password=sepppasswd  -n seppsvc
   ```

2. Run the following command to verify the secret created:

   ```
   $ kubectl describe secret <OCSEPP User secret name> -n <Namespace>
   ```

   Where,

   - <OCSEPP User secret name> is the secret name of the user.
   - <Namespace> is the namespace of SEPP deployment.

     For example:

   ```
   $ kubectl describe secret ocsepp-mysql-cred -n seppsvc
   ```

   Sample output:

   ```
   Name:  ocsepp-mysql-cred
   Namespace: seppsvc
   Labels: <none>
   Annotations: <none>
   Type: Opaque
   Data
   ====
   mysql-password: 10 bytes
   mysql-username: 7 bytes
   ```

> **Note**
>
> If the secret name is anything other than ocsepp-mysql-cred, update the following parameter values in the `ocsepp_custom_values_<version>.yaml` file before deploying:
>
> - `global:dbCredSecretName: &dbCredSecretNameRef 'ocsepp-mysql-cred'`
> - `global:privilegedDbCredSecretName: &privDbCredSecretNameRef 'ocsepp-mysql- cred'`

3. To update the Kubernetes secret, update the command used in step 1 with string "--dryrun -o yaml" and "kubectl replace -f - -n <Namespace>". After the update is performed, use the following command:

   ```
   $ kubectl create secret generic <OCSEPP User secret name> --
   fromliteral=mysql-username=<OCSEPP MySQL Database User Name> --
   fromliteral=mysql-password=<OCSEPP Mysql User Password> --dryrun -o yaml -
   n <Namespace> | kubectl replace -f - -n <Namespace>
   ```

   Where,

   - <OCSEPP User secret name> is the secret name of the user.
   - <OCSEPP MySQL Database User Name> is the username of the ocsepp MySQL user.
   - <OCSEPP MySQL User Password> is the password of the ocsepp MySQL user.
   - <Namespace> is the namespace of SEPP deployment.

4. Run the updated command. The following message is displayed:

   ```
   secret/<OCSEPP User secret name> replaced
   ```

   Where, <OCSEPP User secret name> is the updated secret name of the application user.

   Example:

   ```
   secret/ocsepp-mysql-cred replaced
   ```

2.2.1.9 Configuring Kubernetes Secret for Enabling HTTPS

This section explains the steps to configure HTTPS at Ingress and Egress Gateways.

2.2.1.9.1 Configuring Secrets at N32 Gateway (n32-egress-gateway and n32-ingress-gateway)

This section explains the steps to configure secrets for enabling HTTP over TLS in N32 Ingress and Egress Gateways. This procedure must be performed before deploying SEPP.

> **Note**
>
> The passwords for TrustStore and KeyStore are stored in respective password files.

To create Kubernetes secret for HTTP over TLS, the following files are required:

- ECDSA private key and CA signed certificate of SEPP (if initialAlgorithm is ES256)
- or, RSA private key and CA signed certificate of SEPP (if initialAlgorithm is RSA256)
- TrustStore password file
- KeyStore password file
- CA certificate

> **Note**
>
> - Creation process for private keys, certificates, and passwords is on discretion of user/operator.
> - f the certificates are not available, then create them following the instructions given in the 'Creating Private Keys and Certificates for Gateways' section.

You can manage Kubernetes secrets for enabling HTTPS in SEPP using one of the following methods:

- Managing secrets through OCCM
- Managing secrets manually

Managing Secrets Through OCCM

To create the secrets using OCCM, see "Managing Certificates" in *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

The secrets created by OCCM are then patched to add keyStore password and trustStore password files by running the following commands:

1. To patch the secrets created with the keyStore password file:

   ```
   TLS_CRT=$(base64 < "key.txt" | tr -d '\n')
   kubectl patch secret server-primary-ocsepp-secret-occm -n seppsvc -p
   "{\"data\":{\"key.txt\":\"${TLS_CRT}\"}}"
   ```

   Where,

   - `key.txt` is the password file that contains KeyStore password.
   - `server-primary-ocsepp-secret-occm` is the secret created by OCCM.

2. To patch the secrets created with the trustStore password file:

   ```
   TLS_CRT=$(base64 < "trust.txt" | tr -d '\n')
   kubectl patch secret server-primary-ocsepp-secret-occm -n seppsvc -p
   "{\"data\":{\"trust.txt\":\"${TLS_CRT}\"}}"
   ```

   Where,

- `trust.txt` is the password file that contains TrustStore password.
- `server-primary-ocsepp-secret-occm` is the secret created by OCCM.

> **Note**
>
> To monitor the lifecycle management of the certificates through OCCM, do not patch the Kubernetes secrets manually to update the TLS certificate or keys. It must be done through the OCCM GUI.

Managing Secrets Manually

1. Run the following command to create secret:

```
$ kubectl create secret generic <ocsepp-n32-secret> --
fromfile=<ssl_ecdsa_private_key.pem> --from-
file=<rsa_private_key_pkcs1.pem> --fromfile=<trust.txt> --from-
file=<key.txt> --from-file=<caroot.cer> --
fromfile=<ssl_rsa_certificate.crt> --from-file=<ssl_ecdsa_certificate.crt>
-n <Namespace of SEPP deployment>
```

Where,

```
<ocsepp-n32-secre> is the secret name for n32-egress-gateway and n32-
ingress-agteway.
<ssl_ecdsa_private_key.pem> is the ECDSA private key.
<rsa_private_key_pkcs1.pem> is the RSA private key.
<trust.txt> is the SSL Truststore file.
<key.txt> is the SSL Keystore file.
<caroot.cer> is the CA root certificate authority
<ssl_rsa_certificate.crt> is the SSL RSA certificate.
<ssl_ecdsa_certificate.crt> is the SSL ECDSA certificate.
<Namespace> of SEPP deployment.
```

> **Note**
>
> - Note down the command used during the creation of Kubernetes secret, this command will be used for updates in future.
> - It is recommended to use the same secret name as mentioned in the example. In case you change <ocsepp-n32-secret>, then update the `k8SecretName` parameter under n32-ingress-gateway and n32-egress-gateway section in the `ocsepp_custom_values_<version>.yaml`. For more information, see the n32-ingress-gateway and n32-egress-gateway section.

Example:

```
kubectl create secret generic ocsepp-n32-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=trust.txt --from-file=key.txt --from-file=caroot.cer --from-
```

```
file=rsa_certificate.crt --from-file=ssl_ecdsa_private_key.pem --from-
file=ocsepp.cer -n seppsvc
```

2. Run the following command to verify the secret:

   ```
   $ kubectl describe secret <ocsepp-n32-secret> -n <Namespace>
   ```

   Where, `<ocsepp-n32-secret>` is the secret name for n32-egress-gateway and n32-ingress-agteway and <Namespace> is the namespace of SEPP deployment.
   Example:

   ```
   $ kubectl describe secret ocsepp-n32-secret -n seppsvc
   ```

> **Note**
>
> If the certificates are not available, then create them following the instructions given in the 'Creating Private Keys and Certificates for Gateways' section.

2.2.1.9.2 Configuring Secrets at PLMN SEPP Egress and Ingress Gateway

This section explains the steps to configure secrets for enabling HTTPS/HTTP over TLS in Public Land Mobile Network (PLMN) Ingress and Egress Gateways. This procedure must be performed before deploying SEPP.

> **Note**
>
> The passwords for TrustStore and KeyStore are stored in respective password files.

To create kubernetes secret for HTTPS/HTTP over TLS, the following files are required:

- ECDSA private key and CA signed certificate of SEPP, if initialAlgorithm is ES256
- RSA private key and CA signed certificate of SEPP, if initialAlgorithm is RS256
- TrustStore password file
- KeyStore password file
- Certificate chain for trust store
- Signed server certificate or Signed client certificate

> **Note**
>
> The creation process for private keys, certificates, and passwords are at the discretion of the user or operator.

You can manage Kubernetes secrets for enabling HTTPS in SEPP using one of the following methods:

- Managing secrets through OCCM
- Managing secrets manually

Managing Secrets Through OCCM

To create the secrets using OCCM, see "Managing Certificates" in *Oracle Communications Cloud Native Core, Certificate Management User Guide*.

The secrets created by OCCM are then patched to add keyStore password and trustStore password files by running the following commands:

1. To patch the secrets created with the keyStore password file:

   ```
   TLS_CRT=$(base64 < "key.txt" | tr -d '\n')
   kubectl patch secret server-primary-seppsvc-secret-occm -n seppsvc -p
   "{\"data\":{\"key.txt\":\"${TLS_CRT}\"}}"
   ```

   Where,

   - `key.txt` is the password file that contains KeyStore password.
   - `server-primary-ocsepp-secret-occm` is the secret created by OCCM.

2. To patch the secrets created with the trustStore password file:

   ```
   TLS_CRT=$(base64 < "trust.txt" | tr -d '\n')
   kubectl patch secret server-primary-ocsepp-secret-occm -n seppsvc -p
   "{\"data\":{\"trust.txt\":\"${TLS_CRT}\"}}"
   ```

   Where,

   - `trust.txt` is the password file that contains TrustStore password.
   - `server-primary-ocsepp-secret-occm` is the secret created by OCCM.

> **Note**
>
> To monitor the lifecycle management of the certificates through OCCM, do not patch the Kubernetes secrets manually to update the TLS certificate or keys. It must be done through the OCCM GUI.

Managing Secrets Manually

1. Run the following command to create secret:

   ```
   $ kubectl create secret generic <ocsepp-plmn-secret> --
   fromfile=<ssl_ecdsa_private_key.pem> --from-
   file=<rsa_private_key_pkcs1.pem> --fromfile=<trust.txt> --from-
   file=<key.txt> --from-file=<caroot.cer> --
   fromfile=<ssl_rsa_certificate.crt> --from-file=<ssl_ecdsa_certificate.crt>
   -n <Namespace of SEPP deployment>
   ```

   Where,

   ```
   <ocsepp-plmn-secret> is the secret name for plmn-egress-gateway and plmn-
   ingress-agteway.
   <ssl_ecdsa_private_key.pem> is the ECDSA private key.
   ```

```
<rsa_private_key_pkcs1.pem> is the RSA private key.
<trust.txt> is the SSL Truststore file.
<key.txt> is the SSL Keystore file.
<caroot.cer> is the CA root certificate authority
<ssl_rsa_certificate.crt> is the SSL RSA certificate.
<ssl_ecdsa_certificate.crt> is the SSL ECDSA certificate.
<Namespace> of SEPP deployment.
```

Note

- Note down the command used during the creation of kubernetes secret, this command will be used for updates in future.
- It is recommended to use the same secret name as mentioned in the example. In case you change `<ocsepp-plmn-secret>`, then update the `k8SecretName` parameter under `plmn-ingress-gateway` and `plmn-egress-gateway` section in the `ocsepp-custom-values-<version>.yaml` file. For more information, see the plmn-ingress-gateway and plmn-egress-gateway section.
- For multiple CA root partners, the SEPP CA certificate should contain the CA information in the particular format. The CAs of the roaming partners should be concatenated in the single file separated by eight hyphens as given below:

```
CA1 content
--------
CA2 content
--------
CA3 content
```

Example:

```
kubectl create secret generic ocsepp-plmn-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=trust.txt --from-file=key.txt --from-file=caroot.cer --from-
file=rsa_certificate.crt --from-file=ssl_ecdsa_certificate.crt --from-
file=ocsepp.cer -n seppsvc
```

2. Run the following command to verify the secret:

```
$ kubectl describe secret <ocsepp-plmn-secret> -n <Namespace>
```

Where,

```
<ocsepp-plmn-secret> is the secret name for plmn-egress-gateway and plmn-
ingress-gateway.
<Namespace> is the namespace of SEPP deployment.
```

Example:

```
$ kubectl describe secret  ocsepp-plmn-secret -n seppsvc
```

2.2.1.10 SEPP Compatibility with Kubernetes, CNE and, Kyverno Policies

This section explains about SEPP compatibility with Kubernetes, CNE and, Kyverno Policies.

1. If Istio or Aspen Service Mesh (ASM) is installed on CNE, run the following command to patch the "disallow-capabilities" clusterpolicy of CNE and exclude the NF namespace before the NF deployment:

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

   where, namespace of NF is the SEPP namespace used for deployment.
   Example:

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

2. Run the following command to verify that cluster policuies are updates with the SEPP namespace in exclude list:

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

   Example:

   ```
   spec:
     background: true
     failurePolicy: Ignore
     rules:
     - exclude:
         any:
         - resources:
             kinds:
             - Pod
             - DaemonSet
             namespaces:
             - kube-system
             - occne-infra
             - rook-ceph
             - seppsvc
   ```

2.2.1.11 Configuring SEPP to Support Aspen Service Mesh

SEPP leverages Aspen Service Mesh (ASM) for all the internal and external TLS communication. 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 special sidecar proxy in each pod to intercept all the network communication between microservices.

Supported ASM version: 1.14.6

For ASM installation and configuration, refer to official Aspen Service Mesh website for details.

Aspen Service Mesh (ASM) configurations are categorized as follows:

- **Control Plane**: It involves adding labels or annotations to inject sidecar. The control plane configurations are part of the NF Helm chart.
- **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 different versions. This configuration is done manually by considering each NF requirement and ASM deployment. This configuration can be done using `ocsepp_servicemesh_config_custom_values_<version>.yaml` file.

Data Plane Configuration

Data Plane configuration consists of following Custom Resource Definitions (CRDs):

- Service Entry (SE)
- Destination Rule (DR)
- Envoy Filter (EF)
- Peer Authentication (PA)
- Virtual Service (VS)

> **Note**
>
> Use `ocsepp_servicemesh_config_custom_values_<version>.yaml` file and Helm charts to add or remove CRDs that you may require due to ASM upgrades to configure features across different releases.

The data plane configuration is applicable in the following scenarios:

- **Service Entry:** Enables adding additional entries into Sidecar's internal service registry, so that auto-discovered services in the mesh can access or route to these manually specified services. A service entry describes the properties of a service (DNS name, VIPs, ports, protocols, endpoints).
- **Destination Rule:** Defines policies that apply to traffic intended for service after routing has occurred. These rules specify configuration for load balancing, connection pool size from the sidecar, and outlier detection settings to detect and evict unhealthy hosts from the load balancing pool.
- **Envoy Filters:** Sidecars rewrite the header with its own default value. Therefore, the headers from back-end services are lost. You require Envoy Filters to help in passing the headers from back-end services to use it as it is, for eg. server header.
- **Peer Authentication:** Used for service-to-service authentication to verify the client making the connection. This template can be used to change the default mTLS mode on the deployment. It allows values such as STRICT, PERMISSIVE, and DISABLE.
- **Virtual Service:** Defines a set of traffic routing rules to apply when a host is addressed. Each routing rule defines matching criteria for the traffic of a specific protocol. If the traffic is matched, then it is sent to a named destination service (or subset or version of it) defined in the registry.

Service Mesh Configuration File

The following are supported fields in CRD:

- Service Entry
  - hosts
  - exportTo
  - location
  - addresses
  - ports.name
  - ports.number
  - ports.protocol
- Destination Rule
  - host
  - mode
  - name
  - exportTo
- Envoy Filters
  - labelselector
  - applyTo
  - filtername
  - operation
  - typeconfig
  - configkey
  - configvalue
- Peer Authentication
  - name
  - labelselector
  - tlsmode
- Virtual Service
  - name
  - prefix
  - host
  - destinationhost
  - port
  - exportTo

For more information about the CRDs and the parameters, see Aspen Service Mesh.

A sample `ocsepp_servicemesh_config_custom_values_<version>.yaml` is available in Custom_Templates file. For downloading the file, see Customizing SEPP.

> **Note**
>
> To connect to vDBTier, create an Service Entry (SE) and Destination Rule (DR) for MySQL connectivity service if the database is in different cluster. Else, the sidecar rejects request as vDBTier does not support sidecars.

2.2.1.11.1 Predeployment Configurations

This section explains the predeployment configuration procedure to install SEPP with Service Mesh support.

> **Note**
>
> From Release 25.1.100 onwards, SEPP ASM supports mediation.

Prerequisites

Ensure that ASM is deployed on the cluster. Validate the following parameters:

1. Run the following command to verify the `certificateCustomFields` parameter value in ASM deployed namespace. This parameter should be set to true.

   ```
   kubectl describe  cm istio-sidecar-injector -n <namespace in which ASM is
   deployed>| grep "certificateCustomFields"
   ```

   Example:

   ```
   kubectl describe  cm istio-sidecar-injector -nistio-system | grep
   "certificateCustomFields"

          "certificateCustomFields": true,
   ```

2. If this parameter is set to false, update the ASM charts to set it to true and perform an upgrade.

   ```
   ./manifests/charts/istio-control/istio-discovery/values.yaml
           certificateCustomFields: true
   ```

3. Run the following command to verify that `istio-base` and `istiod` are installed in the cluster.

   ```
   helm ls -nistio-system
   ```

   Example:

   ```
   helm ls -nistio-system
   NAME            NAMESPACE       REVISION
   UPDATED                                 STATUS
   CHART                   APP VERSION
   ```

```
istio-base      istio-system    1               2024-12-20
10:31:27.240210738 +0000 UTC deployed        base-1.14.6-am1
1.14.6-am1
istiod          istio-system    1               2024-12-20
10:32:45.905279498 +0000 UTC deployed        istiod-1.14.6-am1
1.14.6-am1
```

Predeployment Configuration

Follow the predeployment configuration procedure as mentioned below:

1. Creating SEPP namespace
   a. Run the following command to verify if the required namespace already exists in the system:

      ```
      kubectl get namespaces
      ```

   b. In the output of the above command, check if required namespace is available. If not available, then create the namespace using the following command:

      ```
      kubectl create namespace <namespace>
      ```

      Where,

      `<Namespace>` is the SEPP namespace.

      Example:

      ```
      kubectl create namespace seppsvc
      ```

SEPP Specific Changes

In the `ocsepp_custom_values_<version>.yaml`, do the following changes:

1. Modify `serviceMeshCheck` flag from false to true in all the sections.
2. Modify all occurrence of `serviceMeshEnabled` flag from false to true .
3. In the PLMN Ingress Gateway section, do the following:
   a. change `initssl` to false.
   b. change `enableIncomingHttp` to true.
   c. change `enableIncomingHttps` to false.
4. In the N32 Egress Gateway section, do the following:
   a. Update the sanValues paramter to the SEPP Inter PLMN FQDN.

      Example : sanValues: ["sepp2.inter.oracle.com"]

      > **Note**
      >
      > This value should match with FQDN in the ssl.conf file, which is used for creating TLS certificate.

   b. change `initssl` to false.

c. change `enableOutgoingHttps` to false.

d. change the following to false:

```
sepp:
   tlsConnectionMode: false
```

.

5. In the N32 Ingress Gateway section, do the following:
   a. change `initssl` to false.
   b. change `enableIncomingHttp` to true.
   c. change `enableIncomingHttps` to false.
   d. Do the following to extract the SAN from DNS header which is received from N32 Egress Gateway (Skip this step, if deploying the SEPP only for ATS):

```
xfccHeaderValidation:
 validation:
   enabled: false
 extract:
   enabled: true
   certextractindex: 0
   extractfield: DNS
   extractindex: -99
```

6. In the PLMN Egress Gateway section, do the following:
   a. change `initssl` to false.
   b. change `enableOutgoingHttps` to false.
7. In the PN32C microservice, do the following changes for SAN header name, regex and delimiter (Skip this step, if deploying the SEPP only for ATS):

> **Note**
>
> If SEPP is deployed with single service account default value of the `extractSANDelimiter:","` parameter should not be modified.

```
sanHeaderName: "oc-xfcc-dns"
extractSANRegex: "(.*)"
extractSANDelimiter: " "
```

8. In the PN32F microservice, do the following changes for SAN header name, regex and delimiter (Skip this step, if deploying the SEPP is only for ATS):

> **Note**
>
> If SEPP is deployed with single service account default value of the `extractSANDelimiter:","` parameter should not be modified.

```
sanHeaderName: "oc-xfcc-dns"
extractSANRegex: "(.*)"
extractSANDelimiter: " "
```

2.2.1.11.2 Installation of ASM Configuration Charts

This section explains the installation of ASM configuration charts.
In the `ocsepp_servicemesh_config_custom_values_<version>.yaml` file, do the following changes:

1. Create a destination rule to establish a connection between OCSEPP and cnDBTier. Sample template is given below:

   > **Note**
   >
   > If the cnDBTier does not have istio sidecar injection, then create the destination rule. Else, skip this step.

   Destination Rules:

   ```
   - host: "<db-service-fqdn>.<db-namespace>.svc.<domain>"
     mode: DISABLE
     name: ocsepp-db-service-dr
     exportTo: |-
       [ "." ]
     namespace: seppsvc
   ```

   where,

   - host is the complete hostname of cnDBtier.

     For example, mysql-connectivity-service.cndb-ankit.svc.occne-24-2-cluster-user1"
   - namespace is the Namespace in which SEPP will be deployed.

   DestinationRule section:

   ```
   apiVersion: networking.istio.io/v1alpha3
   kind: DestinationRule
   metadata:
     name: ocsepp-db-service-dr
     namespace: <ocsepp-namespace>
   spec:
     exportTo:
     - "."
     host: "<db-service-fqdn>.<db-namespace>.svc.<domain>"          #
   Example:  mysql-connectivity-service.seppsvc.svc.cluster.local"
     trafficPolicy:
       tls:
         mode: DISABLE
   ```

2. Modify the service entry in pod networking, so that the pods can access Kubernetes api-server. Update the following parameters value:

   - hosts
   - addresses

kube-api-se

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: kube-api-server
  namespace: <ocsepp-namespace>
spec:
  hosts:
  - kubernetes.default.svc.<domain> # domain can be extracted using
kubectl -n kube-system get configmap kubeadm-config -o yaml | grep -i
dnsDomain
  exportTo:
  - "."
  addresses:
  - <20.96.0.1> # cluster IP of kubernetes api server, can be extracted
using  this command --  kubectl get svc -n default
  location: MESH_INTERNAL
  ports:
  - number: 443
    name: https
    protocol: HTTPS
  resolution: NONE
```

3. PeerAuthentication is created for the namespace with default mTLS mode as PERMISSIVE. If user wants to configure, modify the following parameter to STRICT or DISABLE.

```
 tlsmode: STRICT
```

A sample template is as follows:
peerauth

```
apiVersion: security.istio.io/v1beta1
kind: PeerAuthentication
metadata:
 name: ocsepp-peerauthentication
spec:
 selector:
  matchLabels:
   app.kubernetes.io/part-of: ocsepp
 mtls:
  mode: PERMISSIVE
```

> **Note**
>
> - After the successful deployment, you can change the PeerAuthentication mtls mode to STRICT from PERMISSIVE and perform Helm upgrade.
> - Ensure that spec.selector.matchLabels must be `app.kubernetes.io/part-of: ocsepp` value. User should not change it.

4. **Optional:** Uncomment the SE section below, if deploying OCSEPP in ASM mode (only for ATS):

```
apiVersion: networking.istio.io/v1beta1
kind: ServiceEntry
metadata:
  name: stub-serviceentry
  namespace: seppsvc
spec:
  exportTo:
  - '*'
  hosts:
  - '*.svc.cluster.local'
  - '*.3gppnetwork.org'
  location: MESH_INTERNAL
  ports:
  - name: http2
    number: 8080
    protocol: HTTP2
  resolution: NONE
```

5. Envoy filter will be deployed with the following default configuration:

```
envoyFilters_v_19x_111x:
  - name: serverheaderfilter
    configpatch:
      - applyTo: NETWORK_FILTER
        filtername: envoy.filters.network.http_connection_manager
        operation: MERGE
        typeconfig: type.googleapis.com/
envoy.extensions.filters.network.http_connection_manager.v3.HttpConnectionM
anager
        configkey: server_header_transformation
        configvalue: PASS_THROUGH
```

6. Run the following command to verify if all CRDs are installed:

```
kubectl get <CRD-Name> -n <Namespace>
```

Where,

- CRD-Name are the resource names
- Namespace is the namespace in which SEPP should be deployed

Example:

```
kubectl get se,dr,peerauthentication,envoyfilter,vs -n seppsvc
```

> **Note**
>
> Any modification to the existing CRDs or adding CRDs can be done by updating the `ocsepp_servicemesh_config_custom_values_<version>.yaml` file and running Helm upgrade.

7. Run the following command to install ASM specific resources in your namespace:

   ```
   helm install -f ocsepp_servicemesh_config_custom_values_<version>.yaml
   <release-name> ocsepp-servicemesh-config-<version>.tgz --namespace <sepp
   namespace>
   ```

   Example:

   ```
   helm install -f ocsepp_servicemesh_config_custom_values_25.1.200.yaml
   ocsepp-servicemesh ocsepp-servicemesh-config-25.1.200.tgz --namespace
   seppsvc
   ```

2.2.1.11.3 Deploying SEPP with ASM

This section explains how to deploy SEPP using ASM.

1. Create namespace label for auto sidecar injection to automatically add the sidecars in all of the pods spawned in SEPP namespace:

   ```
   kubectl label ns <ocsepp-namespace> istio-injection=enabled
   ```

   Example:

   ```
   kubectl label ns seppsvc istio-injection=enabled
   ```

2. Run the following command to verify that label is applied on the namespace:

   ```
   kubectl describe ns seppsvc
   ```

   Output:

   ```
   Name:         seppsvc
   Labels:       istio-injection=enabled
                 kubernetes.io/metadata.name=seppsvc
   Annotations:  <none>
   Status:       Active
   ```

3. Update `ocsepp_custom_values_<version>.yaml` with the following:
   a. Update the following sidecar resource configuration in allResources section of customExtension in global section:
      - sidecar.istio.io/proxyCPULimit: "2"
      - sidecar.istio.io/proxyMemoryLimit: 1Gi
      - sidecar.istio.io/proxyCPU: 200m

- sidecar.istio.io/proxyMemory: 128Mi

```
customExtension:
  allResources:
    labels: {}
    annotations:
      sidecar.istio.io/proxyCPULimit: "2"
      sidecar.istio.io/proxyMemoryLimit: 1Gi
      sidecar.istio.io/proxyCPU: 200m
      sidecar.istio.io/proxyMemory: 128Mi
  lbServices:
    labels: {}
    annotations: {}
  lbDeployments:
    labels: {}
    annotations: {}
  nonlbServices:
    labels: {}
    annotations: {}
  nonlbDeployments:
    labels: {}
    annotations: {}
```

b. To scrape metrics from SEPP pods, add oracle.com/cnc: "true" annotation under lbDeployments and nonlbDeployments section of customExtension in global section:

> **Note**
>
> This step is required only if OSO is deployed.

```
customExtension:
  allResources:
    labels: {}
    annotations: {}
  lbServices:
    labels: {}
    annotations: {}
  lbDeployments:
    labels: {}
    annotations:
      oracle.com/cnc: "true"
  nonlbServices:
    labels: {}
    annotations: {}
  nonlbDeployments:
    labels: {}
    annotations:
      oracle.com/cnc: "true"
```

c. To enable Prometheus to scrape metrics from app-info, perf-info, and ocpm-config pods, add the following annotation in service specific customExtension section: traffic.sidecar.istio.io/excludeInboundPorts: "9000".
To exclude additional inbound and outbound ports, the same procedure can be applied to these microservices.

> **Note**
>
> The addition of `excludeInboundPorts` and `excludeOutboundPorts` in global sections like `customExtension.lbDeployments` or `customExtension.nonlbDeployments` is not allowed, as it can override essential ports and disrupt inter-microservice communication.

```
nrfclient:
  perf-info:
    deployment:
      customExtension:
        labels: {}
        annotations:
          traffic.sidecar.istio.io/excludeInboundPorts: "9000"
  config-server:
    deployment:
      customExtension:
        labels: {}
        annotations:
          traffic.sidecar.istio.io/excludeInboundPorts: "9000"
  appinfo:
    deployment:
      customExtension:
        labels: {}
        annotations:
          traffic.sidecar.istio.io/excludeInboundPorts: "9000"
```

> **Note**
>
> This step is required when OSO is deployed with ASM sidecar.

d. Add the following sample configurations to exclude istio inbound and outbound ports in nfmanagement and nfdiscovery microservices:

```
cacheServicePortStart: 8095
cacheServicePortEnd: 8096
istioExcludePorts: true
cacheServiceLivenessPort: 7
```

e. In the nrf-client-nfmanagement and nrf-client-nfdiscovery section, verify that the value 9091 is given to the istioExcludePorts parameter:

```
istioExcludePorts: 53,9091
```

4. To deploy and use SEPP with ASM, ensure to use `ocsepp_custom_values_<version>.yaml` file while performing helm install or upgrade. The file must have all the necessary changes mentioned in the Predeployment Configurations section for deploying SEPP with ASM.

2.2.1.11.4 Postdeployment Configuration

This section explains the postdeployment configurations.

> **Note**
>
> The steps 1 to 3 are not required if SEPP is deployed only in ATS mode.

1. In the `ocsepp_servicemesh_config_custom_values_<version>.yaml` file, do the following:
   a. Uncomment the section and add the following values for Service entry:
      i. In the `hosts` parameter, add the FQDN of the Remote SEPP. If the user has different N32C and N32F end points, user can create two seperate service entries.
      ii. Add IP in the format <IP/32> for N32 Ingress Gateway of Remote SEPP in `addresses` parameter.
      iii. Add IP in the `endPointAddress` parameter as given in step ii.
      iv. Ensure that `ports.number` parameter is updated to the port number of N32 Ingress Gateway of Remote SEPP.
      service-entry

```
- hosts: |-
    [ "prod.sepp.inter.oracle.com" ]         # FQDN of Remote SEPP
  exportTo: |-
    [ "." ]
  location: MESH_INTERNAL
  addresses: |-
    [ "10.233.12.232/32" ]
  ports:
  - number: 80
    name: http2
    protocol: HTTP2
  resolution: STATIC                  # should be NONE/DNS - if we
are using wildchars in fqdn it must be NONE
  endPointAddress: 10.233.12.232
  name: seppendpoint
```

   b. Uncomment the section and add values for Virtual service as follows:
      i. In the `host` parameter, add the FQDN of the Remote SEPP. If the user has different N32C and N32F end points, user can create two seperate virtual services.
      ii. In the `destinationhost` parameter, add the Remote SEPP fqdn , Remote SEPP namespace, and Remote SEPP domain name.
      iii. Ensure that `port` parameter is updated to the port number of N32 Ingress Gateway of Remote SEPP.

virtual Service

```
virtualService:
  - name: remote-sepp-vs
    prefix: "/"
    host: prod.sepp.inter.oracle.com #FQDN of Remote SEPP
    destinationhost: <remote-sepp-fqdn>.<remote-sepp-
namespace>.svc.<domain>
    port: 80
    exportTo: |-
      [ "." ]
```

2. The above changes will be done on C-SEPP as well as on P-SEPP. Ensure correct values are populated on both sides.
3. Run the following command to add these changes:

   ```
   helm upgrade -f ocsepp_servicemesh_config_custom_values_<version>.yaml
   <release-name> ocsepp-servicemesh-config-25.1.100.tgz --namespace <ns>
   ```

   Example:

   ```
   helm upgrade -f ocsepp_servicemesh_config_custom_values_25.1.100.yaml
   ocsepp-servicemesh ocsepp-servicemesh-config-25.1.100.tgz --namespace
   seppsvc
   ```

Enable Inter-NF communication

For every new NF participating in call flows when SEPP is a client, DestinationRule, and ServiceEntry must be created in SEPP namespace to enable communication. Following is the inter-NF communication with SEPP:

- SEPP to NRF communication (for registration and heartbeat) Create CRDs as mentioned in above step.

OSO deployment

1. If OSO is deployed with service mesh, add this annotation in OSO `ocoso_csar_vzw_<release-number>_prom_custom_values.yaml` file file to exclude outbound ports of all the SEPP services.
   Example:

   ```
   traffic.sidecar.istio.io/excludeOutboundPorts: 9090, 9093, 9094, 8085,
   9091,
   8091, 9000, 8081
   ```

> **Note**
>
> This is applicable only when OSO is deployed with istio side car.

For more information on OSO deployment, see *Oracle Communications Operations Services Overlay Installation and Upgrade Guide* and *Oracle Communications Operations Services Overlay User Guide*.

2.2.1.11.5 Deleting Service Mesh

This section describes the steps to disable or delete the service mesh.

To disable service mesh, run the following command:

```
kubectl label --overwrite namespace seppsvc istio-injection=disabled
```

To verify if service mesh is disabled, run the following command:

```
kubectl get se,dr,peerauthentication,envoyfilter,vs -n seppsvc
```

To delete service mesh, run the following command:

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

Where,

- <helm-release-name> is the release name used by the helm command. This release name must be the same as the release name used for ServiceMesh.
- <namespace> is the deployment namespcae used by Helm command.

For example:

```
helm delete ocsepp-servicemesh -n seppsvc
```

> **Note**
>
> The changes due to the disabling of service mesh will be reflected only if SEPP is redeployed.

2.2.1.12 Configuring Network Policies

Kubernetes network policies allow you to define ingress or egress rules based on Kubernetes resources such as Pod, Namespace, IP, and Port. These rules are selected based on Kubernetes labels in the application. These network policies enforce access restrictions for all the applicable data flows except communication from Kubernetes node to pod for invoking container probe.

> **Note**
>
> Configuring network policies is an optional step. Based on the security requirements, network policies may or may not be configured.

For more information on network policies, see https://kubernetes.io/docs/concepts/services-networking/network-policies/.

> **Note**
>
> - If the traffic is blocked or unblocked between the pods even after applying network policies, check if any existing policy is impacting the same pod or set of pods that might alter the overall cumulative behavior.
> - If changing default ports of services such as Prometheus, Database, Jaegar, or if Ingress or Egress Gateway names are overridden, update them in the corresponding network policies.

Configuring Network Policies

The following are the various operations that can be performed for network policies:

2.2.1.12.1 Installing Network Policies

Prerequisite

Network Policies are implemented by using the network plug-in. To use network policies, you must use a networking solution that supports Network Policy.

> **Note**
>
> For a fresh installation, it is recommended to install Network Policies before installing SEPP. However, if SEPP is already installed, you can still install the Network Policies.

To install network policy:

1. Open the `ocsepp_network_policies_custom_values_25.1.202.yaml` file provided in the release package zip file. For downloading the file, see Downloading SEPP Package, Pushing the SEPP Images to Customer Docker Registry, and Pushing the Roaming Hub or Hosted SEPP Images to Customer Docker Registry.
2. The file is provided with the default network policies. If required, update the `ocsepp_network_policies_custom_values_25.1.202.yaml` file. For more information on the parameters, see the Configuration Parameters for network policy parameter table.

Note

- To run ATS, uncomment the following policies from `ocsepp_network_policies_custom_values_25.1.202.yaml` file:
  - allow-ingress-traffic-to-notification
  - allow-egress-ats
  - allow-ingress-ats
- To connect with CNC Console, update the below parameter in the `allow-ingress-from-console` policy in the `ocsepp_network_policies_custom_values_25.1.202.yaml` file:
  - `kubernetes.io/metadata.name`: <namespace in which CNCC is deployed>
- To copy messages from plmn-ingress-gateway and n32-ingress-gateway to kafka broker in Data Director, update the below parameter in the `allow-egress-to-data-director-from-igw` policy in the `ocsepp_network_policies_custom_values_25.1.202.yaml` file:
  - `kubernetes.io/metadata.name`: <namespace in which kafka broker is present>
- In `allow-ingress-prometheus` and `allow-egress-to-prometheus` policies, `kubernetes.io/metadata.name` parameter must contain the value for the namespace where Prometheus is deployed, and `app.kubernetes.io/name` parameter value should match the label from Prometheus pod.
- The following Network Policies require modification for ASM deployment. The required modifications are mentioned in the comments in `ocsepp_custom_values_network_policies.yaml` file. Update the policies as per the comments.
  - allow-ingress-sbi-n32-igw
  - allow-ingress-sbi-plmn-igw

3. Run the following command to install the network policies:

```
helm install <helm-release-name> <network-policy>/ -n <namepsace> -f
      <custom-value-file>
```

For Example:

```
helm install ocsepp-network-policy
        ocsepp-network-policy-25.1.202/ -n seppsvc -f
        ocsepp_network_policies_custom_values_25.1.202.yaml
```

Where,

- `helm-release-name`: ocsepp-network-policy helm release name.
- `custom-value-file`: ocsepp-network-policy custom value file.
- `namespace`: SEPP namespace.
- `network-policy`: location where the network-policy package is stored.

> **Note**
>
> - Connections that were created before installing network policy and still persist are not impacted by the new network policy. Only the new connections would be impacted.
> - If you are using ATS suite along with network policies, it is required to install the SEPP and ATS in the same namespace.

2.2.1.12.2 Upgrading Network Policies

To add, delete, or update network policy:

1. Modify the `ocsepp_network_policies_custom_values_25.1.202.yaml` file to update, add, and delete the network policy.
2. Run the following command to upgrade the network policies:

```
helm upgrade <helm-release-name> <network-policy>/ -n <namespace> -f <custom-value-file>
```

For Example:

```
helm upgrade ocsepp-network-policy
        ocsepp-network-policy-25.1.200/ -n seppsvc -f
        ocsepp_network_policies_custom_values_25.1.202.yaml
```

Where,

- `helm-release-name`: ocsepp-network-policy Helm release name.
- `custom-value-file`: ocsepp-network-policy custom value file.
- `namespace`: SEPP namespace.
- `network-policy`: location where the network-policy package is stored

2.2.1.12.3 Verifying Network Policies

Run the following command to verify that the network policies have been applied successfully:

```
kubectl get <helm-release-name> -n <namespace>
```

For Example:

```
kubectl get ocsepp-release-network-policy -n seppsvc
```

Where,

- `helm-release-name`: ocsepp-network-policy Helm release name
- `namespace`: SEPP namespace

Sample output:

```
NAME                                POD-
SELECTOR                                                    AGE
allow-egress-database               app.kubernetes.io/name notin (n32-egress-
gateway,plmn-egress-gateway)        2m35s
allow-egress-dns                    app.kubernetes.io/name notin (n32-egress-
gateway,plmn-egress-gateway)        2m35s
allow-egress-jaeger                 app.kubernetes.io/name notin (n32-egress-
gateway,plmn-egress-gateway)        2m35s
allow-egress-k8-api                 app.kubernetes.io/name notin (n32-egress-
gateway,plmn-egress-gateway)        2m35s
allow-egress-to-prometheus          app.kubernetes.io/name notin (n32-egress-
gateway,plmn-egress-gateway)        7s
allow-egress-to-sepp-pods           app.kubernetes.io/name notin (n32-egress-
gateway,plmn-egress-gateway)        2m35s
allow-ingress-from-console          app.kubernetes.io/name=config-mgr-
svc                                        2m35s
allow-ingress-from-sepp-pods        app.kubernetes.io/part-
of=ocsepp                                  2m35s
allow-ingress-prometheus            app.kubernetes.io/part-
of=ocsepp                                  2m35s
allow-ingress-sbi-n32-igw           app.kubernetes.io/name=n32-ingress-
gateway                                    2m35s
allow-ingress-sbi-plmn-igw          app.kubernetes.io/name=plmn-ingress-
gateway                                   2m35s
deny-egress-all-except-egw          app.kubernetes.io/name notin (n32-egress-
gateway,plmn-egress-gateway)        2m35s
deny-ingress-all                    app.kubernetes.io/part-
of=ocsepp                                  2m35s
```

2.2.1.12.4 Uninstalling Network Policies

1. Run the following command to uninstall the network policies:

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

For Example:

```
helm uninstall ocsepp-network-policy -n seppsvc
```

> **Note**
>
> While using the debug container, it is recommended to uninstall the network policies or update them as required to establish the connections.

2.2.1.12.5 Configuration Parameters for Network Policies

This section includes information about the supported Kubernetes resource and configuration parameters for configuring Network Policies.

Table 2-23 Supported Kubernetes Resource for Configuring Network Policies

Parameter	Description	Details
`apiVersion`	This is a mandatory parameter. Specifies the Kubernetes version for access control. **Note:** This is the supported API version for network policy. This is a read-only parameter.	**DataType:** String **Default Value:** networking.k8s.io/v1
`kind`	This is a mandatory parameter. Represents the kind of REST resource this object represents. **Note:** This is a read only parameter.	**DataType:** String **Default Value:** NetworkPolicy

Table 2-24 Configuration Parameters for Network Policies

Parameter	Description	Details
`metadata.name`	This is a mandatory parameter. Specifies a unique name for the network policy.	**DataType:** String **Default Value:** {{ .metadata.name }}
`spec.{}`	This is a mandatory parameter. This consists of all the information needed to define a particular network policy in the given namespace. Note: SEPP supports the spec parameters defined in Kubernetes Resource Category.	**DataType:** Object **Default Value:** NA

For more information about this functionality, see "Network Policies" in the *Cloud Native Core, Security Edge Protection Proxy User Guide*.

2.2.1.13 Configuring Traffic Segregation

This section provides information on how to configure Traffic Segregation in SEPP. For description of " Traffic Segregation" feature, see " Traffic Segregation" section in "SEPP Supported Features " chapter of *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* .

Various networks can be created at the time of CNE cluster installation. The following things can be customized at the time of the cluster installation using `cnlb.ini` file provided as part of CNE installation.

1. Number of network pools
2. Number of Egress IPs
3. Number of Service IPs/Ingress IPs
4. External IPs/subnet

For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment User Guide*.

To use one or multiple interfaces, you must configure annotations in the `deployment.customExtension.annotations` parameter of the `ocsepp_custom_values_<version>.yaml` file.

Configuration at Ingress Gateway

Use the following annotation to configure network segregation at ingress-side in `ocsepp_custom_values_<version>.yaml`:

Annotation for a single interface

```
k8s.v1.cni.cncf.io/networks: default/<network interface>@<network interface>
oracle.com.cnc/cnlb: '[{"backendPortName": "<igw port name>", "cnlbIp":
"<external IP>","cnlbPort":"<port number>"}]'
```

Here,

- `k8s.v1.cni.cncf.io/networks`: Contains all the network attachment information the pod uses for network segregation.
- `oracle.com.cnc/cnlb`: To define service IP and port configurations that the deployment will employ for ingress load balancing.
  Where,
  - `cnlbIp` is the front-end IP utilized by the application.
  - `cnlbPort` is the front-end port used in conjunction with the CNLB IP for load balancing.
  - `backendPortName` is the backend port name of the container that needs load balancing, retrievable from the deployment or pod spec of the application.

Sample annotation for a single interface:

```
k8s.v1.cni.cncf.io/networks: default/nf-sig1-int8@nf-sig1-int8
oracle.com.cnc/cnlb: '[{"backendPortName": "igw-port", "cnlbIp":
"10.123.155.16","cnlbPort":"80"}]'
```

Sample annotation for multiport:

```
        k8s.v1.cni.cncf.io/networks: default/nf-oam-int5@nf-oam-int5
        oracle.com.cnc/cnlb: '[{"backendPortName": "query", "cnlbIp":
"10.75.180.128","cnlbPort": "80"}, {"backendPortName": "admin", "cnlbIp":
"10.75.180.128", "cnlbPort":"16687"}]''
```

In the above example, each item in the list refers to a different backend port name with the same CNLB IP, but the ports for the front end are distinct.

Ensure that the backend port name aligns with the container port name specified in the deployment's specification, which needs to be load balanced from the port list. The CNLB IP represents the external IP of the service, and cnlbPort is the external-facing port:

```
ports:
- containerPort: 16686
  name: query
  protocol: TCP
- containerPort: 16687
  name: admin
  protocol: TCP
```

Configuration at Egress Gateway

Use the following annotation to configure network segregation at egress-side in `ocsepp_custom_values_<version>.yaml`:

Sample annotation for a single interface:

```
k8s.v1.cni.cncf.io/networks: default/nf-sig-egr1@nf-sig-egr1
```

Sample annotation for a multiple interface:

```
k8s.v1.cni.cncf.io/networks: default/nf-oam-egr1@nf-oam-egr1,default/nf-sig-egr1@nf-sig-egr1
```

> **Note**
>
> - The network attachments will be deployed as a part of cluster installation only.
> - The network attachment name should be unique for all the pods.

For information about the above mentioned annotations, see "Configuring Cloud Native Load Balancer (CNLB)" in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.

2.2.2 Installation Tasks

This section provides installation procedures to install Security Edge Protection Proxy (SEPP) using Command Line Interface (CLI).

Before installing SEPP, you must complete Prerequisites and Preinstallation Tasks for both the deployment methods.

2.2.2.1 Installing SEPP Package

To install the SEPP package:

1. Navigate to the Helm directory which is a part of Files directory of unzipped csar package. Run the following command:

   ```
   cd Files/Helm
   ```

2. Run the following command to verify the SEPP Helm charts in the Helm directory:

   ```
   ls
   ```

   The output must be:

   - `ocsepp-25.1.201.tgz`
   - `ocsepp-network-policy-25.1.201.tgz`
   - `ocsepp-servicemesh-config-25.1.201.tgz`

3. Customize the `ocsepp_custom_values_25.1.2000.yaml` file with the required deployment parameters. See Customizing SEPP section to customize the file. For more information about predeployment parameter configurations, see Predeployment Configuration tasks.

> **Note**
>
> Customize the `ocsepp_custom_values_25.1.201.yaml` file for SEPP deployment. See Customizing SEPP section for the details of the parameters. Some of the mandatory parameters are:
>
> - `dockerRegistry`
> - `namespace`
> - `mysql.primary.host`
> - SEPP inter and intra FQDN (`nfFqdnRef, viaHeaderSeppViaInterFqdn, viaHeaderSeppViaIntraFqdn, intraPlmnFqdn, sanValues`).

> **Note**
>
> - In case of multisite georedundant setups, configure nfInstanceId uniquely for each SEPP site.
> - Ensure the nfInstanceId configuration in the global section is same as that in the appProfile section of NRF client. `- dockerRegistry: occne-repo-host:5000`

4. Run the following command to install SEPP:

```
helm install <helm-release> ocsepp-25.1.201.tgz --namespace <k8s namespace> -f <path to ocsepp_customized_values.yaml>
```

Example:

```
helm install ocsepp-release ocsepp-25.1.201.tgz --namespace seppsvc -f ocsepp_custom_values_25.1.201.yaml
```

> **Note**
>
> - Ensure the following:
>
> `<helm-release>` must not exceed 20 characters.
> `namespacename` is the deployment namespace used by helm command.
>
> `custom_values.yaml` file name is the name of the custom values yaml file (including location).
> - **Timeout duration:** Timeout duration is an optional parameter that can be used in the Helm install command. If it is not specified, the default value will be 5m (5 minutes) in Helm3. It sets the time to wait for any individual Kubernetes operation (like Jobs for hooks). The default value is 5ms. If the helm install command fails at any point to create a Kubernetes object, it will internally call the purge to delete after the timeout value (default: 300s). Here, timeout value is not for overall installation but automatic purge on installation failure.
> - In Georedundant deployment, if you want to add or remove a site, refer to Adding a Site to an Existing SEPP Georedundant Site and Removing a Site to from an Existing Georedundant Deployment.

> **Caution**
>
> Do not exit from `helm install` command manually. After running the `helm install` command, it takes some time to install all the services. In the meantime, you must not press "ctrl+c" to come out from `helm install` command. It leads to some anomalous behavior.

2.2.2.2 Installing Roaming Hub or Hosted SEPP

This section describes how to install Roaming Hub or Hosted SEPP in the Cloud Native Environment.

> **Note**
>
> This is applicable only for Roaming Hub or Hosted SEPP installation.

1. Navigate to the Helm directory which is a part of Files directory of unzipped csar package. Run the following command:

   ```
   cd Files/Helm
   ```

2. Run the following command to verify the SEPP Helm charts in the Helm directory:

   ```
   ls
   ```

   The output must be:

   - `ocsepp-25.1.201.tgz`

- `ocsepp-network-policy-25.1.201.tgz`
- `ocsepp-servicemesh-config-25.1.201.tgz`

3. Customize the `ocsepp_custom_values_25.1.2000.yaml` file with the required deployment parameters. See Customizing SEPP section to customize the file. For more information about predeployment parameter configurations, see Predeployment Configuration tasks.
4. Run the following command to install SEPP:

```
helm install <helm-release> ocsepp-25.1.201.tgz --namespace <k8s
namespace> -f <path to ocsepp_custom_values_roaming_hub_25.1.201.yaml>
```

Example:

```
helm install ocsepp-release ocsepp-25.1.201.tgz --namespace seppsvc -f
ocsepp_custom_values_roaming_hub_25.1.201.yaml
```

Note

- Ensure the following:

  `<helm-release>` must not exceed 20 characters.
  `namespacename` is the deployment namespace used by helm command.

  `custom_values.yaml` file name is the name of the custom values yaml file (including location).
- **Timeout duration:** Timeout duration is an optional parameter that can be used in the Helm install command. If it is not specified, the default value will be 5m (5 minutes) in Helm3. It sets the time to wait for any individual Kubernetes operation (like Jobs for hooks). The default value is 5ms. If the helm install command fails at any point to create a Kubernetes object, it will internally call the purge to delete after the timeout value (default: 300s). Here, timeout value is not for overall installation but automatic purge on installation failure.
- In Georedundant deployment, if you want to add or remove a site, refer to Adding a Site to an Existing SEPP Georedundant Site and Removing a Site to from an Existing Georedundant Deployment.

Caution

Do not exit from `helm install` command manually. After running the `helm install` command, it takes some time to install all the services. In the meantime, you must not press "ctrl+c" to come out from `helm install` command. It leads to some anomalous behavior.

2.2.3 Postinstallation Tasks

This section explains the postinstallation tasks for SEPP.

2.2.3.1 Verifying Installation

To verify the installation:

1. To verify the deployment status, open a new terminal and run the following command:

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

   The pod status gets updated at regular intervals.
2. Run the following command to verify the installation status:

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

   Example:

   ```
   helm status ocsepp-release -n seppsvc
   ```

   Where,

   - `<helm-release>` is the Helm release name of SEPP.
   - `<SEPP namespace>` is the namespace of SEPP deployment.

   If the deployment is successful, then the status is displayed as `deployed`.

   Sample output:

   ```
   NAME: ocsepp-release
   LAST DEPLOYED: Sat Jan 11 20:08:03 2025
   NAMESPACE: seppsvc
   STATUS: deployed
   REVISION: 1
   ```
3. Run the following command to check the status of the services:

   ```
   kubectl -n <SEPP namespace> get services
   ```

   Example:

   ```
   kubectl -n seppsvc get services
   ```
4. Run the following command to check the status of the pods:

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

   The value in the `STATUS` column of all the pods must be `Running`.

   The value in the `READY` column of all the pods must be n/n, where n is the number of containers in the pod.

Example:

```
$ kubectl get pods -n seppsvc


NAME                                                READY   STATUS    RESTARTS   AGE
ocsepp-release-appinfo-55b8d4f687-wqtgj                         1/1
Running   0     141m
ocsepp-release-cn32c-svc-64cd9c555c-ftd8z                       1/1
Running   0     113m
ocsepp-release-cn32f-svc-dd886fbcc-xr2z8                        1/1
Running   0     4m4s
ocsepp-release-config-mgr-svc-6c8ddf4c4f-lb4zj                  1/1
Running   0     141m
ocsepp-release-n32-egress-gateway-5b575bbf5f-z5bbx              2/2
Running   0     131m
ocsepp-release-n32-ingress-gateway-76874c967b-btp46             2/2
Running   0     131m
ocsepp-release-ocpm-config-65978858dc-t4t5k                     1/1
Running   0     141m
ocsepp-release-performance-67d76d9d58-llwmt                     1/1
Running   0     141m
ocsepp-release-plmn-egress-gateway-6dc4759cc7-wn6r8             2/2
Running   0     31m
ocsepp-release-plmn-ingress-gateway-56c9b45658-hfcxx            2/2
Running   0     131m
ocsepp-release-pn32c-svc-57774fdc4-2qpvx                        1/1
Running   0     141m
ocsepp-release-pn32f-svc-586cd87c7b-pxk6m                       1/1
Running   0     3m47s
ocsepp-release-sepp-nrf-client-nfdiscovery-65747884cd-qblqn     1/1
Running   0     141m
ocsepp-release-sepp-nrf-client-nfmanagement-5dd6ff98d6-cr7s7    1/1
Running   0     141m
ocsepp-release-nf-mediation-74bd4dc799-d9ks2                    1/1
Running   0     141m
ocsepp-release-coherence-svc-54f7987c4b-wv4h7                   1/1
Running   0     141m
```

Note

- Take a backup of the following files that are required during fault recovery:
  - Updated `ocsepp_custom_values_<version>.yaml` file
  - Updated Helm charts
  - Secrets, certificates, and keys that are used during installation
- If the installation is not successful or you do not see the status as Running for all the pods, perform the troubleshooting steps provided in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide.*

2.2.3.2 Performing Helm Test

This section describes how to perform sanity check for SEPP installation through Helm test. The pods to be checked should be based on the namespace and label selector configured for the Helm test configurations.

Helm Test is a feature that validates successful installation of SEPP and determines if the NF is ready to take traffic.

This test also checks for all the PVCs to be in bound state under the Release namespace and label selector configured.

> **Note**
>
> Helm Test can be performed only on Helm3.

Perform the following Helm test procedure:

1. Configure the Helm test configurations under the global parameters section of the `ocsepp_custom_values_25.1.201.yaml` file as follows:

```
#helm test configuration
test:
  imageRepository: occne-repo-host:5000
  nfName: ocsepp
  image:
    name: nf_test
    tag: 25.1.200
    pullPolicy: Always
  config:
    logLevel: INFO
    # Configure timeout in SECONDS.
    # Estimated total time required for SEPP deployment and helm test
command completion
    timeout: 240
  resources:
    requests:
      cpu: 1
      memory: 1Gi
      #ephemeral-storage: 70Mi
    limits:
      cpu: 1
      memory: 1Gi
      #ephemeral-storage: 1Gi
  complianceEnable: true
  k8resources:
    - horizontalpodautoscalers/v1
    - deployments/v1
    - configmaps/v1
    - prometheusrules/v1
    - serviceaccounts/v1
    - poddisruptionbudgets/v1
    - roles/v1
```

```
    - services/v1
    - rolebindings/v1
```

2. Run the following Helm test command:

   ```
   helm test <helm-release> -n <namespace>
   ```

   Where,

   <helm-release> is the release name.

   <namspace> is the deployment namespace where SEPP is installed.

   Example:

   ```
   helm test ocsepp-release -n seppsvc
   ```

   Sample Output:

   ```
   [admusr@cnejac0101-bastion-2 ocsepp-22.4.0-0]$  helm test ocsepp-release -
   n seppsvc
   NAME: ocsepp-release
   LAST DEPLOYED: Fri Aug 19 04:56:36 2022
   NAMESPACE: seppsvc
   STATUS: deployed
   REVISION: 1
   TEST SUITE:     ocsepp-release
   Last Started:   Fri Aug 19 05:02:03 2022
   Last Completed: Fri Aug 19 05:02:26 2022
   Phase:          Succeeded
   ```

If the Helm test fails, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide.*

2.2.3.3 Taking the Back Up

Take a backup of the following files, which are required during fault recovery:

- Current custom-values.yaml file from which you are upgrading
- Updated ocsepp_custom_values_25.1.201.yaml file
- Updated Helm charts
- Secrets, certificates, and keys that are used during installation.
- Updated ocsepp_servicemesh_config_custom_values_25.1.201.yaml file.
- Updated ocsepp_custom_values_25.1.201.yaml file.

3
Customizing SEPP

This chapter provides information about customizing SEPP deployment in a cloud native environment.

The SEPP deployment is customized by overriding the default values of various configurable parameters in the `ocsepp_custom_values_25.1.202.yaml` file.

1. Navigate to the Scripts directory under the unzipped csar package. For more information on how to download the package from MOS, see Downloading SEPP package.
2. The following files are used to customize the deployment parameters during installation:
   - `ocsepp_custom_values_25.1.202.yaml`: This file is used to customize the deployment parameters during SEPP installation.
   - `ocsepp_custom_values_roaming_hub_25.1.202.yaml`: This file is used to customize the deployment parameters during Roaming Hub installation.
   - `ocsepp_dashboard_promha_25.1.202.json`: SEPP KPI and metrics representation template that should be loaded on Grafana (CNE 1.9 and Above).
   - `ocsepp_oci_dashboard_25.1.202.json`: This file is used by OCIs Logging Analytics Dashboard service for creating SEPPs metrics dashboard.
   - `ocsepp_dashboard_25.1.202.json`: SEPP KPI and metrics representation template that should be loaded on Grafana.
   - `ocsepp_alertrules_promha_25.1.202.yaml`: This file is used for Prometheus for CNE 1.9.0 and later or CNE with Prometheus Operator.
   - `ocsepp_oci_alertrules_25.1.202.zip`: This file is used by OCIs Resource Mananger (RM) stack to create SEPP alarms in OCI.
   - `ocsepp_alertrules_25.1.202.yaml`: This file is used for Prometheus.
   - `ocsepp_mib_tc_25.1.202.mib`: This is considered as SEPP top level MIB file, where the Objects and their data types are defined.
   - `ocsepp_mib_25.1.202.mib`: This file fetches the Objects from the top level MIB file and based on the Alert notification, these objects can be selected for display.
   - `toplevel.mib`: This file contains TEKELEC top level reg definitions.
   - `ocsepp_configuration_openapi_25.1.202.yaml`: This file is OPEN API specification for SEPP configuration.
   - `ocsepp_dbtier_25.1.200_custom_values_25.1.202.yaml`: This file is used to customize the cnDBTier parameters during SEPP installation.
   - `ocsepp_single_service_account_config_25.1.202.yaml`: This file is used to create a single service account, role, and rolebinding which can be used by all the microservices of SEPP.
   - `ocsepp_network_policies_custom_values_25.1.202.yaml`: This file is used while configuring network policies.
   - `ocsepp_servicemesh_config_custom_values_25.1.202.yaml`: This file is used while configuring ASM Data Plane.

- `ocsepp_rollback_schema_25.1.202.sql`

3. Customize the `ocsepp_custom_values_25.1.202.yaml` file.
4. Save the updated `ocsepp_custom_values_25.1.202.yaml` file in the Helm chart directory.
5. Customize the `ocsepp_servicemesh_config_custom_values_25.1.202.yaml` file, in case ASM Data Plane must be configured. For sample file, see Configuring SEPP to Support ASM.
6. Save the updated `ocsepp_servicemesh_config_custom_values_25.1.202.yaml` file in the helm chart directory.
7. Customize the `ocsepp_network_policy_custom_values_25.1.202.yaml` file, in case network policies must be configured.
8. Save the updated `ocsepp_network_policy_custom_values_25.1.202.yaml` file in the helm chart directory.

3.1 Configurable Parameters

This section includes information about the configuration parameters of SEPP.

SEPP allows customization of parameters for the different microservices and related settings.

> **Note**
>
> - Mandatory parameters must be configured before the SEPP deployment.
> - By default, the plmn-egress-gateway has a single 'default' route. To enable alternate routing, user must configure alternate routes manually through CNC Console or REST API. For more information, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide* and *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide.*

3.1.1 Global Parameters

This section includes information about the global parameters of the SEPP.

> **Note**
>
> The user can add multiple Network Load Balancer (NLB) annotations under the global section in the following format:
>
> ```
> global:
>   customExtension:
>     lbServices:
>       annotations:
>          oci-network-load-balancer.oraclecloud.com/security-list-
> management-mode: All
>          oci.oraclecloud.com/load-balancer-type: nlb
> ```
>
> All the services of type Load Balancer gets these annotations. User can also add annotations specific to a service under NF microservice section. The annotation example given here is OCI specific. It must be customized as per the platform.

Table 3-1 Global Parameters

Parameter	Description	Details
`dockerRegistry`	This is a mandatory parameter. This is the name of the docker registry where SEPPs docker images are available.	Data Type: String Range: It may contain lowercase letters, digits, and separators. A separator is defined as a period, one or two underscores, or one or more dashes. Default Value: reg-1
`dbCredSecretName`	This is a mandatory parameter. This attribute specifies the name of the Kubernetes secret object containing database` credentials.	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
`nameSpace`	This is a mandatory parameter. This attribute specifies the name of the deployed NF.	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
`asm.serviceMeshCheck`	To enable ASM for all services - change flag to true ASM setup: When serviceMeshCheck is enabled signature validation of certificate is skipped. There is no need to configure the certificate or the secret.	Data Type: Boolean Range: true false Default Value: false
`asm.istioSidecarQuitUrl`	This is a mandatory parameter. The sidecar (istio quit url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/quitquitquit

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
asm.istioSidecarReadyUrl	This is a mandatory parameter. The sidecar (istio ready url)when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/ready
mysql.primary.host	This is a mandatory parameter. This attribute specifies the IP address or hostname of the primary database connection service. SEPP connects to the primary database connection service. If the primary database connection service is unavailable, then SEPP connects to the secondary database connection service.	Data Type: String Range: NA Default Value: sepp-mysql-svc
mysql.primary.port	This is a mandatory parameter. This attribute specifies the port that is used while connecting to primary database connection service.	Data Type: Integer Range: NA Default Value: 3306
mysql.secondary.host	This is a mandatory parameter. This attribute specifies the IP address or hostname of the secondary database connection service. SEPP connects to the secondary database connection service only if the primary database connection service is unavailable. It again switches to the primary database connection service once it is available.	Data Type: String Range: NA Default Value: sepp-mysql-svc
mysql.secondary.port	This is a mandatory parameter. This attribute specifies the port that is used while connecting to secondary database connection service.	Data Type: Integer Range: NA Default Value: 3306
seppDbName	This is a mandatory parameter. It is the name of SEPP database.	Data Type: String Range: NA Default Value: seppdb
seppBackupDbName	This is a mandatory parameter. It is the name of SEPP Backup database. Defines backupdb name where backup will be created during upgrade	Data Type: String Range: NA Default Value: seppbackupdb

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
seppDbEngine	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or INNODB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
nfTypeMsgCpy	This is an optional Parameter. Identifies a type of producer NF.	Data Type: String Range: NA Default Value: SEPP
nfInstanceIdMsgCpy	This is an optional Parameter. Identifies a producer NF Instance.	Data Type: String Range: NA Default Value: 9faf1bbc-6e4a-4454-a507-aef01a101a06
nfFqdn	This is a mandatory parameter. This is the NF FQDN for SEPP.	Data Type: String Range: NA Default Value: sepp2.inter.oracle.com
hookJob.weight.subscription	When multiple resources are declared in a hook, they are executed sequentially. If hook weights are specified, execution follows the weight order (from negative to positive). Without weights, the execution order is not guaranteed.	Data Type: Integer Range: NA Default Value: 2
mediationService	This is a mandatory parameter. It is a flag to enable/disable mediation microservice. If set to true, mediation microservice will be deployed otherwise, it will not be deployed.	Data Type: Bolean Range: true or false Default Value: false
seppCoherenceServiceEnabled	This is a mandatory parameter. It is a flag to enable/disable coherence service. If set to true, coherence microservice will be deployed otherwise, it will not be deployed.	Data Type: Bolean Range: true or false Default Value: false
nrfClientHost	This parameter defines the service name of NRF Client NF discovery. It sends a UDR discovery request to the NRF to retrieve the UDR profile required for the Category-3 Previous Location Check feature.	Data Type: String Range: NA Default Value: ocsepp-release-sepp-nrf-client-nfdiscovery

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
nrfClientPort	This parameter defines the port number of NRF Client NF discovery service. It sends a UDR discovery request to the NRF to retrieve the UDR profile required for the Category-3 Previous Location Check feature.	Data Type: Integer Range: NA Default Value: 5910
supiPattern	This parameter defines the regular expression to extract the SUPI range from UDR Profile to select the FQDN which stores the information for the UE's falling in SUPI Range.	Data Type: String Range: NA Default Value: (?<=imsi-)[0-9]{15}
test.imageRepository	This is a mandatory parameter. Name of the Repository.	Data Type: String Range: NA Default Value:reg-1
test.nfName	This is a mandatory parameter. NF name on which the Helm test is performed. For SEPP, the default value is SEPP and is used in container name as suffix.	Data Type: String Range: NA Default Value: ocsepp
test.image.name	This is a mandatory parameter. Image name for the Helm test container image.	Data Type: String Range: NA Default Value: <release version>
test.image.tag	This is a mandatory parameter. Image version tag for Helm test. Image tag to be used for Helm test container.	Data Type: String Range: NA Default Value: <release version>
test.image.pullpolicy	This is a mandatory parameter. Image pull policy.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
test.config.logLevel	This is a mandatory parameter. Log level for Helm test pod.	Data Type: String Range: WARN INFO DEBUG Default Value: WARN
test.config.timeout	This is a mandatory parameter. Option timeout is the total time required for deployment of SEPP and Helm test to take place for checking the readiness probe of SEPP pods. If the timeout value exceeds, Helm test is considered as failure.	Data Type: Integer Range: Min-0, Max:65535 Unit: seconds Unit: seconds Default Value: 180

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
`test.complianceEnable`	This is a mandatory parameter. This field performs compliance check for each Kubernetes resource and Indicates whether or not the Kubernetes logging feature is enabled.	Data Type: Bolean Range: True or False Default Value: True
`test.k8resources`	This is a mandatory parameter. Kubernetes resources for which the API version information needs to be fetched.	Data Type: String Default Value: horizontalpodautoscalers/v1 • deployments/v1 • configmaps/v1 • prometheusrules/v1 • serviceaccounts/v1 • poddisruptionbudgets/v1 • roles/v1 • services/v1 • rolebindings/v1
`nrfClientEnabled`	This is a mandatory parameter. Whether nrf client services are required or not. If mode is nrfClientDisable / Roaming Hub then this value should be set to false.	Data Type: Boolean Range: true or false Default Value: true
`test.limits.memory`	This is an optional parameter. Specifies the maximum memory allocated.	Data Type: String Default Value: 1Gi
`podSecurityPolicy`	This is a mandatory parameter. This parameter allows for default security policies to be set on the cluster.	Data Type: String Range: DISABLED, ENABLED Default Value: DISABLED
`securityContextData`	This is a mandatory parameter. This parameter enables security Context settings such as runAsNonRoot, readOnlyRootFilesystem, runAsUser, runAsGroup.	Data Type: Boolean Range: DISABLED, ENABLED Default Value: ENABLED
`runAsNonRoot`	This is a mandatory parameter. This parameter is used to prevent containers from being run as the root user.	Data Type: Boolean Range: true or false Default Value: true
`readOnlyRootFilesystem`	This is a mandatory parameter. This setting is used to prevent write access to a container's root filesystem. **Note:** The parameter readOnlyRootFilesystem should be false for non occne setups- OKE, OCI etc.	Data Type: Boolean Range: true or false Default Value: true

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
`allowPrivilegeEscalation`	This is a mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the no_new_privs parameter gets configured on the container process. allowPrivilegeEscalation is always set to true when the container: • is run as privileged. • has CAP_SYS_ADMIN	Data Type: Boolean Range: true or false Default Value: false
`privileged`	This is a mandatory parameter. Provides mediation containers' access to the host's resources and kernel capabilities.	Data Type: Boolean Range: true or false Default Value: false
`runAsUser`	This is a mandatory parameter. This setting in Kubernetes is used to specify the user ID that should be used to run a container.	Data Type: Integer Default Value: 10012
`runAsGroup`	This is a mandatory parameter. This setting specifies the group ID under which the container's main process should run.	Data Type: Integer Default Value: 10012
`extraContainers`	This is a mandatory parameter. The flag can be used to enable or disable injecting extra container.	Data Type: String Range: DISABLED, ENABLED Default Value: DISABLED
`debugToolContainerMemoryLimit`	This is a mandatory parameter. Memory limit for debug tool container.	Data Type: String Range: NA Default Value: 4Gi
`extraContainersImageDetails.image`	This is a mandatory parameter. Docker image name.	Data Type: String Range: NA Default Value: ocdebugtool/ocdebug-tools
`extraContainersImageDetails.tag`	This is a mandatory parameter. Docker image tag.	Data Type: String Range: NA Default Value: debug_container_tag
`extraContainersImageDetails.imagePullPolicy`	This is a mandatory parameter. Image Pull Policy.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`extraContainersVolumesTpl.name`	This is a mandatory parameter. Name of the volume for debug tool logs storage.	Data Type: String Range: NA Default Value: debug-tools-dir

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
`extraContainersVolumesTpl.emptyDir.medium`	This is a mandatory parameter. Where emptyDir volume is stored.	Data Type: String Range: Memory Default Value: Memory
`extraContainersVolumesTpl.emptyDir.sizeLimit`	This is a mandatory parameter. emptyDir volume size.	Data Type: String Default Value:
`extraContainersTpl.command`	This is a mandatory parameter. String array used for container command.	Data Type: String Array Range: /bin/sleep infinity Default Value: /bin/sleep infinity
`extraContainersTpl.name`	This is a mandatory parameter. Name of the container.	Data Type: String Range: tools Default Value: tools
`extraContainersTpl.resources.requests.ephemeral-storage`	This is a mandatory parameter. Specifies the maximum amount of compute resources permitted, including limits on ephemeral storage. .	Data Type: String Range: NA Default Value: 512 Mi
`extraContainersTpl.resources.requests.cpu`	This is a mandatory parameter. CPU requests	Data Type: Integer Range: NA Default Value: 0.5
`extraContainersTpl.resources.requests.memory`	This is a mandatory parameter. Memory requests.	Data Type: String Range: NA Default Value:
`extraContainersTpl.resources.limits.ephemeral-storage`	This is a mandatory parameter. Limits define the maximum amount of compute resources allowed, including constraints on ephemeral storage.	Data Type: String Range: NA Default Value: 512 Mi
`extraContainersTpl.resources.limits.cpu`	This is a mandatory parameter. CPU requests	Data Type: Integer Range: NA Default Value: 1
`extraContainersTpl.resources.limits.memory`	This is a mandatory parameter. Memory requests	Data Type: String Range: NA Default Value:
`extraContainersTpl.securityContext.allowPrivilegeEscalation`	This is a mandatory parameter. AllowPrivilegeEscalation controls whether a process can gain more privileges than its parent process. This flag directly controls if the no_new_privs flag will be set on the container process.	Data Type: Boolean Range: true or false Default Value: true

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
`extraContainersTpl.securityContext.capabilities.drop`	This is a mandatory parameter. securityContext.capabilities is the capabilities to add/drop when running containers. Defaults to the default set of capabilities granted by the container runtime. Removed capabilities.	Data Type: String Range: ALL Default Value: ALL
`extraContainersTpl.securityContext.capabilities.add`	This is a mandatory parameter. securityContext.capabilities is the capabilities to add/drop when running containers. Defaults to the default set of capabilities granted by the container runtime. Added capabilities.	Data Type: String Range: NET_RAW NET_ADMIN Default Value: NET_RAW NET_ADMIN
`extraContainersTpl.securityContext.runAsUser`	This is an mandatory parameter. The UID to run the entrypoint of the container process.	Data Type: String Range: NA Default Value:
`extraContainersTpl.volumeMounts.mountPath`	This is an mandatory parameter. For mounting the volume.	Data Type: String Range: NA Default Value: /tmp/tools
`extraContainersTpl.volumeMounts.name`	This is an mandatory parameter. Name of the directory for debug tool logs storage	Data Type: String Range: NA Default Value: debug-tools-dir
`debugToolContainerMemoryLimit`	This is an optional parameter. Indicates the memory assigned for the debug tool container.	Data Type: String Default Value: 4Gi Range: NA
`extraContainersVolumesTpl`	This is an optional parameter. Specifies the extra container template for the debug tool volume.	Data Type: array Default Value: NA Range: NA
`extraContainersVolumesTpl.name`	This is an optional parameter. Indicates the name of the volume for debug tool logs storage.	Data Type: array Default Value: debug-tools-dir Range: NA
`extraContainersVolumesTpl.emptyDir.medium`	This is an optional parameter. Indicates the location where `emptyDir` volume is stored.	Data Type: array Default Value: Memory Range: NA
`extraContainersVolumesTpl.emptyDir.sizeLimit`	This is an optional parameter. Indicates the `emptyDir` volume size.	Data Type: array Default Value: Memory Range: NA
`customExtension.allResources.labels`	This is an optional parameter. Custom Labels that need to be added to all the SEPP Kubernetes resources	Data Type: String Range: NA Default Value: null

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
customExtension.allResources.annotations	This is an optional parameter. Custom Annotations that need to be added to all the OCSEPP Kubernetes resources.	Data Type: String Range: NA Default Value: null
customExtension.lbServices.labels	This is an optional parameter. Custom Labels that needs to be added to OCSEPP Services that are considered as Load Balancer type.	Data Type: String Range: NA Default Value: null
customExtension.lbServices.annotations	This is an optional parameter. Custom Annotations that needs to be added to OCSEPP Services that are considered as Load Balancer type.	Data Type: String Range: NA Default Value: null
customExtension.lbDeployments.labels	This is an optional parameter. Custom Labels that needs to be added to OCSEPP Deployments that are associated to a Service which is of Load Balancer type.	Data Type: String Range: NA Default Value: null
customExtension.lbDeployments.annotations	This is an optional Parameter. Custom Annotations that needs to be added to OCSEPP deployments that are associated to a Service which is of Load Balancer type.	Data Type: String Range: NA Default Value: {}
customExtension.nonlbServices.labels	This is an optional parameter. Custom Labels that needs to be added to OCSEPP Services that are considered as not Load Balancer type.	Data Type: String Range: NA Default Value: null
customExtension.nonlbServices.annotations	This is an optional parameter. Custom Annotations that needs to be added to OCSEPP Services that are considered as not Load Balancer type.	Data Type: String Range: NA Default Value: null
customExtension.nonlbDeployments.labels	This is an optional parameter. Custom Labels that needs to be added to OCSEPP Deployments that are associated to a Service which is not of Load Balancer type.	Data Type: String Range: NA Default Value: null
customExtension.nonlbDeployments.annotations	This is an optional Parameter. Custom Annotations that needs to be added to OCSEPP deployments that are associated to a Service which is not of Load Balancer type.	Data Type: String Range: NA Default Value: {}
KubernetesResource.container.prefix	This is an optional Parameter. Value that will be prefixed to all the container names of OCSEPP.	Data Type: String Range: NA Default Value: null

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
KubernetesResource.container.suffix	This is an optional Parameter. Value that will be suffixed to all the container names of OCSEPP.	Data Type: String Range: NA Default Value: null
configMgrPort	This is a mandatory parameter. SEPP config manager port number.	Data Type: Integer Range: NA Default Value: 9090
hookJobResources.limits.cpu	This is a mandatory parameter. This parameter indicates the resources that are given to hook jobs running for each microservice. Resource requirements (limit of CPU).	Data Type: Integer Range: NA Default Value: 2
hookJobResources.limits.memory	This is a mandatory parameter. This parameter indicates the resources that are given to hook jobs running for each microservice. Resource requirements (limit of memory).	Data Type: Integer Range: NA Default Value: 2Gi
hookJobResources.requests.cpu	This is a mandatory parameter. This parameter indicates the resources that are given to hook jobs running for each microservice. Resource Requirements (requests of CPU).	Data Type: Integer Range: NA Default Value: 1
hookJobResources.requests.memory	This is a mandatory parameter. This parameter indicates the resources that are given to hook jobs running for each microservice. Resource requirements(requests of memory).	Data Type: Integer Range: NA Default Value: 2Gi
Local Profile		
localProfile.name	This is a mandatory parameter. SEPP Local Profile Name.	Data Type: String Range: NA Default Value: SEPP-1
localProfile.plmnIdList	This is a mandatory parameter. List of local PLMN IDs supported by this network List in the form of MCC and MNC.	Data Type: String Range count: Minimum 1 and maximum 30 PLMNs Default Value: [{"mcc": "332","mnc": "221"}]
localProfile.sbiTargetApiRootSupported	This is a mandatory parameter. This parameter signifies whether 3gpp-sbitargte-api-root-header is supported by this SEPP or not.	Data Type: Boolean Range: True or False Default Value: True (for Oracle SEPP)
localProfile.n32cHandshakePlmnIdListValidationEnabled	This parameter is used to enable or disable PLMN ID List Validation in Exchange Capability Request/Response.	Data Type: Boolean Range: True or False Default Value: True (for Oracle SEPP)

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
localProfile.n32cHandshakePlmnIdListValidationType	This parameter indicate PLMN ID List Validation Type in Exchange Capability Request/Response.	Data Type: String Range: SUBSET/ STRICT Default Value: SUBSET
localProfile.n32cHandshakePlmnIdListSend	Indicates whether the list of PLMN IDs can be sent in the exchange capability request to Remote SEPP.	Data Type: Boolean Range: True or False Default Value: True for SEPP mode and False for Roaming hub mode.
localProfile.sanValidationRequired	This is an optional parameter. SAN validation is enabled for incoming capability-exchange handshake request or not.	Data Type: Boolean Range: True or False Default Value: True
localProfile.domain	This is a mandatory parameter. SEPP Local Domain.	Data Type: String Range: NA Default Value: svc.cluster.com
localProfile.seppViaVersion	This is a mandatory parameter. The version number of the SEPP local profile.	Data Type: String Range: NA Default Value: 2.0
localProfile.viaHeaderSeppViaInterFqdn	This is a mandatory parameter. This parameter is used to configure the inter FQDN for Network and will be used in via header N32F message to be sent to Remote SEPP.	Data Type: String Range: NA Default Value: 2.0 SEPP-sepp2.inter.oracle.com
localProfile.viaHeaderSeppViaIntraFqdn	This is a mandatory parameter. This parameter is used to configure the intra FQDN for Network and will be used in via header N32F message to be sent to NF in home network.	Data Type: String Range: NA Default Value: 2.0 SEPP-ocsepp-plmn-ingress-gateway.DEPLOYMENT_NAMESPACE
localProfile.interPlmnFqdn	This is a mandatory parameter. SEPP FQDN for Inter PLMN Access. This value should match with FQDN in ssl.conf file used for creating certificate.	Data Type: String Range: NA Default Value: sepp1.inter.oracle.com
localProfile.intraPlmnFqdn	This is a mandatory parameter. SEPP FQDN for Intra PLMN Access.	Data Type: String Range: NA Default Value: ocsepp-plmn-ingress-gateway.DEPLOYMENT_NAMESPACE
localProfile.supportedSecurityCapabilityList	This is a mandatory parameter. SEPP supported security capability (Only TLS is supported in this release).	Data Type: String Range: NA Default Value: TLS

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
localProfile.apiPrefix	This is an optional parameter. SEPP apiPrefix.	Data Type: String Range: NA Default Value: ""
localProfile.retryInterval	This is a mandatory parameter. SEPP Audit retry interval (For handshake Retry).	Data Type: Integer Range: NA Default Value: 300000 (In milli seconds)
localProfile.maxRetry	This is a mandatory parameter. SEPP Audit Max retry count (for handshake retry), Default is -1 means infinite.	Data Type: Integer Range: -1 means no limit on retry count. Mean infinite. Default Value: -1
localProfile.nfInstanceId	This is a mandatory parameter. SEPP NF Instance Id.	Data Type: String Range: NA Default Value: 9faf1bbc-6e4a-4454-a507-aef01a101a06
enableOpenTelemetry	This is an optional parameter. For enabling the open Telemetry for all SEPP services.	Data Type: Boolean Range: True or False Default Value: False
allowPrivilegeEscalation	This is a mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the no_new_privs parameter gets configured on the container process. allowPrivilegeEscalation is always set to true when the container: • is run as privileged. • has CAP_SYS_ADMIN.	Data Type: Boolean Range: True or False Default Value: False
privileged	This is a mandatory parameter. Provides mediation containers' access to the host's resources and kernel capabilities.	Data Type: Boolean Range: True or False Default Value: False
serviceAccountName	This is an optional parameter. This parameter povides the name of the already created single service account to be used by all the SEPP microservice. It has to be created by the user.	Data Type: String Range: NA Default Value: NA
atsSpecificDeployment	This is a mandatory parameter. This parameter is set to true if the SEPP is deploying for internal lab testing through ATS and not for production environment. Based on this variable certain timeout values will be set dynamically which are needed for ATS to run.	Data Type: Boolean Range: True or False Default Value: False

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
`atsSpecificTimeouts.n32fCacheRefreshTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets the following timeout values for cn32f and pn32f microservice of SEPP: • cacheRefreshTimeout • securityCacheRefreshTimeout • topologyhidingCacheRefreshTimeout • nrfDiscoveryCacheRefreshTimeout	Data Type: Integer Range: Default Value:1000
`atsSpecificTimeouts.n32fRequestTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets requestTimeout for cn32f and pn32f microservices of SEPP.	Data Type: Integer Range:NA Default Value: 2000
`atsSpecificTimeouts.egwRequestTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets requestTimeout for n32-egress-gateway and plmn-egress-gateway microservices of SEPP.	Data Type: Integer Range: Default Value: 2000
`atsSpecificTimeouts.igwRequestTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets requestTimeout for n32-ingress-gateway microservice of SEPP.	Data Type: Integer Range: Default Value: 5000
`atsSpecificTimeouts.pn32fEvictSanHeaderCacheDelay`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets evictSanHeaderCacheDelay for pn32f microservice of SEPP.	Data Type: Integer Range: Default Value: 100
`atsSpecificTimeouts.configMgrEgwRerouteAttempts`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets sbiRoutingErrorActionSets attempts of config-mgr service in case of alternate routing.	Data Type: Integer Range: Default Value: 3
`seppLciEnabledN32Ingress`	This is a mandatory parameter. If this parameter is set to true, LCI Header support over n32-ingress-gateway is enabled.	Data Type: Boolean Range: True or False Default Value: False

Table 3-1 (Cont.) Global Parameters

Parameter	Description	Details
seppOciEnabledN32Ingress	This is a mandatory parameter. If this parameter is set to true, OCI Header support over n32-ingress-gateway will be enabled.	Data Type: Boolean Range: True or False Default Value: False
seppLciEnabledPlmnIngress	This is a mandatory parameter. If this parameter is set to true, LCI Header support over plmn-ingress-gateway will be enabled.	Data Type: Boolean Range: True or False Default Value: False
seppOciEnabledPlmnIngress	This is a mandatory parameter. If this parameter is set to true, OCI Header support over plmn-ingress-gateway will be enabled.	Data Type: Boolean Range: True or False Default Value: False
egwPeerMonitoringThreshold	This is a mandatory parameter. This parameter is used to set success or failure threshold in peer monitoring configuration for proactive status update.	Data Type: Integer Range: NA Default Value: 1

3.1.2 cn32c-svc

This section includes information about the cn32c-svc parameters of the SEPP.

Table 3-2 cn32c-svc

Parameter	Description	Details
cn32c-svc.extraContainers	This is a mandatory parameter. Use 'extraContainers' attribute to control the usage of extra container(DEBU G tool). # If assigned with ENABLED or USE_GLOBAL_V ALUE, then ensure "extraContainers Tpl" Yaml chunk is defined # at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
cn32c-svc.image.repository	This is a mandatory parameter. Repo location of image.	Data Type: String Range: NA Default Value: reg-1
cn32c-svc.image.name	This is a mandatory parameter. Name of image.	Data Type: String Range: NA Default Value: ocsepp-cn32f-svc
cn32c-svc.image.tag	This is a mandatory parameter. Tag of image.	Data Type: String Range: NA Default Value: helm-tag

Table 3-2 (Cont.) cn32c-svc

Parameter	Description	Details
cn32c-svc.image.pullPolicy	This is a mandatory parameter. This setting indicates if the image needs to be pulled or not.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
cn32c-svc.minReplicas	This is a mandatory parameter. Minimum Number of Replicas.	Data Type: Integer Range: NA Default Value: 2
cn32c-svc.maxReplicas	This is a mandatory parameter. Maximum num of replicas of pod.	Data Type: Integer Range: NA Default Value: 2
cn32c-svc.log.root	This is a mandatory parameter. Root log level.	Data Type: String Range: WARN, INFO, DEBUG , ERROR Default Value: ERROR
cn32c-svc.log.sepp	This is a mandatory parameter. Sepp sepecific log level.	Data Type: String Range: WARN, INFO, DEBUG, ERROR Default Value: ERROR
cn32c-svc.resources.limit.cpu	This is a mandatory parameter. Resource Requirements(limit of cpu)	Data Type: Integer Range: NA Default Value: 2
cn32c-svc.resources.limit.memory	This is a mandatory parameter. Resource Requirements(limit of memory).	Data Type: Integer Range: NA Default Value: 2Gi
cn32c-svc.resources.requests.cpu	This is a mandatory parameter. Resource Requirements(requested cpu).	Data Type: Integer Range: NA Default Value: 2
cn32c-svc.resources.requests.memory	This is a mandatory parameter. Resource Requirements(requested memory).	Data Type: Integer Range: NA Default Value: 2Gi
cn32c-svc.resources.target.averageCpuUtil	This is a mandatory parameter. Resource Requirements(avg cpu utilisation).	Data Type: Integer Range: NA Default Value: 70
cn32c-svc.maxSurge	This is a mandatory parameter. The number of pods that can be created above the desired amount of pods during an update	Data Type: Integer Range: NA Default Value: 25%
cn32c-svc.maxUnavailable	This is a mandatory parameter. The number of pods that can be unavailable during an update.	Data Type: Integer Range: NA Default Value: 0%

Table 3-2 (Cont.) cn32c-svc

Parameter	Description	Details
cn32c-svc.pdbMaxUnavailable	This is a mandatory parameter. PDB limits the number of Pods of a replicated application that are down simultaneously from voluntary disruptions.	Data Type: Integer Range: NA Default Value: 25%
cn32c-svc.bodyInTraceEnabled	This is an optional parameter. Enables openTelemetry trace for Body.	Data Type: boolean Range: true or false Default Value: false
cn32c-svc.openTelemetry.jaeger.httpExporter.host	This is an optional parameter. openTelemetry host	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
cn32c-svc.openTelemetry.jaeger.httpExporter.port	This is an optional parameter. openTelemetry port	Data Type: Integer Range: NA Default Value: 4318
cn32c-svc.openTelemetry.jaeger.logSpans	This is an optional parameter. openTelemetry logspans	Data Type: boolean Range: true or false Default Value: false
cn32c-svc.openTelemetry.jaeger.probabilisticSamplingRate	This is an optional parameter. Trace capture in percentage	Data Type: Float Range: NA Default Value: 0.5 (Note: it means 50%)
cn32c-svc.nameSpace	This is a mandatory parameter. This parameter is used for displaying namespace and corresponding service name from where the traces are generated.	Data Type: String Range: NA Default Value: Value will be deployment namespace as per custom-values.yaml file.
cn32c-svc.enableOpenTelemetry	This is an optional parameter. This parameter enables the openTelemetry.	Data Type: boolean Range: true or false Default Value: false
cn32c-svc.service.active.svcPortHttp	This is a mandatory parameter. It defines the http port for cn32c service.	Data Type: Integer Range: NA Default Value: 8081
cn32c-svc.service.active.svcPortHttps	This is a mandatory parameter. It defines the https port for cn32c service.	Data Type: Integer Range: NA Default Value: 8082
cn32c-svc.service.active.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range: NA Default Value: 8085
cn32c-svc.service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to cn32c specific Service.	Data Type: String Range: NA Default Value: { }

Table 3-2 (Cont.) cn32c-svc

Parameter	Description	Details
cn32c-svc.service.customExtension.anotations	This is an optional parameter. Custom Annotations that needs to be added to cn32c specific Services.	Data Type: String Range: NA Default Value: { }
cn32c-svc.deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to cn32c specific Deployment	Data Type: String Range: NA Default Value: { }
cn32c-svc.deployment.customExtension.annotations	This is an optional parameter.Custom Annotations that needs to be added to cn32c specific Deployment.	Data Type: String Range: NA Default Value: { }
cn32c-svc.resources.requests.ephemeralStorage	This is an optional parameter. pods and containers can require ephemeral storage for their operation.	Data Type: String Range: depends on cluster resources Default Value: 70Mi
cn32c-svc.resources.limits.ephemeralStorage	This is an optional parameter. Pods use ephemeral local storage for scratch space, caching, and logs.	Data Type: String Range: depends on cluster Resources Default Value: 1Gi
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	Data Type: Integer Default Value: 30000ms

3.1.3 pn32c-svc

This section includes information about the pn32c-svc parameters of the SEPP.

Table 3-3 pn32c-svc

Parameter	Description	Details
pn32c-svc.extraContainers	This is a mandatory parameter. Use 'extraContainers' attribute to control the usage of extra container(DEBU G tool). # If assigned with ENABLED or USE_GLOBAL_V ALUE, then ensure "extraContainers Tpl" Yaml chunk is defined # at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: ENUM Range : DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
pn32c-svc.image.repository	This is a mandatory parameter.Repo location of image	Data Type: String Range : NA Default Value: reg-1

Table 3-3 (Cont.) pn32c-svc

Parameter	Description	Details
pn32c-svc.image.name	This is a mandatory parameter.Name of image	Data Type: String Range : NA Default Value: ocsepp-pn32c-svc
pn32c-svc.image.tag	This is a mandatory parameter.Tag of image	Data Type: String Range : NA Default Value: helm-tag
pn32c-svc.image.pullPolicy	This is a mandatory parameter.This setting indicates if the image needs to be pulled or not	Data Type: String Range : NA Default Value: Always
pn32c-svc.minReplicas	This is a mandatory parameter.Minimum Number of Replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range : NA Default Value: 2
pn32c-svc.maxReplicas	This is a mandatory parameter.Maximum num of replicas of pod to scale to maintain an average CPU utilisation	Data Type: Integer Range : NA Default Value: 2
pn32c-svc.maxSurge	This is a mandatory parameter. The number of pods that can be created above the desired amount of pods during an update	Data Type: Integer Range : NA Default Value: 25%
pn32c-svc.maxUnavailable	This is a mandatory parameter. The number of pods that can be unavailable during an update	Data Type: Integer Range : NA Default Value: 0%
pn32c-svc.pdbMaxUnavailable	This is a mandatory parameter. PDB limits the number of Pods of a replicated application that are down simultaneously from voluntary disruptions.	Data Type: Integer Range : NA Default Value: 25%
pn32c-svc.log.root	This is a mandatory parameter. Root log level	Data Type: String Range: WARN, INFO, DEBUG, ERROR Default Value: ERROR
pn32c-svc.log.sepp	This is a mandatory parameter. Sepp specific log level	Data Type: String Range: WARN, INFO, DEBUG, ERROR Default Value: ERROR
pn32c-svc.resources.limit.cpu	This is a mandatory parameter. Resource Requirements(limit of cpu)	Data Type: Integer Range : NA Default Value: 2
pn32c-svc.resources.limit.memory	This is a mandatory parameter. Resource Requirements(limit of memory)	Data Type: String Range : NA Default Value: 2Gi

Table 3-3 (Cont.) pn32c-svc

Parameter	Description	Details
pn32c-svc.resources.requests.cpu	This is a mandatory parameter. Resource Requirements(requested cpu)	Data Type: Integer Range : NA Default Value: 1
pn32c-svc.resources.requests.memory	This is a mandatory parameter. Resource Requirements(requested memory)	Data Type: String Range : NA Default Value: 1Gi
pn32c-svc.resources.target.averageCpuUtil	This is a mandatory parameter. Resource Requirements(avg cpu utilisation)	Data Type: Integer Range : NA Default Value: 50
pn32c-svc.service.active.svcPortHttp	This is a mandatory parameter. It defines the http port for pn32c service	Data Type: Integer Range : NA Default Value: 8083
pn32c-svc.service.active.svcPortHttps	This is a mandatory parameter. It defines the https port for pn32c service	Data Type: Integer Range : NA Default Value: 8084
pn32c-svc.service.active.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range : NA Default Value: 8085
pn32c-svc.configs.sanHeaderName	This is a mandatory parameter. Header name to use to pick SAN values at PN32F	Data Type: String Range : NA Default Value: x-custom-ingress-client-identity
pn32c-svc.configs.extractSANRegex	This is a mandatory parameter. Regex expression to use to extract SAN values at PN32F	Data Type: String Range : NA Default Value: SAN=(.*)\\s
pn32c-svc.configs.extractSANDelimiter	This is a mandatory parameter. Delimiter used for extracting SAN values at PN32F	Data Type: String Range : NA Default Value: ","
pn32c-svc.jaegerTracingEnabled	This is an optional parameter. Enable Jaeger trace	Data Type: boolean Range: true or false Default Value: false
pn32c-svc.bodyInTraceEnabled	This is an optional parameter. Enable Jaeger trace for Body	Data Type: boolean Range: true or false Default Value: false
pn32c-svc.openTelemetry.jaeger.httpExporter.host	This is an optional parameter. openTelemetry host	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra

Table 3-3 (Cont.) pn32c-svc

Parameter	Description	Details
pn32c-svc.openTelemetry.jaeger.httpExporter.port	This is an optional parameter. openTelemetry port	Data Type: Integer Range: NA Default Value: 4318
pn32c-svc.openTelemetry.jaeger.logSpans	This is an optional parameter. openTelemetry logspans	Data Type: boolean Range: true or false Default Value: false
pn32c-svc.openTelemetry.jaeger.probabilisticSamplingRate	This is an optional parameter. Trace capture in percentage	Data Type: Float Range: NA Default Value: 0.5 (Note: it means 50%)
pn32c-svc.nameSpace	This is a mandatory parameter. This parameter is used for displaying namespace and corresponding service name from where the traces are generated.	Data Type: String Range: NA Default Value: Value will be deployment namespace as per custom-values.yaml file.
pn32c-svc.enableOpenTelemetry	This is an optional parameter. This parameter enables the openTelemetry.	Data Type: boolean Range: true or false Default Value: false
pn32c-svc.service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to pn32c specific Services	Data Type: String Range : NA Default Value:
pn32c-svc.service.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to pn32c specific Services	Data Type: String Range : NA Default Value:
pn32c-svc.deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to pn32c specific Deployment	Data Type: String Range : NA Default Value:
pn32c-svc.deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to pn32c specific Deployment	Data Type: String Range : NA Default Value:
pn32c-svc.resources.requests.ephemeralStorage	This is an optional parameter. pods and containers can require ephemeral storage for their operation.	Data Type: String Range: depends on cluster resources Default Value: 75Mi
pn32c-svc.resources.limits.ephemeralStorage	This is an optional parameter. Pods use ephemeral local storage for scratch space, caching, and logs.	Data Type: String Range: depends on cluster Resources Default Value: 1Gi
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	Data Type: Integer Default Value: 30000ms

3.1.4 cn32f-svc

This section includes information about the cn32f-svc parameters of the SEPP.

Table 3-4 cn32f-svc

Parameter	Description	Details
`cn32f-svc.extraContainers`	This is a mandatory parameter. Use 'extraContainers' attribute to control the usage of extra container(DEBU G tool). # If assigned with ENABLED or USE_GLOBAL_V ALUE, then ensure "extraContainers Tpl" Yaml chunk is defined # at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
`cn32f-svc.image.repository`	This is a mandatory parameter.Repo location of image	Data Type: String Range : NA Default Value: reg-1
`cn32f-svc.image.name`	This is a mandatory parameter.Name of image	Data Type: String Range : NA Default Value: ocsepp-cn32f-svc
`cn32f-svc.image.tag`	This is a mandatory parameter.Tag of image	Data Type: String Range : NA Default Value: helm-tag
`cn32f-svc.image.pullPolicy`	This is a mandatory parameter.This setting indicates if the image needs to be pulled or not	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`cn32f-svc.minReplicas`	This is a mandatory parameter.Minimum Number of Replicas for cn32f service	Data Type: Integer Range : NA Default Value: 14
`cn32f-svc.maxReplicas`	This is a mandatory parameter.Maximum num of replicas for cn32f service	Data Type: Integer Range : NA Default Value: 14
`cn32f-svc.log.root`	This is a mandatory parameter.Root log level	Data Type: String Range: WARN, INFO, DEBUG, ERROR Default Value: ERROR
`cn32f-svc.log.sepp`	This is a mandatory parameter.Sepp specific log level	Data Type: String Range: WARN, INFO, DEBUG,ERROR Default Value: ERROR
`cn32f-svc.resources.limit.cpu`	This is a mandatory parameter.Resource Requirements(limit of cpu)	Data Type: Integer Range : NA Default Value: 5

Table 3-4 (Cont.) cn32f-svc

Parameter	Description	Details
cn32f-svc.resources.limit.memory	This is a mandatory parameter.Resource Requirements(limit of memory)	Data Type: String Range : NA Default Value: 8Gi
cn32f-svc.resources.limit.ephemeralStorage	This is an optional parameter.Pods use ephemeral local storage for scratch space, caching, and logs.	Data Type: String Range : NA Default Value: 1Gi
cn32f-svc.resources.requests.cpu	This is a mandatory parameter.Resource Requirements(requested cpu)	Data Type: Integer Range : NA Default Value: 5
cn32f-svc.resources.requests.memory	This is a mandatory parameter.Resource Requirements(requested memory)	Data Type: String Range : NA Default Value: 8Gi
cn32f-svc.resources.target.averageCpuUtil	This is a mandatory parameter.Resource Requirements(avg cpu utilisation)	Data Type: Integer Range : NA Default Value: 70
cn32f-svc.maxSurge	This is a mandatory parameter. The number of pods that can be created above the desired amount of pods during an update	Data Type: Integer Range : NA Default Value: 25%
cn32f-svc.maxUnavailable	This is a mandatory parameter. The number of pods that can be unavailable during an update	Data Type: Integer Range : NA Default Value: 0%
cn32f-svc.pdbMaxUnavailable	This is a mandatory parameter. PDB limits the number of Pods of a replicated application that are down simultaneously from voluntary disruptions.	Data Type: Integer Range : NA Default Value: 25%
cn32f-svc.service.active.svcPortHttp	This is a mandatory parameter. This is the http port number for cn32f service	Data Type: Integer Range : NA Default Value: 9090
cn32f-svc.service.active.svcPortHttps	This is a mandatory parameter. This is the https port number for cn32f service	Data Type: Integer Range : NA Default Value: 9091
cn32f-svc.service.active.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range : NA Default Value: 8085
cn32f-svc.service.customExtension.labels	This is an optional parameter. Indicates the Custom Labels that needs to be added to cn32f specific Service	Data Type: String Range : NA Default Value: { }

Table 3-4 (Cont.) cn32f-svc

Parameter	Description	Details
cn32f-svc.service.customExtension.annotations	This is an optional parameter. Indicates the Custom Annotations that needs to be added to cn32f specific Services	Data Type: String Range : NA Default Value: { }
cn32f-svc.deployment.customExtension.labels	This is an optional parameter. Indicates the Custom Labels that needs to be added to cn32f specific deployments.	Data Type: String Range : NA Default Value: { }
cn32f-svc.deployment.customExtension.annotations	This is an optional parameter. Indicates the Custom Annotations that needs to be added to cn32f specific deployments.	Data Type: String Range : NA Default Value: { }
cn32f-svc.hostedSepp.RequestRejectStatusCodeName	This is a mandatory parameter. Defines global error reason for Hosted SEPP	Data Type: Integer Range : 400, 403 and 406. 401 is not an allowed value Default Value: 400
cn32f-svc.hostedSepp.RequestRejectReasonName	This is a mandatory parameter. Defines global error reason for Hosted SEPP	Data Type: String Range : NA Default Value: Allowed Producer Remote SEPP Set routing failure
cn32f-svc.bodyInTraceEnabled	This is an optional parameter.Enable Jaeger trace for Body	Data Type: boolean Range: true or false Default Value: false
cn32f-svc.openTelemetry.jaeger.httpExporter.port	This is an optional parameter. openTelemetry port	Data Type: Integer Range: NA Default Value: 4318
cn32f-svc.openTelemetry.jaeger.logSpans	This is an optional parameter. openTelemetry logspans	Data Type: boolean Range: true or false Default Value: false
cn32f-svc.openTelemetry.jaeger.probabilisticSamplingRate	This is an optional parameter. Trace capture in percentage	Data Type: Float Range: NA Default Value: 0.5 (Note: it means 50%)
cn32f-svc.nameSpace	This is a mandatory parameter. This parameter is used for displaying namespace and corresponding service name from where the traces are generated.	Data Type: String Range: NA Default Value: Value will be deployment namespace as per custom-values.yaml file.
cn32f-svc.enableOpenTelemetry	This is an optional parameter. This parameter enables the openTelemetry.	Data Type: boolean Range: true or false Default Value: false

Table 3-4 (Cont.) cn32f-svc

Parameter	Description	Details
cn32f-svc.openTracing.jaeger.probabilisticSamplingRate	This is an optional parameter.Trace capture in percentage	Data Type: String Range : NA Default Value: 0.5 (Note: it means 50%)
cn32f-svc.configs.is3gppSbiTargetApiRootSchemeHttp	This is a mandatory parameter. It indicated the http scheme to be used in 3gpp-sbi-target-apiroot header. true indicates http and false indicates https	Data Type: Boolean Range: True or False Default Value: True (for Oracle SEPP)
cn32f-svc.configs.cacheRefreshTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database.	Data Type: Integer Range : NA Default Value:30,000 (ms)
cn32f-svc.configs.cacheRefreshInitTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database at Init time.	Data Type: Integer Range : NA Default Value:5000 (ms)
cn32f-svc.configs.securityCacheRefreshTimeout	This is a mandatory parameter. (If Security Countermeasure Feature is enabled) Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration.	Data Type: Integer Range : NA Default Value:30,000 (ms)
cn32f-svc.configs.securityCacheRefreshInitTimeout	This is a mandatory parameter. (If Security Countermeasure Feature is enabled) Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration at the Init time when Application comes up.	Data Type: Integer Range : NA Default Value:50,000 (ms)
cn32f-svc.topologyHiding.timerConfig.topologyhidingCacheRefreshTimeout	This is a mandatory parameter. (If Topology hiding Feature is enabled) Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration. This is a cache refresh value which triggers every time at a regular interval with a given configured value. This will keeps on making the cache data in sync with database.	Data Type: Integer Range : NA Default Value:30,000 (ms)

Table 3-4 (Cont.) cn32f-svc

Parameter	Description	Details
cn32f-svc.topologyHiding.timerConfig.topologyhidingCacheRefreshInitTimeout	This is a mandatory parameter. (If Topology hiding Feature is enabled) Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration at the Init time when Application comes up.	Data Type: Integer Range : NA Default Value:50,000 (ms)
cn32f-svc.topologyHiding.timerConfig.topologyhidingHistoryUpdateTimeout	This is a mandatory parameter. (If Topology hiding Feature is enabled) This is the Time for the old entries to be removed from cache. Entries older than topologyhidingHistoryRefreshSeconds are purged. In case actual pseudo mapping is deleted, then we still support initial holding of the deleted values to support the messages in progress. This cache keeps on updating with given configured value.	Data Type: Integer Range : NA Default Value:30,000 (ms)
cn32f-svc.topologyHiding.timerConfig.topologyhidingHistoryRefreshSeconds	This is a mandatory parameter. (If Topology hiding Feature is enabled) This is the value which signifies how long the message should be used in cache once it get deleted from the actual to pseudo mapping.	Data Type: Integer Range : NA Default Value:60 (sec)
cn32f-svc.topologyHiding.config.topologyHidingStateCheck	This is a mandatory parameter. This is the value used like if request is unhiding some identifier and in response if we want to hide the identifier with the same value.	Data Type: String Range : NA Default Value:true
cn32f-svc.connectionTimeout	This is Jetty Client Settings. This is a mandatory parameter. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	Data Type: Integer Range : NA Default Value:10,000 (ms)

Table 3-4 (Cont.) cn32f-svc

Parameter	Description	Details
cn32f-svc.dnsRefreshDelay	This is Jetty Client Settings. This is a mandatory parameter. This value represents the Time taken to refresh the DNS entries for a destination	Data Type: Integer Range : NA Default Value:10,000 (ms)
cn32f-svc.requestTimeout	This is Jetty Client Settings. This is a mandatory parameter. Request timeout is the maximum time that can be taken to process HTTP request after the connection is established. Sum of time to process request plus ConnectionTimeout and should always be greater than Connection Timeout.	Data Type: Integer Range : NA Default Value:10,000 (ms)
cn32f-svc.serverMaxConcurrentStreams	This is a mandatory parameter. Max Concurrent Stream sent by PN32F in HTTP2 Settings Frame	Data Type: Integer Range : NA Default Value: 100
cn32f-svc.serverInitialWindowSize	This is a mandatory parameter. Server Initial Window Size sent by PN32F in HTTP2 Settings Frame	Data Type: Integer Range : NA Default Value: 65534
cn32f-svc.mediation.mediationRequestTimeout	This is a conditional parameter. N32f service will wait for mediation service response for mediationRequestTimeout time before sending error message, if mediation service is unreachable	Data Type: Integer Range : NA Default Value: 900 (ms)
cn32f-svc.mediation.header.mediationRequestRejectStatusCodeHeaderName	This is a conditional parameter. The name of the header added in response that will depict that n32f service has to reject this request and value of this header indicates the error code to be returned.	Data Type: String Range : NA Default Value: ocsepp-reject-status
cn32f-svc.mediation.header.mediationRequestRejectReasonHeaderName	This is a conditional parameter. The name of the header added in response that will depict that n32f service has to reject this request and value of this header indicates the error reason/detail to be returned.	Data Type: String Range : NA Default Value: ocsepp-reject-reason
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	Data Type: Integer Default Value: 30000ms

Table 3-4 (Cont.) cn32f-svc

Parameter	Description	Details
payloadSizeLimit	This is a mandatory parameter. This parameter represents the maximum payload size in bytes. Any payload greater than the given limit results the error code HTTP 413. The maximum configurable limit is 2147483647 byte.	Data Type: Integer Default Value: 262144 bytes

3.1.5 pn32f-svc

This section includes information about the pn32f-svc parameters of the SEPP.

Table 3-5 pn32f-svc

Parameter	Description	Details
pn32f-svc.extraContainers	This is a mandatory parameter. Use 'extraContainers' attribute to control the usage of extra container(DEBU G tool). # If assigned with ENABLED or USE_GLOBAL_V ALUE, then ensure "extraContainers Tpl" Yaml chunk is defined # at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
pn32f-svc.image.repository	This is a mandatory parameter.Repo location of image	Data Type: String Range: NA Default Value: reg-1
pn32f-svc.image.name	This is a mandatory parameter.Name of image	Data Type: String Range: NA Default Value: ocsepp-pn32f-svc
pn32f-svc.image.tag	This is a mandatory parameter.Tag of image	Data Type: String Range: NA Default Value: helm-tag
pn32f-svc.image.pullPolicy	This is a mandatory parameter.This setting indicates if the image needs to be pulled or not	Data Type: String Range: NA Default Value: Always
pn32f-svc.log.root	This is a mandatory parameter.Root log level	Data Type: String Range: WARN, INFO, DEBUG, ERROR Default Value: ERROR

Table 3-5 (Cont.) pn32f-svc

Parameter	Description	Details
pn32f-svc.log.sepp	This is a mandatory parameter.Sepp specific log level	Data Type: String Range: WARN, INFO, DEBUG, ERROR Default Value: ERROR
pn32f-svc.minReplicas	This is a mandatory parameter.Minimum Number of Replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
pn32f-svc.maxReplicas	This is a mandatory parameter.Maximum num of replicas of pod to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
pn32f-svc.resources.limit.cpu	This is a mandatory parameter.Resource Requirements(limit of cpu)	Data Type: Integer Range: NA Default Value: 5
pn32f-svc.resources.limit.memory	This is a mandatory parameter.Resource Requirements(limit of memory)	Data Type: String Range: NA Default Value: 8Gi
pn32f-svc.resources.requests.cpu	This is a mandatory parameter.Resource Requirements(requested cpu)	Data Type: Integer Range: NA Default Value: 5
pn32f-svc.resources.requests.memory	This is a mandatory parameter.Resource Requirements(requested memory)	Data Type: String Range: NA Default Value: 8Gi
pn32f-svc.resources.target.averageCpuUtil	This is a mandatory parameter.Resource Requirements(avg cpu utilisation)	Data Type: Integer Range: NA Default Value: 70
pn32f-svc.maxSurge	This is a mandatory parameter. The number of pods that can be created above the desired amount of pods during an update	Data Type: Integer Range: NA Default Value: 25%
pn32f-svc.maxUnavailable	This is a mandatory parameter. The number of pods that can be unavailable during an update	Data Type: Integer Range: NA Default Value: 0%
pn32f-svc.pdbMaxUnavailable	This is a mandatory parameter. PDB limits the number of Pods of a replicated application that are down simultaneously from voluntary disruptions.	Data Type: Integer Range: NA Default Value: 25%
pn32f-svc.hostedSepp.RequestRejectStatusCodeName	This is a mandatory parameter. Defines global error code for Hosted SEPP	Data Type: Integer Range: 400, 403 and 406. 401 is not an allowed value Default Value: 400

Table 3-5 (Cont.) pn32f-svc

Parameter	Description	Details
pn32f-svc.hostedSepp.RequestRejectReasonName	This is a mandatory parameter. Defines global error reason for Hosted SEPP	Data Type: String Range: NA Default Value: Allowed Producer Remote SEPP Set routing failure
pn32f-svc.jaegerTracingEnabled	This is an optional parameter.To Enable Jaeger trace	Data Type: boolean Range: true or false Default Value: false
pn32f-svc.openTelemetry.jaeger.httpExporter.port	This is an optional parameter. openTelemetry port	Data Type: Integer Range: NA Default Value: 4318
pn32f-svc.openTelemetry.jaeger.logSpans	This is an optional parameter. openTelemetry logspans	Data Type: boolean Range: true or false Default Value: false
pn32f-svc.openTelemetry.jaeger.probabilisticSamplingRate	This is an optional parameter. Trace capture in percentage	Data Type: Float Range: NA Default Value: 0.5 (Note: it means 50%)
pn32f-svc.nameSpace	This is a mandatory parameter. This parameter is used for displaying namespace and corresponding service name from where the traces are generated.	Data Type: String Range: NA Default Value: Value will be deployment namespace as per custom-values.yaml file.
pn32f-svc.enableOpenTelemetry	This is an optional parameter. This parameter enables the openTelemetry.	Data Type: boolean Range: true or false Default Value: false
pn32f-svc.openTelemetry.jaeger.httpExporter.host	This is an optional parameter. openTelemetry host	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
pn32f-svc.configs.is3gppSbiTargetApiRootSchemeHttp	This is a mandatory parameter. Indicates scheme to be used for egress SBI request 3gpp-Sbi-Target-apiRoot header in absence of 3gpp-Sbi-Target-apiRoot header in the ingress SBI request. This is applicable only when 3gpp-Sbi-Target-apiRoot is supported for egress SBI request. true indicates http and false indicates https	Data Type: Boolean Range: true or false Default Value:true
pn32f-svc.configs.cacheRefreshTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database.	Data Type: Integer Range: NA Default Value:30,000 (ms)

Table 3-5 (Cont.) pn32f-svc

Parameter	Description	Details
pn32f-svc.configs.cacheRefreshInitTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database at Init time.	Data Type: Integer Range: NA Default Value:5000 (ms)
pn32f-svc.configs.securityCacheRefreshTimeout	This is a mandatory parameter. (If Security Countermeasure Feature is enabled) Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration.	Data Type: Integer Range: NA Default Value:30,000 (ms)
pn32f-svc.configs.securityCacheRefreshInitTimeout	This is a mandatory parameter. (If Security Countermeasure Feature is enabled) Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration at the Init time when Application comes up.	Data Type: Integer Range: NA Default Value:50,000 (ms)
pn32f-svc.configs.evictSanHeaderCacheDelay	This is a mandatory parameter. This parameter defines the timer value after which San Header Cache gets cleared out and updated with new N32F Context (if added).	Data Type: Integer Range: NA Default Value:50,000 (ms) Note: In ATS setup, set the value as 100.
pn32f-svc.configs.nrfDiscoveryCacheRefreshTimeout	This is a mandatory parameter. This parameter defines the timer value when UDR Discovery request will be triggered if coherence map containing UDR Profile information is empty. After this timer expiry, UDR Discovery request will be initiated by NRF Client towards NRF.	Data Type: Integer Range: NA Default Value:30,000 (ms) Note: In ATS setup, set the value as 10.
pn32f-svc.configs.nrfDiscoveryCacheRefreshInitTimeout	This is a mandatory parameter. This parameter defines the timer value after which UDR Discovery request will be triggered at SEPP INIT Time. After this timer expiry, UDR Discovery request will be initiated by NRF Client towards NRF.	Data Type: Integer Range: NA Default Value:5,000 (ms)
pn32f-svc.configs.sanHeaderName	This is a mandatory parameter. Header name to use to pick SAN values at PN32F	Data Type: String Range: NA Default Value: x-custom-ingress-client-identity

Table 3-5 (Cont.) pn32f-svc

Parameter	Description	Details
pn32f-svc.configs.extractSANRegex	This is a mandatory parameter. Regex expression to use to extract SAN values at PN32F	Data Type: String Range: NA Default Value: SAN=(.*)\\s
pn32f-svc.configs.extractSANDelimiter	This is a mandatory parameter. Delimiter used for extracting SAN values at PN32F	Data Type: String Range: NA Default Value: ","
pn32f-svc.topologyHiding.timerConfig.topologyhidingCacheRefreshTimeout	This is a mandatory parameter. (If Topology hiding Feature is enabled) Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration.	Data Type: Integer Range: NA Default Value:30,000 (ms)
pn32f-svc.topologyHiding.timerConfig.topologyhidingCacheRefreshInitTimeout	This is a mandatory parameter. (If Topology hiding Feature is enabled) Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration at the Init time when Application comes up.	Data Type: Integer Range: NA Default Value:50,000 (ms)
pn32f-svc.topologyHiding.timerConfig.topologyhidingHistoryUpdateTimeout	This is a mandatory parameter. (If Topology hiding Feature is enabled) This is the Time for the old entries to be removed from cache. Entries older than topologyhidingHistoryRefreshSeconds are purged.	Data Type: Integer Range: NA Default Value:30,000 (ms)
pn32f-svc.topologyHiding.timerConfig.topologyhidingHistoryRefreshSeconds	This is a mandatory parameter. (If Topology hiding Feature is enabled) This value represents the Time until old Topology Hiding feature entries are kept in cache.	Data Type: Integer Range: NA Default Value:60 (sec)
pn32f-svc.topologyHiding.config.topologyHidingStateCheck	This is a mandatory parameter. This is the value used like if request is unhiding some identifier and in response if we want to hide the identifier with the same value.	Data Type: Boolean Range: True or False Default Value: true

Table 3-5 (Cont.) pn32f-svc

Parameter	Description	Details
pn32f-svc.connectionTimeout	This is Jetty Client Settings. This is a mandatory parameter. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	Data Type: Integer Range: NA Default Value: 60(ms)
pn32f-svc.dnsRefreshDelay	This is Jetty Client Settings. This is a mandatory parameter. This value represents the Time taken to refresh the DNS entries for a destination	Data Type: Integer Range: NA Default Value: 10,000 (ms)
pn32f-svc.requestTimeout	This is Jetty Client Settings. This is a mandatory parameter. This value represents the Time to wait for the response.	Data Type: Integer Range: NA Default Value: 600 (ms)
pn32f-svc.serverMaxConcurrentStreams	This is a mandatory parameter. Max Concurrent Stream sent by PN32F in HTTP2 Settings Frame	Data Type: Integer Range: NA Default Value: 100
pn32f-svc.serverInitialWindowSize	This is a mandatory parameter. Server Initial Window Size sent by PN32F in HTTP2 Settings Frame	Data Type: Integer Range: NA Default Value: 65534
pn32f-svc.mediation.mediationRequestTimeout	This is a conditional parameter. N32f service will wait for mediation service response for mediationRequestTimeout time before sending error message, if mediation service is unreachable	Data Type: Integer Range: NA Default Value: 900 (ms)
pn32f-svc.mediation.header.mediationRequestRejectStatusCodeHeaderName	This is a conditional parameter. The name of the header added in response that will depict that n32f service has to reject this request and value of this header indicates the error code to be returned.	Data Type: String Range: NA Default Value: ocsepp-reject-status
pn32f-svc.mediation.header.mediationRequestRejectReasonHeaderName	This is a conditional parameter. The name of the header added in response that will depict that n32f service has to reject this request and value of this header indicates the error reason/detail to be returned.	Data Type: String Range: NA Default Value: ocsepp-reject-reason
nrfconfiguration.service.type	This is an optional parameter. Kind of Service that will be used for this Deployment	Data Type: String Default Value:

Table 3-5 (Cont.) pn32f-svc

Parameter	Description	Details
pn32f-svc.service.active.svcPortHttp	This is a mandatory parameter. It defines the http port for pn32f service	Data Type: Integer Range: NA Default Value: 9090
pn32f-svc.service.active.svcPortHttps	This is a mandatory parameter. It defines the https port for pn32f service	Data Type: Integer Range: NA Default Value: 9091
pn32f-svc.service.active.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range: NA Default Value: 8085
pn32f-svc.service.customExtension.labels	This is an optional parameter.Custom Labels that needs to be added to pn32f specific Service	Data Type: String Range: NA Default Value: { }
pn32f-svc.service.customExtension.annotations	This is an optional parameter.Custom Annotations that needs to be added to pn32f specific Services	Data Type: String Range: NA Default Value: { }
pn32f-svc.deployment.customExtension.labels	This is an optional parameter.Custom Labels that needs to be added to pn32f specific Deployment	Data Type: String Range: NA Default Value: { }
pn32f-svc.deployment.customExtension.annotations	This is an optional parameter.Custom Annotations that needs to be added to pn32f specific Deployment	Data Type: String Range: NA Default Value: { }
pn32f-svc.resources.requests.ephemeralStorage	This is an optional parameter.pods and containers can require ephemeral storage for their operation.	Data Type: String Range: depends on cluster resources Default Value: 70Mi
pn32f-svc.resources.limits.ephemeralStorage	This is an optional parameter.Pods use ephemeral local storage for scratch space, caching, and logs.	Data Type: String Range: depends on cluster Resources Default Value: 1G
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	Data Type: Integer Default Value: 30000ms
suciPattern	This is a Mandatory Parameter. This is an SUCI routing indicator pattern that is used to extract the routing indicator.	Datatype: String Example: `suciPattern: (?<=suci-0-[0-9]{3}-[0-9]{3}-)[0-9]{1,4}`

Table 3-5 (Cont.) pn32f-svc

Parameter	Description	Details
payloadSizeLimit	This is a mandatory parameter. This parameter represents the maximum payload size in bytes. Any payload greater than the given limit results the error code HTTP 413. The maximum configurable limit is 2147483647 byte.	Data Type: Integer Default Value: 262144 bytes

3.1.6 config-mgr-svc

This section includes information about the config-mgr-svc parameters of the SEPP.

Table 3-6 config-mgr-svc

Parameter	Description	Details
config-mgr-svc.extraContainers	This is a mandatory parameter. Use 'extraContainers' attribute to control the usage of extra container(DEBU G tool). # If assigned with ENABLED or USE_GLOBAL_V ALUE, then ensure "extraContainers Tpl" Yaml chunk is defined # at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
config-mgr-svc.image.repository	This is a mandatory parameter. Indicates the repo location of image	Data Type: String Range: NA Default Value: reg-1
config-mgr-svc.image.name	This is a mandatory parameter. Indicates the name of image	Data Type: String Range: NA Default Value: ocsepp-config-mgr-svc
config-mgr-svc.image.tag	This is a mandatory parameter. Indicates the tag of image	Data Type: String Range: NA Default Value: helm-tag
config-mgr-svc.image.pullPolicy	This is a mandatory parameter. This setting indicates if the image needs to be pulled or not	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always

Table 3-6 (Cont.) config-mgr-svc

Parameter	Description	Details
config-mgr-svc.service.loadBalancer.addressPool	This is a mandatory parameter. To request the assignment of public IP from a specific IP pool using metallb.universe.tf/address-pool annotation to config-mgr-svc.	Data Type: String Range: NA Default Value: signaling1
config-mgr-svc.log.root	This is a mandatory parameter. Indicates the Root log level	Data Type: String Range: DEBUG, INFO, WARN, ERROR Default Value: ERROR
config-mgr-svc.log.sepp	This is a mandatory parameter. Indicates the Sepp sepecific log level	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
config-mgr-svc.resources.limit.cpu	This is a mandatory parameter. Indicates the Requirements(limit of cpu)	Data Type: Integer Range: Valid Integer Default Value: 2
config-mgr-svc.resources.limit.memory	This is a mandatory parameter. Indicates the Resource Requirements(limit of memory)	Data Type: String Range: NA Default Value: 2Gi
config-mgr-svc.resources.limits.ephemeralStorage	This is an optional parameter.Pods use ephemeral local storage for scratch space, caching, and logs.	Data Type: String Range: depends on cluster Resources Default Value: 1Gi
config-mgr-svc.resources.requests.ephemeralStorage	This is an optional parameter.pods and containers can require ephemeral storage for their operation.	Data Type: String Range: depends on cluster resources Default Value: 70Mi
config-mgr-svc.resources.requests.cpu	This is a mandatory parameter. Indicates the Resource Requirements(requested cpu)	Data Type: Integer Range: NA Default Value: 2
config-mgr-svc.resources.requests.memory	This is a mandatory parameter. Indicates the Resource Requirements(requested memory)	Data Type: String Range: NA Default Value: 2Gi
config-mgr-svc.service.customExtension.labels	This is an optional parameter. Indicates the Custom Labels that needs to be added to config-mgr-svc specific Service	Data Type: String Range: NA Default Value: NA
config-mgr-svc.service.customExtension.annotations	This is an optional parameter. Indicates the Custom Annotations that needs to be added to config-mgr-svc specific Services	Data Type: String Range: NA Default Value: NA

Table 3-6 (Cont.) config-mgr-svc

Parameter	Description	Details
config-mgr-svc.deployment.customExtension.labels	This is an optional parameter. Indicates the Custom Labels that needs to be added to config-mgr-svc specific Deployment.	Data Type: String Range: NA Default Value: NA
config-mgr-svc.deployment.customExtension.annotations	This is an optional parameter. Indicates the Custom Annotations that needs to be added to config-mgr-svc specific Deployment.	Data Type: String Range: NA Default Value: NA
config-mgr-svc.startupProbe.initialDelaySeconds	This is a mandatory parameter.Tells the kubelet that it should wait second before performing the first probe.	Data Type: Integer Range: NA Default Value: 30
config-mgr-svc.startupProbe.timeoutSeconds	This is a mandatory parameter. Number of seconds after which the probe times out.	Data Type: Integer Range: NA Default Value: 3
config-mgr-svc.startupProbe.periodSeconds	This is a mandatory parameter. Specifies that the kubelet should perform a readiness probe every xx seconds.	Data Type: Integer Range: NA Default Value: 10
config-mgr-svc.startupProbe.successThreshold	This is a mandatory parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	Data Type: Integer Range: NA Default Value: 1
config-mgr-svc.startupProbe.failureThreshold	This is a mandatory parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	Data Type: Integer Range: NA Default Value: 6
config-mgr-svc.readinessProbe.initialDelaySeconds	This is a mandatory parameter. Tells the kubelet that it should wait second before performing the first probe.	Data Type: Integer Range: NA Default Value: 30
config-mgr-svc.readinessProbe.timeoutSeconds	This is a mandatory parameter. Number of seconds after which the probe times out.	Data Type: Integer Range: NA Default Value: 3
config-mgr-svc.readinessProbe.periodSeconds	This is a mandatory parameter. specifies that the kubelet should perform a readiness probe every xx seconds	Data Type: Integer Range: NA Default Value: 10
config-mgr-svc.readinessProbe.successThreshold	This is a mandatory parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	Data Type: Integer Range: NA Default Value: 1
config-mgr-svc.readinessProbe.failureThreshold	This is a mandatory parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	Data Type: Integer Range: NA Default Value: 3

Table 3-6 (Cont.) config-mgr-svc

Parameter	Description	Details
config-mgr-svc.livenessProbe.initialDelaySeconds	This is a mandatory parameter. Tells the kubelet that it should wait second before performing the first probe.	Data Type: Integer Range: NA Default Value: 180
config-mgr-svc.livenessProbe.timeoutSeconds	This is a mandatory parameter. Number of seconds after which the probe times out	Data Type: Integer Range: NA Default Value: 3
config-mgr-svc.livenessProbe.periodSeconds	This is a mandatory parameter. specifies that the kubelet should perform a liveliness probe every xx seconds.	Data Type: Integer Range: NA Default Value: 15
config-mgr-svc.livenessProbe.successThreshold	This is a mandatory parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	Data Type: Integer Range: NA Default Value: 1
config-mgr-svc.livenessProbe.failureThreshold	This is a mandatory parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	Data Type: Integer Range: NA Default Value: 3
config-mgr-svc.maxPerRemotePlmnListSize	This is a mandatory parameter. This value defines the max number of PLMNs allowed per remote SEPP# Value of MaxAllowedPLMNs, can be increased upto 900 in nrfClientDisable/Roaming-Hub Mode.	Data Type: Integer Range: NA Default Value: 30
config-mgr-svc.totalRemotePlmnListSize	This is a mandatory parameter. Value for total PLMNs that can be configured for the remote SEPPs on local SEPP.	Data Type: Integer Range: NA Default Value: 900
config-mgr-svc.maxSurge	This is a mandatory parameter. The number of pods that can be created above the desired amount of pods during an update	Data Type: Integer Range: NA Default Value: 25%
config-mgr-svc.maxUnavailable	This is a mandatory parameter. The number of pods that can be unavailable during an update	Data Type: Integer Range: NA Default Value: 0%
config-mgr-svc.service.active.type	This is a mandatory parameter. It defines the type of service	Data Type: String Range: ClusterIP, NodePort, LoadBalancer and ExternalName Default Value: NodePort
config-mgr-svc.service.active.svcPortHttp	This is a mandatory parameter. It defines the http port for config-mgr-svc service	Data Type: Integer Range: NA Default Value: 9090

Table 3-6 (Cont.) config-mgr-svc

Parameter	Description	Details
`config-mgr-svc.service.active.svcPortHttps`	This is a mandatory parameter. It defines the https port for config-mgr-svc service	Data Type: Integer Range: NA Default Value: 9091
`config-mgr-svc.service.active.actuatorPort`	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range: NA Default Value: 8085
`alternateRoute.orderId.rejectAll`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. Specifies the OrderId of RejectAll Route. RejectAll route will be selected when there is no matching N32f route.	**Data Type:** Integer **Default Value**: 90
`alternateRoute.orderId:n32c`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. Specifies the OrderId of N32c Route. N32c route will be used for all the capability-exchange message sent on N32C interface.	**Data Type**: Integer **Default Value**: 80
`alternateRoute.path.format1`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. Specifies the API format of n32c capability-exchnage message.	**Data Type**: String **Default Value**: /n32c-handshake/**
`alternateRoute.path.format2`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. Specifies the API format of n32c capability-exchnage message.	**Data Type**: String **Default Value**: /*/n32c-handshake/**
`alternateRoute.sbiReRoute.sbiRoutingErrorCriteriaSets[]`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. It is an array and contains the list of error criteria set. Error criteria's can be created on the basis of status or exceptions (not both). Only 2 criteria's are currently supported – criteria_0 and criteria_1.	**Data Type**: String **Default Value**: NA
`alternateRoute.sbiReRoute.sbiRoutingErrorCriteriaSets[].Id`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. This defined the unique name of the criteria set.	**Data Type**: String **Default Value:** criteria_0 and criteria_1

Table 3-6 (Cont.) config-mgr-svc

Parameter	Description	Details
`alternateRoute.sbiReRoute.sbiRoutingErrorCriteriaSets[].method`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. The methods supported while doing sbi rerouting. The alternate routing takes place only for the response messages that share the defined methods present.	**Data Type**: String **Range:** GET, POST, PUT, DELETE, PATCH
`alternateRoute.sbiReRoute.sbiRoutingErrorCriteriaSets[].Response.statuses.status`	This is an optional parameter. The error response status supported while doing sbi rerouting. The alternate routing takes place only for the response that matches the status code defined in this array list.	**Data Type**: array of integer **Range**: [500,503,504], [400,404]
`alternateRoute.sbiReRoute.sbiRoutingErrorCriteriaSets[].Response.statuses.statusSeries`	This is an optional parameter. This needs to be set along with status code. statusSeries will defined the HTTP error code series and status will define the specific HTTP error code status.	Data Type: string Range and Default value: “4xx”, “5xx”
`alternateRoute.sbiReRoute.sbiRoutingErrorCriteriaSets[].exceptions`	This is an optional parameter. Rerouting will happen either on the basis of status code or exception (any one). When exceptions are defined in errorCriterisSet, re-Routing takes place only if the exception received in the error response matched with the configured exception.	**Data Type**: String **Range**: • java.util.concurrent.TimeoutException • java.net.SocketException • java.net.SocketTimeoutException • java.net.UnknownHostException • java.net.ConnectException • java.net.NoRouteToHostException • javax.net.ssl.SSLHandshakeException
`alternateRoute.sbiReRoute.exceptionPriority`	This is an optional parameter. 2 errorCriteriaSets are created – one with status code and other with exception. When an error response is received, which error criteria set will get the priority will be defined by this parameter. This parameter defines the priority of exception error criteria set.	**Data Type**: Integer **Default Value**: 1

Table 3-6 (Cont.) config-mgr-svc

Parameter	Description	Details
`alternateRoute.sbiReRoute.responsePriority`	This is an optional parameter. Two errorCriteriaSets are created – one with status code and other with exception. When an error response is received, which error criteria set will get the priority will be defined by this parameter. This parameter defines the priority of status response error criteria set.	**Data Type**: Integer **Default Value**: 2
`alternateRoute.sbiReRoute.sbiRoutingErrorActionSets[]`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. It is an array and contains the list of actions set. When an error criteria defined above matches with the response, what action would be taken, reroute/redirect/drop and their corresponding parmaeters.	**Data Type**: String **Default Value**: NA
`alternateRoute.sbiReRoute.sbiRoutingErrorActionSets[].Id`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. This defined the unique name of the error action set.	**Data Type**: String **Default Value**: action_0
`alternateRoute.sbiReRoute.sbiRoutingErrorActionSets[].action`	This is a mandatory parameter for SBI routing to work on N32-egress-gateway. This defined the action to be performed if the error criteria set matches with the response received.	**Data Type**: String **Default Value**: reroute (rerouting to secondary/tertiary)
`alternateRoute.sbiReRoute.sbiRoutingErrorActionSets[].Attempts`	This is an optional parameter. The routing takes place based on the retries count set here. Example: if retry count is 1, then EGW will try to route towards secondary SEPP only (and not tertiary), if routing to primary SEPP fails.	**Data Type**: Integer **Default Value**: 0 **Note:** To enable alternate routing feature, change this parameter value to 2. This allows switching from primary to secondary to tertiary Remote SEPPs

Table 3-6 (Cont.) config-mgr-svc

Parameter	Description	Details
`alternateRoute.sbiReRoute.sbiRoutingErrorCriteriaSets[].headersMatchingScript`	This is an optional parameter. To enable server and Via Header handling, headersMatchingScript is added under the response entity within sbiRoutingErrorCriteriaSets. This headersMatchingScript configuration will get satisfied, if the response contains server or via header and the content of the header matches the regex configured. A comma separated String values, with the following format: 1st token: headerCheck (Hard coded values). 2nd to n-1 token: Header names which has to be validated. nth token: regex expression for header validation. Note: The final result would be an aggregated OR of the individual header checks.`"headerCheck,server,via,.*(SEPP|UDR).*"` Note: Not Currently used.	**Data Type**: String **Default Value**: ""

> **Note**
>
> The following parameters are configured in SEPP `config-mgr-svc/values.yaml` file.

Table 3-7 config-mgr-svc

Parameter	Description	Details
`sorReRoute.sbiRoutingErrorCriteriaSets[].Id`	This is a mandatory parameter for SOR re-routing to work on PLMN-egress-gateway. This defined the unique name of the criteria set.	**Data Type**: String **Default Value**: criteria_0 and criteria_1
`sorReRoute.sbiRoutingErrorCriteriaSets[].method`	This is a mandatory parameter for SOR re-routing to work on PLMN-egress-gateway. The methods supported while doing SOR rerouting. The alternate routing takes place only for the response messages that share the defined methods present.	**Data Type:** String **Range:** GET, POST, PUT, DELETE, PATCH

Table 3-7 (Cont.) config-mgr-svc

Parameter	Description	Details
`sorReRoute.sbiRoutingErrorCriteriaSets[].Response.statuses.status`	This is an optional parameter. The error response status supported while doing SOR rerouting. The alternate routing takes place only for the response that matches the status code defined in this array list.	**Data Type**: array of integer **Range**: [500,503,504]
`sorReRoute.sbiRoutingErrorCriteriaSets[].Response.statuses.statusSeries`	This is an optional parameter. This needs to be set along with status code. statusSeries will defined the HTTP error code series and status will define the specific HTTP error code status.	**Data Type**: string **Default value**: “5xx”
`sorReRoute.sbiRoutingErrorCriteriaSets[].exceptions`	This is an optional parameter. Rerouting will happen either on the basis of status code or exception (any one). When exceptions are defined in errorCriterisSet, re-Routing takes place only if the exception received in the error response matched with the configured exception.	Data Type: String Range: • java.util.concurrent.TimeoutException, • java.net.SocketException, • java.net.SocketTimeoutException, • java.net.UnknownHostException, • java.net.NoRouteToHostException, • java.net.ConnectException
`sorReRoute.sbiRoutingErrorCriteriaSets[].headersMatchingScript`	This is an optional parameter. Excluding the destination will happen if the server header value received in error response matches the string criteria defined in this field.	Data Type: String Default Value: "headerCheck,server,via,.*(SEPP|SOR).*"
`sorReRoute.exceptionPriority`	This is an optional parameter. 2 errorCriteriaSets are created – one with status code and other with exception. When an error response is received, which error criteria set will get the priority will be defined by this parameter. This parameter defines the priority of exception error criteria set.	Data Type: Integer Default Value: 2
`sorReRoute.responsePriority`	This is an optional parameter. 2 errorCriteriaSets are created – one with status code and other with exception. When an error response is received, which error criteria set will get the priority will be defined by this parameter. This parameter defines the priority of status response error criteria set.	Data Type: Integer Default Value: 1

Table 3-7 (Cont.) config-mgr-svc

Parameter	Description	Details
sorReRoute.sbiRoutingErrorActionSets[]	This is a mandatory parameter for SOR re-routing to work on PLMN-egress-gateway. It is an array and contains the list of actions set. When an error criteria defined above matches with the response, what action would be taken – reroute/redirect/drop and their corresponding parmaeters.	Data Type: String Default Value: NA
sorReRoute.sbiRoutingErrorActionSets[].Id	This is a mandatory parameter for SOR re-routing to work on PLMN-egress-gateway. This defined the unique name of the error action set.	Data Type: String Default Value: action_0
sorReRoute.sbiRoutingErrorActionSets[].action	This is a mandatory parameter. SOR re-routing to work on PLMN-egress-gateway. This defined the action to be performed if the error criteria set matches with the response received.	Data Type: String Default Value: reroute (rerouting to secondary/tertiary)
sorReRoute.sbiRoutingErrorActionSets[].Attempts	This is an optional parameter. The routing takes place based on the retries count set here. Example: if retry count is 1, then EGW will try to route towards secondary SEPP only (and not tertiary), if routing to primary SEPP fails.	Data Type: Integer Default Value: 2
sorReRoute.sbiRoutingErrorActionSets[].blacklist	This is an optional parameter. This defines whether the destination should be excluded for some amount of time	Data Type: String Default Value: NA
sorReRoute.sbiRoutingErrorActionSets[].blacklist.enabled	This is an optional parameter. If it is enabled, the functionality will work if the server header values matches with the error response received	Data Type: boolean Default Value: false
sorReRoute.sbiRoutingErrorActionSets[].blacklist.duration	This is an optional parameter. This defines the duration for which a destination is excluded. Time in MS.	Data Type: Integer Default Value: 60000
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	Data Type: Integer Default Value: 30000ms

3.1.7 n32-ingress-gateway

This section includes information about the n32-ingress-gateway parameters of the SEPP.

Table 3-8 n32-ingress-gateway

Name	Description	Details
cmName	This is an optional parameter. To enable the span	Data Type: String Range: NA Default Value: ingressgateway
serviceMeshCheck	This is a mandatory parameter. when enabled, OAuth signature validation is disabled ASM setup: When serviceMeshCheck is enabled signature validation of certificate is skipped. There is no need to configure the certificate or the secret.	Data Type: Boolean Range: true or false Default Value: false
istioSidecarQuitUrl	This is a mandatory parameter. The sidecar (istio quit url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/quitquitquit Note: Port should be envoy admin port.
istioSidecarReadyUrl	This is a mandatory parameter. The sidecar (istio ready url)when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/ready Note: Port should be envoy admin port.
ingressServer.keepAlive.enabled	This is a Optional parameter. If enabled netty server will send keep alive message for each connection	Data Type: Boolean Range: true or false Default Value: false
ingressServer.keepAlive.idleTime	This is a Optional parameter. Time after which keep alive will be tried after successful response from the peer	Data Type: Integer Range: NA Default Value: 180 #(Second)
ingressServer.keepAlive.count	This is a Optional parameter. No of times it should retry if there is no response for keep alive	Data Type: Integer Range: NA Default Value: 9
ingressServer.keepAlive.interval	This is an Optional parameter. The interval after which it should retry in case of failure	Data Type: Integer Range: NA Default Value: 60 #(Second)

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
serverHeaderConfigMode	This is a mandatory parameter. 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.	Data Type: ENUM Range: NA Default Value: HELM
serverHeaderDetails.enabled	This is a mandatory parameter. All attributes under "serverHeaderDetails" will need to be configured only if "serverHeaderConfigMode" is set as "HELM" If enabled at Global level, Global configuration will be used by default if no configuration exists at Route level.	Data Type: Boolean Range: HELM or REST Default Value: false
serverHeaderDetails.errorCodeSeriesId	This is a mandatory parameter if not defined at Route level. By default used for Global level configuration. Value need to be one among "errorCodeSeriesList" resource defined below.	Data Type: String Range: NA Default Value: E1
serverHeaderDetails.configuration.nfType	This is a mandatory parameter. This value is common across Global and Route level configuration. If not defined, server header will not be included in response.	Data Type: String Range: NA Default Value: SEPP
serverHeaderDetails.configuration.nfInstanceId	This is an Optional parameter. This value is common across Global and Route level configuration. If not defined, only "nfType" will be used for server header value.	Data Type: String Range: NA Default Value: 9faf1bbc-6e4a-4454-a507-aef01a101a06
errorCodeSeriesList[0].id	This is an Optional parameter. it is used for assigning "errorCodeSeriesId" either at Global or Route level configuration for Server header.	Data Type: String Range: NA Default Value: E1
errorCodeSeriesList[0].errorCodeSeries[0].errorSet	This is a mandatory parameter. Possible values for "errorSet" attribute: 5xx, 4xx, 3xx, 2xx, 1xx	Data Type: String Range: NA Default Value: 4xx
errorCodeSeriesList[0].errorCodeSeries[0].errorCodes	This is a mandatory parameter. Possible values include all error codes in the respective HttpSeries(Ex: 4xx) value assinged for "errorSet". Use single value of -1 if all error codes are to be considered.	Data Type: String Range: NA Default Value: 400, 408,404,429

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
errorCodeSeriesList[0].errorCodeSeries[1].errorSet	This is a mandatory parameter. Possible values for "errorSet" attribute: 5xx, 4xx, 3xx, 2xx, 1xx	Data Type: String Range: NA Default Value: 5xx
errorCodeSeriesList[0].errorCodeSeries[1].errorCodes	This is a mandatory parameter. Possible values include all error codes in the respective HttpSeries(Ex: 4xx) value assinged for "errorSet". Use single value of -1 if all error codes are to be considered.	Data Type: String Range: NA Default Value: 500, 503, 504
routesConfig[0].id	This is a mandatory parameter. It represents the id of the route.	Data Type: String Range: NA Default Value: n32f
routesConfig[0].uri	This is a mandatory parameter. Service name of the internal microservice of this NF. Note: Provide the actual port number of pn32f, if the user has modified the port.	Data Type: String Range: NA Default Value: http://{{ .Release.Name }}-pn32f-svc:9090/
routesConfig[0].path	This is a mandatory parameter. Provide the path to be matched.	Data Type: String Range: NA Default Value: /**
routesConfig[0].order	This is a mandatory parameter. Provide the order of the execution of this route.	Data Type: Integer Range: NA Default Value: 3
routesConfig[0].metadata.requestTimeout	This is a Optional parameter. requestTimeout is used to set timeout at route level. Value should be in milliseconds.	Data Type: Integer Range: NA Default Value: 700
routesConfig[0].metadata.requiredTime	This is a Optional parameter. requiredTime is minimum time below which request will be rejected if isSbiTimerEnabled is true. Value should be in milliseconds	Data Type: Integer Range: NA Default Value: 3000
routesConfig[0].metadata.xfccHeaderValidation.validationEnabled	This is a Optional parameter. This is used to provide an option to enable/not enable route level xfccHeaderValidation. It overrides global configuration for xfccHeaderValidation.enabled	Data Type: Boolean Range: true or false Default Value: false

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
routesConfig[0].metadata.svcName	This is a Optional parameter. The following parameter is configurable per route in route-metadata is used to track Overload Control data. If this parameter is not configured in route metadata then svc name from routesConfig.uri field is used as the required key to track Overload Control data. The value of "svcName" attribute denotes the back-end service tag to be used as the required key (configurable per route) to track Overload Control data instead of using back-end service name from routesConfig[0].uri as the required key.	Data Type: String Range: NA Default Value:
routesConfig[0].filters.addRequestHeader[0].name	This is a Optional parameter. This field is used for adding a request header at route level. Additional header can be configured by adding a new element in the next line and so on.	Data Type: String Range: NA Default Value:
routesConfig[0].filters.addRequestHeader[0].value	This is an Optional parameter. value of the header to be added	Data Type: String Range: NA Default Value:
routesConfig[0].filters.invalidRouteFilter.errorCodeOnInvalidRoute	This is a mandatory parameter, (if invalidRouteFilter is required) If invalidRouteFilter filter is configured, then keep the 'order' value highest compared to other routes. Comment the parameters related to invalidRouteFilter if configurable error code is not required for invalid route. Configurable error code for invalid route.	Data Type: String Range: NA Default Value:
routesConfig[0].filters.invalidRouteFilter.errorCauseOnInvalidRoute	This is a mandatory parameter, (if invalidRouteFilter is required) Error cause for invalid route	Data Type: String Range: NA Default Value:
routesConfig[0].filters.invalidRouteFilter.errorTitleOnInvalidRoute	This is a mandatory parameter, (if invalidRouteFilter is required) Error cause for invalid route	Data Type: String Range: NA Default Value:
routesConfig[0].filters.invalidRouteFilter.errorDescriptionOnInvalidRoute	This is a mandatory parameter, (if invalidRouteFilter is required) Error cause for invalid route	Data Type: String Range: NA Default Value:

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
routesConfig[0].removeRequestHeader[0].name	This is a Optional parameter. This field is used for removing a request header at route level. Additional header can be configured by adding a new element in the next line and so on.	Data Type: Range: NA Default Value: forwarded x-http2-scheme
routesConfig[0].removeResponseHeader[0].name	This is a Optional parameter. Below field is used for removing a response header at route level. Additional header can be configured by adding a new element in the next line and so on.	Data Type: Range: NA Default Value: nettylatency requestmethod error-reason
extraContainers	This is a mandatory parameter. Use 'extraContainers' attribute to control the usage of extra container(DEBUG tool). Allowed Values: DISABLED, ENABLED, USE_GLOBAL_VALUE If assigned with ENABLED or USE_GLOBAL_VALUE, then ensure "extraContainers Tpl" Yaml chunk is defined at Service level or Global level in the parent chart based on the value assigned respectivley.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
prefix	This is a mandatory parameter. Support for multiple egress instances. When set to some value then that value will be used in the names of resources along with release name so that there will not be any clash between the instances. When the value of this flag is set to '' then the resources are prepended with release name only.	Data Type: String Range: NA Default Value: 'n32'
global.k8sResources.hpat.supportedVersions	Kubernetes resource	Data Type: String Range: NA Default Value: autoscaling/v1
global.k8sResources.pdb.supportedVersions	Kubernetes resource PDB supported version	Data Type: String Range: NA Default Value: policy/v1
global.publicHttpSignalingPort	This is a mandatory parameter. Http Signalling port	Data Type: Integer Range: NA Default Value: 80

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
gloabl.publicHttpsSignallingPort	This is a mandatory parameter. Https Signalling port	Data Type: Integer Range: NA Default Value: 443
gloabl.serviceAccountName	This is an optional parameter. Service Account name. Specify type of service - Possible values are :- ClusterIP, NodePort, LoadBalancer and ExternalName	Data Type: String Range: NA Default Value: ' '
global.type	This is a mandatory parameter. type of service	Data Type: String Range: ClusterIP, NodePort, LoadBalancer and ExternalName Default Value: NodePort
global.staticIpAddressEnabled	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress.	Data Type: Boolean Range: True or False Default Value: False
global.staticIpAddress	This is an optional parameter. Static load balancer IP.	Data Type: String Range: NA Default Value: 10.75.212.60
global.staticNodePortEnabled	This is an optional parameter. If Static node port needs to be set, then set staticNodePortEnabled flag to true and provide value for staticNodePort, else random node port will be assigned by K8.	Data Type: Boolean Range: True or False Default Value: false
global.staticHttpNodePort	This is a mandatory parameter. Http Node Port	Data Type: Integer Range: NA Default Value: 30075
global.staticHttpsNodePort	This is a mandatory parameter. Https Node Port	Data Type: Integer Range: NA Default Value: 30043
global.logStorage	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
global.crictlStorage	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
global.ephemeralStorageLimit	This is an optional parameter. Ephemeral storage Limit	Data Type: Integer Range: NA Default Value: 1024

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
global.app_name	This is an optional parameter. App Name	Data Type: String Range: NA Default Value: ingress-gateway
global.xfccHeaderValidation.validation.enabled	This is a mandatory parameter. This parameter should be enabled in an ASM setup. It validates the xfcc header.	Data Type: Boolean Range: True or False Default Value: false
global.xfccHeaderValidation.extract.enabled	This is a mandatory parameter if global.xfccHeaderValidation.validation.enabled is true. if set to true then xfcc header value is extracted for validation.	Data Type: Boolean Range: True or False Default Value: false
global.xfccHeaderValidation.extract.certExtractIndex	This is a mandatory parameter if global.xfccHeaderValidation.validation.enabled is true. 0 represents the right most field 1 represents the left most and 2-3rd from right most.	Data Type: Integer Range: NA Default Value: 0
global.xfccHeaderValidation.extract.extractField	This is a mandatory parameter if global.xfccHeaderValidation.validation.enabled is true. name of the field to be extracted.	Data Type: String Range: NA Default Value: DNS
global.xfccHeaderValidation.extract.extractIndex	This is a mandatory parameter if global.xfccHeaderValidation.validation.enabled is true. 0 represents the right most field 1 represents the left most and 2-3rd from right most.	Data Type: Integer Range: NA Default Value: 0
cfgServer.enabled	This is an optional parameter. Config server switch. For the usage of Policy teams. For other NF's this has to be left false	Data Type: Boolean Range: True or False Default Value: false
cfgClient.enabled	This is an optional parameter. Config Client switch	Data Type: Boolean Range: True or False Default Value: false
commonCfgClient.enabled	This is an optional parameter. Set it to true if persistent configuration needs to be enabled.	Data Type: Boolean Range: True or False Default Value: false
commonCfgServer.configServerSvcName	This is a Mandatory parameter if commonCfgClient.enabled is set to true Service name of common configuration service to which the client tries to poll for configuration updates	Data Type: String Range: NA Default Value: config-mgr-svc

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
commonCfgServer.host	This is an optional parameter. Host name of Common configuration server to which client tries to poll for configuration updates. This value is picked up if commonCfgServer.configServerSvcName is not available.	Data Type: String Range: NA Default Value: config-mgr-svc
commonCfgServer.port	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Port of Common Configuration server.	Data Type: Integer Range: NA Default Value: 9090
commonCfgServer.pollingInterval	This is a Mandatory parameter if commonCfgClient.enabled is set to true. This is the interval between two subsequent polling requests from config client to server	Data Type: Integer Range: NA Default Value: 5000
commonServiceName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. This is the common service name that is currently requesting for configuration updates from server.	Data Type: String Range: NA Default Value: igw
restoreBackupOnInstall	This is an optional parameter. This flag when enabled picks up the data from the backup table during installation of ingress gateway.	Data Type: Boolean Range: true or false Default Value: false
dbConfig.dbHost	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Hostname of Mysql in which the configuration must be stored.	Data Type: String Range: NA Default Value: sepp-mysql-svc
dbConfig.dbPort	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Port of mysql.	Data Type: Integer Range: NA Default Value: 3306
dbConfig.configFile	This is a Mandatory parameter if commonCfgClient.enabled is set to true. File name for initial configuration that must be stored in the db.	Data Type: String Range: NA Default Value: defaultconfig.yaml
dbConfig.schemaFile	This is a Mandatory parameter if commonCfgClient.enabled is set to true. File name for json schema validation.	Data Type: String Range: NA Default Value: defaultconfig.yaml

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
dbConfig.secretName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Secret name from which the db name, db password and db user name is picked.	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
dbConfig.dbName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Database name	Data Type: String Range: NA Default Value: seppdb
dbConfig.dbUNameLiteral	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Name of the Key configured for "DB Username" in Secret with following name: "<dbConfig.secretName>" .	Data Type: String Range: NA Default Value: mysql-username
dbConfig.dbPwdLiteral	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Name of the Key configured for "DB Password" in Secret with following name: "<dbConfig.secretName>"	Data Type: String Range: NA Default Value: mysql-password
dbConfig.dbEngine	This is a Mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
image.name	This is an optional parameter. Image name of ingress gateway	Data Type: String Range: NA Default Value: ocingress_gateway
image.tag	This is an optional parameter. Image Tag name of ingress gateway	Data Type: String Range: NA Default Value: helm-gateway-ingress-tag
image.pullPolicy	This is an optional parameter. Image Pull Policy	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
initContainersImage.name	This is an optional parameter. Image name of initContainer	Data Type: String Range: NA Default Value: configurationinit

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
initContainersImage.tag	This is an optional parameter. Image tag name of initContainer	Data Type: String Range: NA Default Value: helm-gateway-config-tag
initContainersImage.pullPolicy	This is an optional parameter. Image Pull Policy	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
updateContainersImage.name	This is an optional parameter. Image name of updateContainer	Data Type: String Range: NA Default Value: configurationupdate
updateContainersImage.tag	This is an optional parameter. Image tag name of updateContainer	Data Type: String Range: NA Default Value: helm-gateway-config-tag
updateContainersImage.pullPolicy	This is an optional parameter. Image Pull Policy	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
dbHookImage.name	This is an optional parameter. Image name of dbHook	Data Type: String Range: NA Default Value: common_config_hook
dbHookImage.tag	This is an optional parameter. Image tag name of dbHook	Data Type: String Range: NA Default Value: helm-gateway-dbhook-tag
dbHookImage.pullPolicy	This is an optional parameter. Pull Policy of Image	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
service.ssl.privateKey.k8SecretName	This is a mandatory parameter. Name of the privatekey secret	Data Type: String Range: NA Default Value: ocsepp-n32-secret
service.ssl.privateKey.k8NameSpace	This is a mandatory parameter. Namespace of privatekey	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.privateKey.rsa.fileName	This is a mandatory parameter. rsa private key file name	Data Type: String Range: NA Default Value: rsa_private_key_pkcs1.pem

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
service.ssl.privateKey.ecdsa.fileName	This is a mandatory parameter. ecdsa private key file name	Data Type: String Range: NA Default Value: ssl_ecdsa_private_key.pem
service.ssl.certificate.k8SecretName	This is a mandatory parameter. Name of the certificate secret	Data Type: String Range: NA Default Value: ocsepp-n32-secret
service.ssl.certificate.k8NameSpace	This is a mandatory parameter. Namespace of certificate	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.certificate.rsa.fileName	This is a mandatory parameter. rsa certificate key file name	Data Type: String Range: NA Default Value: ocsepp.cer
service.ssl.certificate.ecdsa.fileName	This is a mandatory parameter. ecdsa certificate key file name	Data Type: String Range: NA Default Value: ssl_ecdsa_certificate.crt
service.ssl.caBundle.k8SecretName	This is a mandatory parameter. Name of the caBundle secret	Data Type: String Range: NA Default Value: ocsepp-n32-secret
service.ssl.caBundle.k8NameSpace	This is a mandatory parameter. Namespace of the caBundle	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.caBundle.fileName	This is a mandatory parameter. rsa private key file name	Data Type: String Range: NA Default Value: caroot.cer
service.ssl.keyStorePassword.k8SecretName	This is a mandatory parameter. Secret name that contains keyStorePassword	Data Type: String Range: NA Default Value: ocsepp-n32-secret
service.ssl.keyStorePassword.k8NameSpace	This is a mandatory parameter. Namespace in which SEPPs keystore password is present	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.keyStorePassword.fileName	This is a mandatory parameter. File name that has password for keyStore	Data Type: String Range: NA Default Value: key.txt
service.ssl.trustStorePassword.k8SecretName	This is a mandatory parameter. Secret name that contains trustStorePassword	Data Type: String Range: NA Default Value: ocsepp-n32-secret

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
service.ssl.trustStorePassword.k8NameSpace	This is a mandatory parameter. Namespace in which trustStorePassword is present	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.trustStorePassword.fileName	This is a mandatory parameter. File name that has password for trustStore	Data Type: String Range: NA Default Value: trust.txt
service.ssl.initialAlgorithm	This is a mandatory parameter. Algorithm based on the certificate	Data Type: String Range: NA Default Value: RS256
service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to n32-igw specific Service	Data Type: String Range: NA Default Value: { }
service.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to n32-igw specific Services	Data Type: String Range: NA Default Value: { }
deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to n32-igw specific deployment	Data Type: String Range: NA Default Value: { }
deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to n32-igw specific deployment	Data Type: String Range: NA Default Value: { }
ports.containerPort	This is an optional parameter. ContainerPort represents a network port in a single container	Data Type: Integer Range: NA Default Value: 8081
ports.containersslPort	This is an optional parameter. Ssl port of the container	Data Type: Integer Range: NA Default Value: 8443
ports.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range: NA Default Value: 9094
log.level.root	This is an optional parameter. Log level for root logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.ingress	This is an optional parameter. Log level for ingress logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
log.level.oauth	This is an optional parameter. Log level for oauth logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.updateContainer	This is an optional parameter. Log level for updateContainer	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.hook	This is an optional parameter. Log level for hook	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.cncc.root	This is an optional parameter. Log level for cncc logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.cncc.audit	This is an optional parameter. Log level for cncc logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.cncc.security	This is an optional parameter. Log level for cncc logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: WARN
log.level.cncc.loggingFilters	This is an optional parameter. logging filters	Data Type: String Range: NA Default Value: [ ]
log.level.cncc.loggingMasks	This is an optional parameter. logging mask	Data Type: String Range: NA Default Value: [ ]
log.traceIdGenerationEnabled	This is an optional parameter. TraceId Generation is Enabled	Data Type: Boolean Range: True or False Default Value: True
resources.limits.cpu	This is an optional parameter. CPU Limit	Data Type: Integer Range: NA Default Value: 6
resources.limits.initServiceCpu	This is an optional parameter. Init Container CPU Limit	Data Type: Integer Range: NA Default Value: 1
resources.limits.updateServiceCpu	This is an optional parameter. Update Container CPU Limit	Data Type: Integer Range: NA Default Value: 1

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`resources.limits.memory`	This is an optional parameter. Memory Limit	Data Type: String Range: NA Default Value: 5Gi
`resources.limits.commonHooksCpu`	This is an optional parameter. Db Hook Container CPU Limit	Data Type: Integer Range: NA Default Value: 1
`resources.limits.updateServiceMemory`	This is an optional parameter. Update Container Memory Limit	Data Type: String Range: NA Default Value: 1Gi
`resources.limits.initServiceMemory`	This is an optional parameter. int Container Memory Limit	Data Type: String Range: NA Default Value: 1Gi
`resources.limits.commonHooksMemory`	This is an optional parameter. Db Hook Container Memory Limit	Data Type: String Range: NA Default Value: 1Gi
`resources.requests.cpu`	This is an optional parameter. CPU for requests	Data Type: Integer Range: NA Default Value: 6
`resources.requests.initServiceCpu`	This is an optional parameter. Init Container CPU for requests	Data Type: Integer Range: NA Default Value: 1
`resources.requests.updateServiceCpu`	This is an optional parameter. Update Container CPU for requests	Data Type: Integer Range: NA Default Value: 1
`resources.requests.memory`	This is an optional parameter. Memory for requests	Data Type: String Range: NA Default Value: 5Gi
`resources.requests.commonHooksCpu`	This is an optional parameter. Db Hook Container CPU for requests	Data Type: Integer Range: NA Default Value: 1
`resources.requests.updateServiceMemory`	This is an optional parameter. Update Container Memory for requests	Data Type: String Range: NA Default Value: 1Gi
`resources.requests.initServiceMemory`	This is an optional parameter. Init Container Memory for requests	Data Type: String Range: NA Default Value: 1Gi
`resources.requests.commonHooksMemory`	This is an optional parameter. Db Hook Container Memory for requests	Data Type: String Range: NA Default Value: 1Gi
`resources.target.averageCpuUtil`	This is an optional parameter. Average CPU for target	Data Type: Integer Range: NA Default Value: 70

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`maxUnavailable`	This is an optional parameter. Number of Pods that will be unavailable during a disruption	Data Type: String Range: NA Default Value: 25%
`minReplicas`	This is an optional parameter. Min replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
`maxReplicas`	This is an optional parameter. Max replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
`jaegerTracingEnabled`	This is an optional parameter. Enable jaeger tracing	Data Type: Boolean Range: True or False Default Value: False
`openTracing.jaeger.enableb3Propagation`	This is an Mandatory parameter If jaegerTracingEna bled is true To send b3 zipkin headers instead of uber-trace-id	Data Type: Boolean Range: True or False Default Value: False
`openTracing.jaeger.udpSender.host`	This is an optional parameter. Jaeger Host	Data Type: String Range: NA Default Value: occne-tracer-jaeger-agent.occne-infra
`openTracing.jaeger.udpSender.port`	This is an optional parameter. Jaeger Port	Data Type: Integer Range: NA Default Value: 6831
`openTracing.jaeger.probabilisticSampler`	This is an optional parameter. Trace capture in percentage	Data Type: Float Range: NA Default Value: 0.5
`initssl`	This is an optional parameter. Enabling it generates key and trust store for https support	Data Type: Boolean Range: True or False Default Value: True **Note:** • The default value will be true, if the user wants to deploy in non ASM mode. • The default value will be false, if the user wants to deploy in ASM mode.
`enableIncomingHttp`	This is an optional parameter. Enabling it for incoming http request	Data Type: Boolean Range: True or False Default Value: false **Note:** • The default value will be false, if the user wants to deploy in non ASM mode. • The default value will be true, if the user wants to deploy in ASM mode.

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`enableIncomingHttps`	This is an optional parameter. Enabling it for incoming https request	Data Type: Boolean Range: True or False Default Value: True **Note:** • The default value will be true, if the user wants to deploy in non ASM mode. • The default value will be false, if the user wants to deploy in ASM mode.
`enableOutgoingHttps`	This is an optional parameter. Enabling it for outgoing https request	Data Type: Boolean Range: True or False Default Value: False **Note:** This value must be set to false always.
`needClientAuth`	This is an optional parameter. This must be true if client certificate identity is required in the header x-custom-ingress-client-identity	Data Type: Boolean Range: True or False Default Value: True
`sbiPriorityHeaderName`	This is an optional parameter. This parameters defines the header name which will contain the SBI Priority value	Data Type: String Range: NA Default Value: 3gpp-sbi-message-priority
`dnsRefreshDelay`	This is an optional parameter. Dns Refresh Delay in milli-seconds	Data Type: Integer Range: NA Default Value: 120000 # ms
`ingressGwCertReloadEnabled`	This is an optional parameter. changes in k8s secrets	Data Type: boolean Range: True or False Default Value: True
`ingressGwCertReloadPath`	This is an optional parameter. Path to reload ingress gateway certificate	Data Type: String Range: NA Default Value: /ingress-gw/certificate/reload
`ingressGwCertReloadDelay`	This is an optional parameter. The polling interval to monitor k8s secrets for changes.	Data Type: init Range: NA Default Value: 15000
`rateLimiting.enabled`	This is an optional parameter. This parameter enables Rate Limiting on Ingress Gateway.	Data Type: boolean Range: True or False Default Value: True
`rssRateLimiter.enabled`	This is an optional parameter. This parameter enables Ingress Rate Limiting per Remote SEPP Set on Ingress Gateway.	Data Type: boolean Range: True or False Default Value: True

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`globalIngressRateLimiting.enabled`	This is an optional parameter. This parameter enables Global Rate Limiting on Ingress Gateway.	Data Type: boolean Range: True or False Default Value: false
`globalIngressRateLimiting.duration`	This is a mandatory parameter(if globalIngressRateLimiting is enabled to true). Iterations of time duration(In seconds) for which bucketCapacity and refillRate are reset.	Data Type: Integer Range: NA Default Value: 1
`globalIngressRateLimiting.burstCapacity`	This is a mandatory parameter. (if globalIngressRateLimiting is enabled true)Holds maximum number of tokens in the bucket for the given duration	Data Type: Integer Range: NA Default Value: 7500
`globalIngressRateLimiting.refillRate`	This is a mandatory parameter (if globalIngressRateLimiting is enabled true) Number of tokens to be added to the bucket for the given duration Recommended to have refillRate equal to burstCapacity	Data Type: Integer Range: NA Default Value: 7500
`errorCodeOnRateLimit`	This is a conditional parameter (if globalIngressRateLimiting is enabled true) Configurable error code returned when ratelimit is reached. Populated in ProblemDetails response in ProblemDetails.status section.	Data Type: Integer Range: NA Default Value: 429
`gracefulShutdown.gracePeriod`	This is an optional parameter. Grace period to wait for active requests to be executed. If there are no active requests then this period is neglected. # 's' in case of seconds and 'm' in case of minutes	Data Type: String Range: NA Default Value: 1m
`gracefulShutdown.defaultErrorCode`	This is a optional parameter Default error code returned at the time of Graceful shut down	Data Type: Integer Range: NA Default Value: 500
`gracefulShutdown.errorDescription`	This is an optional parameter. Graceful shut down Error description	Data Type: String Range: NA Default Value: " "
`gracefulShutdown.errorCause`	This is an optional parameter. Graceful shut down error cause	Data Type: String Range: NA Default Value: " "

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
gracefulShutdown.errorTitle	This is an optional parameter. Graceful shut down error title	Data Type: String Range: NA Default Value: " "
gracefulShutdown.retryAfter	This is an optional parameter. determines the value in seconds per particular date after which the service should be retried post graceful shutdown.	Data Type: String Range: NA Default Value: " "
gracefulShutdown.redirectUrl	This is an optional parameter. redirection URL for validation failure due to graceful shutdown	Data Type: String Range: NA Default Value: " "
dnsSrv.host	This is an optional parameter. DNS SRV Host name	Data Type: String Range: NA Default Value: localhost
dnsSrv.port	This is an optional parameter. DNS SRV port number	Data Type: Integer Range: NA Default Value: 8004
dnsSrv.scheme	This is an optional parameter. DNS SRV scheme name	Data Type: String Range: NA Default Value: http
nettyIdleTimeout	This is an optional parameter. Netty Idle Timeout in milliseconds	Data Type: Integer Range: NA Default Value: 120000000 #(ms)
nfFqdn	This is a mandatory parameter. NF FQDN	Data Type: String Range: NA Default Value: sepp2.inter.oracle.com
messageCopy.enabled	This is an optional parameter. This parameter enables or disables the Message feed feature at the Ingress Gateway.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.copyPayload	This is an optional parameter. This parameter specifies whether to copy the message payload in the feed towards Data Director or not. true: the complete payload message is copied. false: Only the header information is copied.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.topicName	This is an optional parameter. Name of the topic to which Ingress Gateway send the payloads.	Data Type: String Range: NA Default Value: message.copy

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
messageCopy.ackRequired	This is a mandatory parameter. This parameter specifies if we wait for any acknowledgement from DD.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.retryOnFailure	This is a mandatory parameter. This parameter specifies how many times SEPP should retry if message was not sent to DD successfully.	Data Type: Integer Range: NA Default Value: 0
messageCopy.security.enabled	This is a mandatory parameter. Security mode enabled for message feed feature	Data Type: Boolean Range: True or False Default Value: False
messageCopy.security.protocol	This is a conditional parameter. It is used for message feed feature when security is enabled between SEPP and Gateway.	Data Type: String Range: SASL_SSL or SSL Default Value: SASL_SSL
messageCopy.security.tlsVersion	This is a mandatory parameter. TLS version details.	Data Type: String Range: TLSv1.2, TLSv1.3 Default Value: TLSv1.3
messageCopy.security.saslConfiguration.username	This is a mandatory parameter. username for DD Refer to DD guide for more details	Data Type: String Range: NA Default Value: test
messageCopy.security.saslConfiguration.password	This is a mandatory parameter. Password for gateway on which feature enabled	Data Type: Object Range: NA Default:
messageCopy.security.saslConfiguration.password.k8SecretName	This is a mandatory parameter. Secret name for gateway on which feature enabled	Data Type: String Range: ocsepp-plmn-secret for PLMN Gateways and ocsepp-n32-secret for N32 Gateways Default Value: message-copy-secret
messageCopy.security.saslConfiguration.password.k8NameSpace	This is a mandatory parameter. Namespace where DD deployed Please refer to DD guide for more details	Data Type: String Range: NA Default Value: ocingress
messageCopy.security.saslConfiguration.password.fileName	This is a mandatory parameter. File used to create DD secrets Please refer to DD guide for more details	Data Type: String Range: NA Default Value: password.txt
messageCopy.threadPoolConfigurations.coreSize	This is an optional parameter. core Size for thread pool configuration for message feed thread. For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`messageCopy.threadPoolConfigurations.maxSize`	This is an optional parameter. max Size for thread pool configuration for message feed thread For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8
`messageCopy.threadPoolConfigurations.queueCapacity`	This is an optional parameter. queue capacity for thread pool configuration message feed thread For performance enhancement, set the value as 3000.	Data Type: Integer Range: NA Default Value: 1000
`kafka.bootstrapAddress`	This is an conditional parameter. List of comma- separated Kafka Nodes (to which messages should be copied if messageCopy feature is enabled).	Data Type: String Range: NA Default Value: <kafka-broker>:<port> Port = 9093 for SSL protocol Port = 9094 for SASL_SSL protocol
`egressRateLimiter.enabled`	This is an optional parameter. This parameter is used to enable or disable the egress rate limiting per egress rate limiting list on Ingress Gateway.	Data Type: Boolean Range: True or False Default Value: True
`clientDisabledExtension`	This is an optional parameter. Disables the extension sent by messages originated by clients (ClientHello).	**Data Type**: String **Range**: NA **Default Value**: ec_point_formats
`serverDisabledExtension`	This is an optional parameter. Disables the extension sent by messages originated by servers (ServerHello).	**Data Type**: String **Range**: NA **Default Value**: null
`tlsNamedGroups`	This is an optional parameter. Provides a list of values sent in the supported_groups extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
`clientSignatureSchemes`	This is an optional parameter. Provides a list of values sent in the signature_algorithms extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
`service.ssl.tlsVersion`	This is a mandatory parameter. Indicates the TLS version.	**Data Type**: String **Range**: • TLSv1.2 , TLSv1.3 • TLSv1.2 • TLSv1.3 **Default Value**: TLSv1.2, TLSv1.3

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
allowedCipherSuites	This is an optional parameter. Indicates allowed Ciphers.	**Data Type**: String **Range**: NA **Default Values**: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 - TLS_CHACHA20_POLY1305_SHA256
cipherSuites	This is an optional parameter. Indicates supported cipher suites.	**Data Type**: String **Range**: NA **Default Values**: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 - TLS_CHACHA20_POLY1305_SHA256
healthCheckMonitoring.enabled	This is an optional parameter. Enables the support of health check API on the N32 Ingress gateway.	**Data Type**: Boolean **Range**: True or False **Default Value**: False

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`keybasedKafkaProducer`	This is a mandatory parameter. This parameter when set to true, enables the functionality of message copy of same transaction into same Kafka partition.	**Data Type**: Boolean **Range**: True or False **Default Value**: False
`podSecurityContext.runAsNonRoot`	This is a mandatory parameter. Prevents pod from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
`podSecurityContext.runAsUser`	This is a mandatory parameter. Specifies that all processes in pod must run with the provided user ID.	Data Type: Integer Default Value: 10001
`securityContext.enable`	This is a mandatory parameter. Enables security context for containers.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.readOnlyRootFilesystem`	This is a mandatory parameter. Mounts the mediation container's root filesystem as read-only.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.allowPrivilegeEscalation`	This is a mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the `no_new_privs` parameter gets configured on the container process. `allowPrivilegeEscalation` is always set to true when the container: • is run as privileged • has CAP_SYS_ADMIN	Data Type: Boolean Range: True or False Default Value: False
`containerSecurityContext.runAsNonRoot`	This is a mandatory parameter. Prevents containers from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.privileged`	This is a mandatory parameter. Provides containers' access to the host’s resources and kernel capabilities.	Data Type: Boolean Range: True or False Default Value: False
`containerSecurityContext.runAsUser`	This is a mandatory parameter. Specifies that for any container in the pod, all processes must run with the provided user ID.	Data Type: Integer Range: Valid IDs for security context for user Default Value: 10001

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
containerSecurityContext.capabilities.drop	This is a mandatory parameter. Manages Linux capabilities for containers. Using Linux capabilities, you can grant certain privileges to a process without granting all the privileges of the root user.	Data Type: List of strings Range: Valid Linux capabilities Default Value: -all
enablePodSecurityContext	This is a mandatory parameter. Enables security context for pod.	Data Type: Boolean Range: True or False Default Value: True
deploymentMode	This is a mandatory parameter. This parameter defines the deployment mode for SEPP. That is, Single Stack or Dual Stack.	Data Type: String Range: IPv4, IPv6, IPv6_IPv4, and IPv4_IPv6. Default Value: SEPP/Roaming Hub: In single stack mode, default value: IPv4 In dual stack mode, default value: IPv6_IPv4 (IPv6 preferred)
global.lciHeaderConfig.enabled	This is an optional parameter. If this parameter is set to true, LCI headers reporting is enabled.	Data Type: Boolean Range: True or False Default Value: False
global.lciHeaderConfig.loadThreshold	This is an optional parameter. This parameter defines the load threshold configuration, if the current load level is beyond previously computed load level plus loadThreshold, LCI headers are reported again.	Data Type: Integer Range: NA Default Value: 40
global.lciHeaderConfig.localLciHeaderValidity	This is an optional parameter. This parameter defines the validity period of LCI headers reported to consumer NF. The LCI headers are reported again once the validity period has expired.	Data Type: Integer Range: NA Default Value: 1000 (milliseconds)
global.ociHeaderConfig.enabled	This is an optional parameter. If this parameter is set to true, OCI headers reporting will be enabled.	Data Type: Boolean Range: True or False Default Value: False
global.ociHeaderConfig.validityPeriod	This is an optional parameter. Validity period of OCI headers reported to consumer NF. The OCI headers are reported again if the headers reported previously expire.	Data Type: Integer Range: NA Default Value: 5000 (milliseconds)

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`global.ociHeaderConfig.overloadConfigRange.minor`	This is a mandatory parameter, if the OCI and LCI header feature is enabled. This parameter defines the range to identify minor overload condition.	Data Type: Integer Range: 0 to 100 Default Value: 60-70
`global.ociHeaderConfig.overloadConfigRange.major`	This is a mandatory parameter, if the OCI and LCI header feature is enabled. This parameter defines the range to identify major overload condition.	Data Type: Integer Range: 0 to 100 Default Value: 70-80
`global.ociHeaderConfig.overloadConfigRange.critical`	This is a mandatory parameter, if the OCI and LCI header feature is enabled. This parameter defines the range to identify critical overload condition.	Data Type: Integer Range: 0 to 100 Default Value: 80-100
`global.ociHeaderConfig.reductionMetrics.minor`	This is a mandatory parameter, if the OCI and LCI header feature is enabled. This parameter defines the reduction metric to be reported for minor overload condition.	Data Type: Integer Range: 1 to 9 Default Value: 5
`global.ociHeaderConfig.reductionMetrics.major`	This is a mandatory parameter, if the OCI and LCI header feature is enabled. This parameter defines the reduction metric to be reported for major overload condition.	Data Type: Integer Range: 5 to 15 Default Value: 10
`global.ociHeaderConfig.reductionMetrics.critical`	This is a mandatory parameter, if the OCI and LCI header feature is enabled. This parameter defines the reduction metric to be reported for critical overload condition.	Data Type: Integer Range: 10 to 50 Default Value: 30
`global.nfInstanceId`	This is a mandatory parameter, if the OCI and LCI header feature is enabled. NF Instance Id of producer NF.	Data Type: String Range: NA Default Value: 6faf1bbc-6e4a-4454-a507-a14ef8e1bc11
`global.nfType`	This is a mandatory parameter, if the f OCI and LCI header eature is enabled. NF type of producer NF.	Data Type: String Range: NA Default Value: NA
`global.nfFqdn`	This is a mandatory parameter. This is the NF FQDN for SEPP	Data Type: String Range: NA Default Value: NA

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`global.svcToSvcInstanceIdMapping.svcName`	This is an optional parameter. This parameter defines the back-end service name which should match `producerSvcIdHeader` value and perf info reported service name for LCI or OCI headers reporting.	Data Type: String Range: NA Default Value: nf-registration
`global.svcToSvcInstanceIdMapping.serviceInstanceId`	This is an optional parameter. This parameter defines the Back-end service instance id to be included in LCI / OCI headers.	Data Type: String Range: NA Default Value: fe7d992b-0541-4c7d-ab84-c6d70b1b01b1
`global.perfInfoConfig.pollingInterval`	This is an optional parameter. This parameter defines the Configurable interval at which load infromation is polled from perf-info service at Gateway.	Data Type: Integer Range: NA Default Value: 5000
`global.perfInfoConfig.serviceName`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info service name.	Data Type: String Range: NA Default Value: NA
`global.perfInfoConfig.host`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info Host IP.	Data Type: String Range: NA Default Value: NA
`global.perfInfoConfig.port`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info port.	Data Type: String Range: NA Default Value: NA
`global.perfInfoConfig.perfInfoRequestMap`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info service request endpoint.	Data Type: String Range: NA Default Value: NA
`tlsVersionSupportForKubeApiServer.enabled`	This is an optional parameter. This parameter enables or disables TLS 1.3 support for establishing communication between Gateway Services and Kubernetes API server (Kube\u0002Api-Server). If this parameter is enabled, support for establishing communication with Kube\u0002Api-Server is provided through TLS 1.3, along with TLS 1.2 as configured in `kubeApiServerTlsVersion`. If this parameter is disabled, support for communication with Kube-Api-Server is provided only through TLS 1.2.	Data Type: Boolean Range: True or False Default Value: False

Table 3-8 (Cont.) n32-ingress-gateway

Name	Description	Details
`tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`	This is a mandatory parameter. This parameter defines the supported TLS versions used by Gateway Services to communicate with the Kube-API-Server.	Data Type: String Range: TLS 1.2 and TLS 1.3 Default Value: TLS 1.3
`tlsVersionSupportForKubeApiServer.cipherSuites`	This is a mandatory parameter. This parameter indicates the Cipher suites that are compliant with the configured `tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`	Data Type: String Range: NA Default Value: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CH ACHA20 _POLY1305_SHA 256
`tlsVersionSupportForKubeApiServer.featureSecrets`	This is an optional parameter. This parameter indicates the list of all the secrets that are used for all the features of Gateway Services. These secrets are volume mounted during the pod deployment.	Data Type: String Range: NA Default Value: • ocegress -secret1 • ocegress -secret2 • ocegress -secret3
`overloadControlLocalDiscardEnabled`	This is an optional parameter. This parameter enables each pod independently to discard requests based on its local load. This parameter can have the following values: • true: No coherence-based token reservation is required. • false: Coherence is used for token reservations across pods.	Data Type: Boolean Range: true or false Default Value: false

3.1.8 plmn-ingress-gateway

This section includes information about the plmn-ingress-gateway parameters of the SEPP.

Table 3-9 plmn-ingress-gateway

Name	Description	Details
`cmName`	This is an optional parameter. To enable the span	Data Type: String Range: NA Default Value: ingress gateway

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
serviceMeshCheck	This is a mandatory parameter. when enabled, OAuth signature validation is disabled ASM setup: When serviceMeshCheck is enabled signature validation of certificate is skipped. There is no need to configure the certificate or the secret.	Data Type: Boolean Range: NA Default Value: false
istioSidecarQuitUrl	This is a mandatory parameter. The sidecar (istio quit url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: Boolean Range: NA Default value: http://127.0.0.1:15020/quitquitquit Note: Port should be envoy admin port.
istioSidecarReadyUrl	This is a mandatory parameter. The sidecar (istio ready url)when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: Boolean Range: NA Default value: http://127.0.0.1:15020/ready Note: Port should be envoy admin port.
ingressServer.keepAlive.enabled	This is a Optional parameter. If enabled netty server will send keep alive message for each connection.	Data Type: Boolean Range: NA Default Value: true
ingressServer.keepAlive.idleTime	This is a Optional parameter. Time after which keep alive will be tried after successful response from the peer.	Data Type: Integer Range: NA Default Value: 180 (Second)
ingressServer.keepAlive.count	This is a Optional parameter. No of times it should retry if there is no response for keep alive.	Data Type: Integer Range: NA Default Value: 6
ingressServer.keepAlive.interval	This is a Optional parameter. The interval after which it should retry in case of failure.	Data Type: Integer Range: NA Default Value: 60 (Second)
serverHeaderConfigMode	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.	Data Type: Enum Range: NA Default Value: HELM

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
`serverHeaderDetails.enabled`	All attributes under "serverHeaderDetails" will need to be configured only if "serverHeaderConfigMode" is set as "HELM" If enabled at Global level, Global conf will be used by default if no conf exists at Route level.	Data Type: Boolean Range: NA Default Value: false
`serverHeaderDetails.errorCodeSeriesId`	Mandatory attribute if not defined at Route level. By default used for Global level conf. Value need to be one among "errorCodeSeriesList" resource defined below.	Data Type: String Range: NA Default Value: E1
`serverHeaderDetails.configuration.nfType`	Mandatory attribute. This value is common across Global and Route level conf. If not defined, server header will not be included in response.	Data Type: String Range: NA Default Value: SEPP
`serverHeaderDetails.configuration.nfInstanceId`	Optional attribute. This value is common across Global and Route level conf. If not defined, only "nfType" will be used for server header value.	Data Type: String Range: NA Default Value: 9faf1bbc-6e4a-4454-a507-aef01a101a06
`errorCodeSeriesList[0].id`	This is a Optional parameter. it is used for assigning "errorCodeSeriesId" either at Global or Route level conf for Server header.	Data Type: String Range: NA Default Value: E1
`errorCodeSeriesList[0].errorCodeSeries[0].errorSet`	This is a mandatory parameter. Possible values for "errorSet" attribute: 5xx, 4xx, 3xx, 2xx, 1xx	Data Type: String Range: NA Default Value: 4xx
`errorCodeSeriesList[0].errorCodeSeries[0].errorCodes[0]`	This is a mandatory parameter. Possible values include all error codes in the respective HttpSeries(Ex: 4xx) value assinged for "errorSet". Use single value of -1 if all error codes are to be considered.	Data Type: String Range: NA Default Value: 400, 408, 404

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
extraContainers	This is a mandatory parameter. The attribute is used to control the usage of extra container(DEBUG tool). Allowed Values: DISABLED, ENABLED, USE_GLOBAL_VALUE If assigned with ENABLED or USE_GLOBAL_VALUE, then ensure "extraContainers Tpl" yaml chunk is defined at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: String Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
prefix	This is a mandatory parameter. When set to some value then that value will be used in the names of resources along with release name.	Data Type: String Range: NA Default Value: 'plmn'
global.k8sResources.hpat.supportedVersions	Kubernetes resource.	Data Type: String Range: NA Default Value: autoscaling/v1
global.k8sResources.pdb.supportedVersions	Kubernetes resource PDB supported version.	Data Type: String Range: NA Default Value: policy/v1
global.publicHttpSignalingPort	This is a mandatory parameter. Http Signalling port.	Data Type: IntegerRange: NADefault Value: Data Type: Integer Range: NA Default Value: 80
gloabl.publicHttpsSignallingPort	This is a mandatory parameter. Https Signalling port.	Data Type: Integer Range: NA Default Value: 443
gloabl.serviceAccountName	This is an optional parameter. Service Account name.	Data Type: String Range: NA Default Value: ' '
global.type	This is an optional parameter. Type of service.	Data Type: String Default Value: Possible values are ClusterIP, NodePort, LoadBalancer and ExternalNameDefault Value: NodePort

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
global.staticIpAddressEnabled	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress Else random IP will be assigned by the metalLB from its IP Pool.	Data Type: Boolean Range: True or False Default Value: False
global.staticIpAddress	This is an optional parameter. StaticIp.	Data Type: String Range: NA Default Value: 10.75.212.60
global.staticNodePortEnabled	This is an optional parameter. Node Port Enabled.	Data Type: Boolean Range: True or False Default Value: True
global.staticHttpNodePort	Http Node Port.	Data Type: Integer Range: NA Default Value: 30085
global.staticHttpsNodePort	Https Node Port.	Data Type: Integer Range: NA Default Value: 30053
global.logStorage	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
global.crictlStorage	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
global.ephemeralStorageLimit	This is an optional parameter. Ephemeral storage Limit.	Data Type: Range: NA Default Value: 1024
commonCfgClient.enabled	This is an optional parameter. Set it to true if persistent configuration needs to be enabled.	Data Type: Boolean Range: true or false Default Value: true
commonCfgServer.configServerSvcName	This is a Mandatory parameter if commonCfgClient.enabled is set to true Service name of common configuration service to which the client tries to poll for configuration updates.	Data Type: String Range: NA Default Value: config-mgr-svc

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
commonCfgServer.host	This is an optional parameter. Host name of Common configuration server to which client tries to poll for configuration updates. This value is picked up if commonCfgServer.configServerSvcName is not available.	Data Type: String Range: NA Default Value: config-mgr-svc
commonCfgServer.port	This is a Mandatory parameter if commonCfgClient.enabled is set to true Port of Common Configuration server.	Data Type: Integer Range: NA Default Value: 9090
commonCfgServer.pollingInterval	This is a Mandatory parameter if commonCfgClient.enabled is set to true. This is the interval between two subsequent polling requests from config client to server	Data Type: Integer Range: NA Default Value: 5000
commonServiceName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. This is the common service name that is currently requesting for configuration updates from server.	Data Type: string Range: NA Default Value: egw
restoreBackupOnInstall	This is an optional parameter. This flag when enabled picks up the data from the backup table during installation of ingress gateway.	Data Type: Boolean Range: true or false Default Value: false
dbConfig.dbHost	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Hostname of Mysql in which the configuration must be stored.	Data Type: String Range: NA Default Value: sepp-mysql-svc
dbConfig.dbPort	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Port of mysql.	Data Type: Integer Range: NA Default Value: 3306
dbConfig.configFile	This is a Mandatory parameter if commonCfgClient.enabled is set to true. File name for initial configuration that must be stored in the db.	Data Type: String Range: NA Default Value: defaultconfig.yaml
dbConfig.schemaFile	This is a Mandatory parameter if commonCfgClient.enabled is set to true. File name for json schema validation.	Data Type: String Range: NA Default Value: defaultschema.json

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
dbConfig.secretName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Secret name from which the db name, db password and db user name is picked.	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
dbConfig.dbName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Database name.	Data Type: String Range: NA Default Value: seppdb
dbConfig.backupDbName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. configure when your backup table should have separate schema	Data Type: Range: NA Default Value:
dbConfig.dbUNameLiteral	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Name of the Key configured for "DB Username" in Secret with following name: "<dbConfig.secretName>".	Data Type: String Range: NA Default Value: mysql-username
dbConfig.dbPwdLiteral	This is a Mandatory parameter if commonCfgClient.enabled is set to true. Name of the Key configured for "DB Password" in Secret with following name: "<dbConfig.secretName>".	Data Type: String Range: NA Default Value: mysql-password
dbConfig.dbEngine	This is a Mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
image.name	This is an optional parameter. Image name of ingress gateway.	Data Type: String Range: NA Default Value: ocingress_gateway
image.tag	This is an optional parameter. Image Tag name of ingress gateway.	Data Type: String Range: NA Default Value: helm-gateway-ingress-tag
image.pullPolicy	This is an optional parameter. Image Pull Policy.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
initContainersImage.name	This is an optional parameter. Image name of initContainer.	Data Type: String Range: NA Default Value: configurationinit
initContainersImage.tag	This is an optional parameter. Image tag name of initContainer.	Data Type: String Range: NA Default Value: helm-gateway-ingress-tag
initContainersImage.pullPolicy	This is an optional parameter. Image Pull Policy.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
updateContainersImage.name	This is an optional parameter. Image name of updateContainer.	Data Type: String Range: NA Default Value: configurationupdate
updateContainersImage.tag	This is an optional parameter. Image tag name of updateContainer.	Data Type: String Range: NA Default Value: helm-gateway-ingress-tag
updateContainersImage.pullPolicy	This is an optional parameter. Image Pull Policy.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
dbHookImage.name	This is an optional parameter. Image name of dbHook.	Data Type: String Range: NA Default Value: common_config_hook
dbHookImage.tag	This is an optional parameter. Image tag name of dbHook.	Data Type: String Range: NA Default Value: helm-gateway-ingress-tag
dbHookImage.pullPolicy	This is an optional parameter. Pull Policy of Image.	Data Type: String Range: NA Default Value: Always
service.ssl.privateKey.k8SecretName	This is a mandatory parameter. Name of the privatekey secret.	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.privateKey.k8NameSpace	This is a mandatory parameter. Namespace of privatekey.	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
service.ssl.privateKey.rsa.fileName	This is a mandatory parameter. rsa private key file name.	Data Type: String Range: NA Default Value: rsa_private_key_pkcs1.pem
service.ssl.privateKey.ecdsa.fileName	This is a mandatory parameter. ecdsa private key file name.	Data Type: String Range: NA Default Value: ssl_ecdsa_private_key.pem
service.ssl.certificate.k8SecretName	This is a mandatory parameter. Name of the certificate secret.	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.certificate.k8NameSpace	This is a mandatory parameter. Namespace of certificate.	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.certificate.rsa.fileName	This is a mandatory parameter. rsa certificate key file name.	Data Type: String Range: NA Default Value: ocsepp.cer
service.ssl.certificate.ecdsa.fileName	This is a mandatory parameter. ecdsa certificate key file name.	Data Type: String Range: NA Default Value: ssl_ecdsa_certificate.crt
service.ssl.caBundle.k8SecretName	This is a mandatory parameter. Name of the caBundle secret.	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.caBundle.k8NameSpace	This is a mandatory parameter. Namespace of private.	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.caBundle.fileName	This is a mandatory parameter. rsa private key file name.	Data Type: String Range: NA Default Value: caroot.cer
service.ssl.keyStorePassword.k8SecretName	This is a mandatory parameter. Name of the privatekey secret.	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.keyStorePassword.k8NameSpace	This is a mandatory parameter. Namespace of privatekey.	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
service.ssl.keyStorePassword.fileName	This is a mandatory parameter. File name that has password for keyStore.	Data Type: String Range: NA Default Value: key.txt
service.ssl.trustStorePassword.k8SecretName	This is a mandatory parameter. Name of the privatekey secret.	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.trustStorePassword.k8NameSpace	This is a mandatory parameter. Namespace of privatekey.	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.trustStorePassword.fileName	This is a mandatory parameter. File name that has password for trustStore.	Data Type: String Range: NA Default Value: trust.txt
service.ssl.initialAlgorithm	This is a mandatory parameter. Algorithm based on the certificate.	Data Type: String Range: NA Default Value: RS256
service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to plmn-igw specific Service.	Data Type: String Range: NA Default Value: { }
service.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to plmn-igw specific Services.	Data Type: String Range: NA Default Value: { }
deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to plmn-igw specific deployment.	Data Type: String Range: NA Default Value: { }
deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to plmn-igw specific deployment.	Data Type: String Range: NA Default Value: { }
ports.containerPort	This is an optional parameter. ContainerPort represents a network port in a single container.	Data Type: Integer Range: NA Default Value: 8081
ports.containersslPort	This is an optional parameter. Ssl port of the container.	Data Type: Integer Range: NA Default Value: 8443

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
ports.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range: NA Default Value: 9094
log.level.root	This is an optional parameter. Log level for root logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERRORD efault Value: ERROR
log.level.ingress	This is an optional parameter. Log level for ingress logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERRORD efault Value: ERROR
log.level.oauth	This is an optional parameter. Log level for oauth logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERRORD efault Value: ERROR
log.level.updateContainer	This is an optional parameter. log.level.updateContainer.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERRORD efault Value: ERROR
log.level.cncc.root	This is an optional parameter. Log level for cncc logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERRORD efault Value: ERROR
log.level.cncc.audit	This is an optional parameter. Log level for cncc logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.cncc.security	This is an optional parameter. Log level for cncc logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERRORD efault Value: ERROR
log.level.cncc.loggingFilters	This is an optional parameter. Log level filters for cncc logs.	Data Type: String Range: NA Default Value: [ ]
log.level.cncc.loggingMasks	This is an optional parameter. Logging mask filters for cncc logs.	Data Type: String Range: NA Default Value: [ ]
log.traceIdGenerationEnabled	This is an optional parameter. TraceId Generation is Enabled.	Data Type: Boolean Range: True or False Default Value: True

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
resources.limits.cpu	This is an optional parameter. CPU Limit.	Data Type: Integer Range: NA Default Value: 5
resources.limits.initServiceCpu	This is an optional parameter. Init Container CPU Limit.	Data Type: Integer Range: NA Default Value: 1
resources.limits.updateServiceCpu	This is an optional parameter. Update Container CPU Limit.	Data Type: Integer Range: NA Default Value: 1
resources.limits.memory	This is an optional parameter. Memory Limit.	Data Type: String Range: NA Default Value: 5Gi
resources.limits.updateServiceMemory	This is an optional parameter. Update Container Memory Limit.	Data Type: String Range: NA Default Value: 1Gi
resources.limits.initServiceMemory	This is an optional parameter. int Container Memory Limit.	Data Type: String Range: NA Default Value: 1Gi
resources.requests.cpu	This is an optional parameter. CPU for requests.	Data Type: Integer Range: NA Default Value: 5
resources.requests.initServiceCpu	This is an optional parameter. Init Container CPU for requests.	Data Type: Float Range: NA Default Value: 1
resources.requests.updateServiceCpu	This is an optional parameter. Update Container CPU for requests.	D Data Type: Float Range: NA Default Value: 1
resources.requests.memory	This is an optional parameter. Memory for requests.	Data Type: String Range: NA Default Value: 5Gi

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
`resources.requests.updateServiceMemory`	This is an optional parameter. Update Container Memory for requests.	Data Type: String Range: NA Default Value: 1Gi
`resources.requests.initServiceMemory`	This is an optional parameter. Init Container Memory for requests.	Data Type: String Range: NA Default Value: 1Gi
`resources.target.averageCpuUtil`	This is an optional parameter. Average CPU Utilisation.	Data Type: Integer Range: NA Default Value: 70
`maxAvailable`	This is an optional parameter. Number of Pods must always be available, even during a disruption.	Data Type: Integer Range: NA Default Value: 25%
`minReplicas`	This is an optional parameter. Min replicas to scale to maintain an average CPU utilization.	Data Type: Integer Range: NA Default Value: 10
`maxReplicas`	This is an optional parameter. Max replicas to scale to maintain an average CPU utilization.	Data Type: Integer Range: NA Default Value: 10
`routesConfig[0].id`	This is a mandatory parameter. It represents the id of the route.	Data Type: String Range: NA Default Value: cn32f
`routesConfig[0].uri`	This is a mandatory parameter. Service name of the internal microservice of this NF. Note: Provide the actual port number of cn32f, if the user has modified the port.	Data Type: String Range: NA Default Value: http://{{ .Release.Name }}-cn32f-svc:9090/
`routesConfig[0].path`	This is a mandatory parameter. Provide the path to be matched.	Data Type: String Range: NA Default Value: /**
`routesConfig[0].order`	This is a mandatory parameter. Provide the order of the execution of this route.	Data Type: Integer Range: NA Default Value: 1
`routesConfig[0].metadata.requestTimeout`	This is a Optional parameter. requestTimeout is used to set timeout at route level. Value should be in milliseconds.	Data Type: Integer Range: NA Default Value: 2100

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
routesConfig[0].metadata.requiredTime	This is a Optional parameter. requiredTime is minimum time below which request will be rejected if isSbiTimerEnabled is true. Value should be in milliseconds.	Data Type: Integer Range: NA Default Value: 3000
routesConfig[0].metadata.xfccHeaderValidation.validationEnabled	This is a Optional parameter. This is used to provide an option to enable/not enable route level xfccHeaderValidation. It overrides global configuration for xfccHeaderValidation.enabled.	Data Type: Boolean Range: true or false Default Value: false
routesConfig[0].metadata.svcName	This is a Optional parameter. The following parameter is configurable per route in route-metadata is used to track Overload Control data. If this parameter is not configured in route metadata then svc name from routesConfig.uri field is used as the required key to track Overload Control data. The value of "svcName" attribute denotes the back-end service tag to be used as the required key (configurable per route) to track Overload Control data instead of using back-end service name from routesConfig[0].uri as the required key.	Data Type: String Range: NA Default Value:
routesConfig[0].filters.addRequestHeader[0].name	This is a Optional parameter. This field is used for adding a request header at route level. Additional header can be configured by adding a new element in the next line and so on.	Data Type: String Range: NA Default Value:
routesConfig[0].filters.addRequestHeader[0].value	This is a Optional parameter. value of the header to be added.	Data Type: String Range: NA Default Value:
routesConfig[0].filters.methodRateLimiting[0].method	specify the list of methods u have to rate limit. Method based route limiting is applied only for the methods that are configured in each route to be rate limited.	Data Type: String Range: NA Default Value: POST
routesConfig[0].filters.methodRateLimiting[0].burstCapacity	The maximum number of token the bucket can hold.	Data Type: Integer Range: NA Default Value: 1

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
routesConfig[0].filters.methodRateLimiting[0].refillRate	The number of tokens that are added to the bucket during a refill N tokens are added to the bucket every M seconds.	Data Type: Integer Range: NA Default Value: 1
routesConfig[0].filters.methodRateLimiting[0].duration	The amount of time between the refills.	Data Type: Integer Range: NA Default Value: 1
routesConfig[0].removeRequestHeader[0].name	This is a Optional parameter. This field is used for removing a request header at route level. Additional header can be configured by adding a new element in the next line and so on.	Data Type: Range: NA Default Value: myheader1 myheader3
routesConfig[0].removeResponseHeader[0].name	This is a Optional parameter. Below field is used for removing a response header at route level. Additional header can be configured by adding a new element in the next line and so on.	Data Type: Range: NA Default Value: myresponseheader1 myresponseheader3 error-reason
jaegerTracingEnabled	This is an optional parameter. Enable jaeger tracing.	Data Type: Boolean Range: True or False Default Value: False
openTracing.jaeger.udpSender.host	This is an optional parameter. Jaeger Host	Data Type: String Range: NA Default Value: occne-tracer-jaeger-agent.occne-infra
openTracing.jaeger.udpSender.port	This is an optional parameter. Jaeger Port.	Data Type: Integer Range: NA Default Value: 6831
openTracing.jaeger.probabilisticSampler	This is an optional parameter. Trace capture in percentage.	Data Type: Float Range: NA Default Value: 0.5

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
initssl	This is an optional parameter. Enabling it generates key and trust store for https support.	Data Type: Boolean Range: True or False Default Value: True **Note:** • The default value will be true, if the user wants to deploy PLMN Ingress Gateway in HTTPs mode only. • The default value will be false, if the user wants to deploy the PLMN Ingress Gateway only in HTTP mode.
enableIncomingHttp	This is an optional parameter. Enabling it for incoming http request.	Data Type: Boolean Range: True or False Default Value: true **Note:** • The default value will be true, if the user wants to enable incoming request over HTTP mode. • The default value will be false, if the user wants to enable incoming request over HTTPs mode only.
enableIncomingHttps	This is an optional parameter. Enabling it for incoming https request.	Data Type: Boolean Range: True or False Default Value: True **Note:** • The default value will be true, if the user wants to enable incoming request over HTTPs mode only. • The default value will be false, if the user wants to enable incoming request over HTTP mode. • For ASM mode, this value is set to false.
enableOutgoingHttps	This is an optional parameter. Enabling it for outgoing https request.	Data Type: Boolean Range: True or False Default Value: False **Note:** • For PLMN Ingress Gateway, this value must be set to false always. • For ASM mode, this value is set to false.

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
needClientAuth	This is an optional parameter. This must be true if client certificate identity is required in the header x-custom-ingress-client-identity.	Data Type: Boolean Range: True or False Default Value: True
sbiPriorityHeaderName	This is an optional parameter. This parameters defines the header name which will contain the SBI Priority value.	Data Type: String Range: NA Default Value: 3gpp-sbi-message-priority
dnsRefreshDelay	This is an optional parameter. Dns Refresh Delay in milli-seconds.	Data Type: Integer Range: NA Default Value: 120000
rateLimiting.enabled	This is an optional parameter. This parameter enables Rate Limiting on Ingress Gateway.	Data Type: boolean Range: True or False Default Value: false
rssRateLimiter.enabled	This is an optional parameter. This parameter enables Ingress Rate Limiting per Remote SEPP Set on Ingress Gateway.	Data Type: boolean Range: True or False Default Value: false
globalIngressRateLimiting.enabled	This is an optional parameter. This parameter enables Global Rate Limiting on Ingress Gateway.	Data Type: boolean Range: True or False Default Value: false
globalIngressRateLimiting.duration	This is a mandatory parameter(if globalIngressRateLimiting is enabled true)Iterations of time duration(in seconds) for which bucketCapacity and refillRate are reset.	Data Type: Integer Range: NA Default Value: 1
globalIngressRateLimiting.burstCapacity	This is a mandatory parameter. (if globalIngressRateLimiting is enabled true)Holds maximum number of tokens in the bucket for the given duration.	Data Type: Integer Range: NA Default Value: 7500
globalIngressRateLimiting.refillRate	This is a mandatory parameter (if globalIngressRateLimiting is enabled true) Number of tokens to be added to the bucket for the given duration Recommended to have refillRate equal to burstCapacity.	Data Type: Integer Range: NA Default Value: 7500
errorCodeOnRateLimit	This is a conditional parameter (if globalIngressRateLimiting is enabled true) Configurable error code returned when ratelimit is reached. Populated in ProblemDetails response in ProblemDetails.status section.	Data Type: Integer Range: NA Default Value: 429

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
gracefulShutdown.gracePeriod	This is an optional parameter. Grace period to wait for active requests to be executed. If there are no active requests then this period is neglected. # 's' in case of seconds and 'm' in case of minutes.	Data Type: String Range: NA Default Value: 1m
gracefulShutdown.defaultErrorCode	This is a optional parameter Default error code returned at the time of Graceful shut down.	Data Type: Integer Range: NA Default Value: 500
gracefulShutdown.errorDescription	This is an optional parameter. Graceful shut down Error description.	Data Type: String Range: NA Default Value: ""
gracefulShutdown.errorCause	This is an optional parameter. Graceful shut down error cause.	Data Type: String Range: NA Default Value: ""
gracefulShutdown.errorTitle	This is an optional parameter. Graceful shut down error title.	Data Type: String Range: NA Default Value: ""
gracefulShutdown.retryAfter	This is an optional parameter. determines the value in seconds per particular date after which the service should be retried post graceful shutdown.	Data Type: String Range: NA Default Value: ""
gracefulShutdown.redirectUrl	This is an optional parameter. redirection URL for validation failure due to graceful shutdown.	Data Type: String Range: NA Default Value: ""
cfgServer.enabled	This is an optional parameter. Config server switch. For the usage of Policy teams. For other NF's this has to be left false.	Data Type: boolean Range: true or false Default Value: false
cfgClient.enabled	This is an optional parameter. flag to enable config client.	Data Type: boolean Range: true or false Default Value: false
dnsSrv.host	This is an optional parameter. DNS SRV Host name.	Data Type: String Range: NA Default Value: localhost
dnsSrv.port	This is an optional parameter. DNS SRV port number.	Data Type: Integer Range: NA Default Value: 8004
dnsSrv.scheme	This is an optional parameter. DNS SRV scheme name.	Data Type: Range: NA Default Value:

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
nettyIdleTimeout	This is an optional parameter. Netty Idle Timeout in milliseconds.	Data Type: Integer Range: NA Default Value: 120000000 #(ms)
nfFqdn	This is a mandatory parameter. NF FQDN	Data Type: String Range: NA Default Value: sepp2.inter.oracle.com
messageCopy.enabled	This is an optional parameter. This parameter enables or disables the Message feed feature at the Ingress Gateway.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.copyPayload	This is an optional parameter. This parameter specifies whether to copy the message payload in the feed towards Data Director or not. true: the complete payload message is copied. false: Only the header information is copied.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.topicName	This is an optional parameter. Name of the topic to which Ingress Gateway send the payloads.	Data Type: StringRange: NADefault Value: message.copy
messageCopy.ackRequired	This is a mandatory parameter. This parameter specifies if we wait for any acknowledgement from DD.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.retryOnFailure	This is a mandatory parameter. This parameter specifies how many times SEPP should retry if message was not sent to DD successfully.	Data Type: Integer Range: NA Default Value: 0
messageCopy.threadPoolConfigurations.coreSize	This is an optional parameter. core Size for thread pool configuration for message feed thread For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8
messageCopy.threadPoolConfigurations.maxSize	This is an optional parameter. max Size for thread pool configuration for message feed thread For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
messageCopy.threadPoolConfigurations.queueCapacity	This is an optional parameter. queue capacity for thread pool configuration message feed thread For performance enhancement, set the value as 3000.	Data Type: Integer Range: NA Default Value: 1000
messageCopy.security.enabled	This is a mandatory parameter. Security mode enabled for message feed feature.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.security.protocol	This is a conditional parameter. It is used for message feed feature when security is enabled between SEPP and Gateway.	Data Type: String Range: SASL_SSL or SSL Default Value: SASL_SSL
messageCopy.security.tlsVersion	This is a mandatory parameter. TLS version details.	Data Type: String Range: TLSv1.2, TLSv1.3 Default Value: TLSv1.3
kafka.bootstrapAddress	This is an conditional parameter. List of comma- separated Kafka Nodes (to which messages should be copied if messageCopy feature is enabled).	Data Type: String Range: NA Default Value: <kafka-broker>:<port> Port = 9093 for SSL protocol Port = 9094 for SASL_SSL protocol
messageCopy.security.saslConfiguration.username	This is a mandatory parameter. username for DD Refer to DD guide for more details.	Data Type: String Range: NA Default Value: test
messageCopy.security.saslConfiguration.password.k8SecretName	This is a mandatory parameter. Secret name for gateway on which feature enabled.	Data Type: String Range: ocsepp-plmn-secret for PLMN Gateways and ocsepp-n32-secret for N32 Gateways Default Value: message-copy-secret
messageCopy.security.saslConfiguration.password.k8NameSpace	This is a mandatory parameter. Namespace where DD deployed Please refer to DD guide for more details.	Data Type: String Range: NA Default Value: ocingress
messageCopy.security.saslConfiguration.password.fileName	This is a mandatory parameter. File used to create DD secrets Please refer to DD guide for more details	Data Type: String Range: NA Default Value: password.txt

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
kafka.bootstrap-servers	This is an conditional parameter. List of comma-separated DD Nodes IP address The port will change to 9092 if security is disabled	Data Type: String Range: NA Default Value: Default Value: <kafka-broker>:<port> Port = 9093 for SSL protocol Port = 9094 for SASL_SSL protocol
egressRateLimiter.enabled	This is an optional parameter. This parameter is used to enable or disable the egress rate limiting per egress rate limiting list on Ingress Gateway	Data Type: Boolean Range: True or False Default Value: True
clientDisabledExtension	This is an optional parameter. Disables the extension sent by messages originated by clients (ClientHello).	**Data Type**: String **Range**: NA **Default Value**: ec_point_formats
serverDisabledExtension	This is an optional parameter. Disables the extension sent by messages originated by servers (ServerHello).	**Data Type**: String **Range**: NA **Default Value**: null
tlsNamedGroups	This is an optional parameter. Provides a list of values sent in the supported_groups extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
clientSignatureSchemes	This is an optional parameter. Provides a list of values sent in the signature_algorithms extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
service.ssl.tlsVersion	This is a mandatory parameter. Indicates the TLS version.	**Data Type**: String **Range**: • TLSv1.2 , TLSv1.3 • TLSv1.2 • TLSv1.3 **Default Value**: TLSv1.2, TLSv1.3

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
allowedCipherSuites	This is an optional parameter. Indicates allowed Ciphers.	**Data Type**: String **Range**: NA **Default Values**: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 - TLS_CHACHA20_POLY1305_SHA256
cipherSuites	This is an optional parameter. Indicates supported cipher suites.	**Data Type**: String **Range**: NA **Default Values**: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 - TLS_CHACHA20_POLY1305_SHA256
keybasedKafkaProducer	This is a mandatory parameter. This parameter when set to true, enables the functionality of message copy of same transaction into same Kafka partition.	**Data Type**: Boolean **Range**: True or False **Default Value**: False

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
`podSecurityContext.runAsNonRoot`	This is a mandatory parameter. Prevents pod from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
`podSecurityContext.runAsUser`	This is a mandatory parameter. Specifies that all processes in pod must run with the provided user ID.	Data Type: Integer Default Value: 10001
`securityContext.enable`	This is a mandatory parameter. Enables security context for containers.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.readOnlyRootFilesystem`	This is a mandatory parameter. Mounts the mediation container's root filesystem as read-only.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.allowPrivilegeEscalation`	This is a mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the `no_new_privs` parameter gets configured on the container process. `allowPrivilegeEscalation` is always set to true when the container: • is run as privileged • has CAP_SYS_ADMIN	Data Type: Boolean Range: True or False Default Value: False
`containerSecurityContext.runAsNonRoot`	This is a mandatory parameter. Prevents containers from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.privileged`	This is a mandatory parameter. Provides containers' access to the host's resources and kernel capabilities.	Data Type: Boolean Range: True or False Default Value: False
`containerSecurityContext.runAsUser`	This is a mandatory parameter. Specifies that for any container in the pod, all processes must run with the provided user ID.	Data Type: Integer Range: Valid IDs for security context for user Default Value: 10001
`containerSecurityContext.capabilities.drop`	This is a mandatory parameter. Manages Linux capabilities for containers. Using Linux capabilities, you can grant certain privileges to a process without granting all the privileges of the root user.	Data Type: List of strings Range: Valid Linux capabilities Default Value: -all
`enablePodSecurityContext`	This is a mandatory parameter. Enables security context for pod.	Data Type: Boolean Range: True or False Default Value: True

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
deploymentMode	This is a mandatory parameter. This parameter defines the deployment mode for SEPP. That is, Single Stack or Dual Stack.	Data Type: String Range: IPv4, IPv6, IPv6_IPv4, and IPv4_IPv6. Default Value: In single stack mode, Default value: IPv4 In dual stack mode, Default value: IPv6_IPv4 (IPv6 preferred) Roaming Hub: Default value : IPv4 (do not change).
global.lciHeaderConfig.enabled	This is an optional parameter. If this parameter is set to true, LCI headers reporting will be enabled.	Data Type: Boolean Range: True or False Default Value: False
global.lciHeaderConfig.loadThreshold	This is an optional parameter. This parameter defines the load threshold configuration, if the current load level is beyond previously computed load level plus loadThreshold, LCI headers are reported again.	Data Type: Integer Range: NA Default Value: 40
global.lciHeaderConfig.localLciHeaderValidity	This is an optional parameter. This parameter defines the validity period of LCI headers reported to consumer NF. The LCI headers are reported again if the headers reported previously expire.	Data Type: Integer Range: NA Default Value: 1000 (milliseconds)
global.ociHeaderConfig.enabled	This is an optional parameter. If this parameter is set to true, OCI headers reporting will be enabled.	Data Type: Boolean Range: True or False Default Value: False
global.ociHeaderConfig.validityPeriod	This is an optional parameter. Validity period of OCI headers reported to consumer NF. The OCI headers are reported again if the headers reported previously expire.	Data Type: Integer Range: NA Default Value: 5000 (milliseconds)
global.ociHeaderConfig.overloadConfigRange.minor	This is a mandatory parameter, if the feature is enabled. This parameter defines the range to identify minor overload condition.	Data Type: Integer Range: 0 to 100 Default Value: [60-70]
global.ociHeaderConfig.overloadConfigRange.major	This is a mandatory parameter, if the feature is enabled. This parameter defines the range to identify major overload condition.	Data Type: Integer Range: 0 to 100 Default Value: [70-80]

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
global.ociHeaderConfig.overloadConfigRange.critical	This is a mandatory parameter, if the feature is enabled. This parameter defines the range to identify critical overload condition.	Data Type: Integer Range: 0 to 100 Default Value: [80-100]
global.ociHeaderConfig.reductionMetrics.minor	This is a mandatory parameter, if the feature is enabled. This parameter defines the reduction metric to be reported for minor overload condition.	Data Type: Integer Range: 1 to 9 Default Value: 5
global.ociHeaderConfig.reductionMetrics.major	This is a mandatory parameter, if the feature is enabled. This parameter defines the reduction metric to be reported for major overload condition.	Data Type: Integer Range: 5 to 15 Default Value: 10
global.ociHeaderConfig.reductionMetrics.critical	This is a mandatory parameter, if the feature is enabled. This parameter defines the reduction metric to be reported for critical overload condition.	Data Type: Integer Range: 10 to 50 Default Value: 30
global.nfInstanceId	This is a mandatory parameter, if the feature is enabled. NF Instance Id of producer NF.	Data Type: String Range: NA Default Value: 6faf1bbc-6e4a-4454-a507-a14ef8e1bc11
global.nfType	This is a mandatory parameter, if the feature is enabled. NF type of producer NF.	Data Type: String Range: NA Default Value: NA
global.nfFqdn	This is a mandatory parameter. This is the NF FQDN for SEPP	Data Type: String Range: NA Default Value: NA
global.svcToSvcInstanceIdMapping.svcName	This is an optional parameter. This parameter defines the back-end service name which should match producerSvcIdHeader value and perf info reported service name for LCI or OCI headers reporting.	Data Type: String Range: NA Default Value: nf-registration
global.svcToSvcInstanceIdMapping.serviceInstanceId	This is an optional parameter. This parameter defines the Back-end service instance id to be included in LCI / OCI headers.	Data Type: String Range: NA Default Value: fe7d992b-0541-4c7d-ab84-c6d70b1b01b1
global.perfInfoConfig.pollingInterval	This is an optional parameter. This parameter defines the Configurable interval at which load infromation is polled from perf-info service at Gateway.	Data Type: Integer Range: NA Default Value: 5000

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
`global.perfInfoConfig.serviceName`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info service name.	Data Type: String Range: NA Default Value: NA
`global.perfInfoConfig.host`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info Host IP.	Data Type: String Range: NA Default Value: NA
`global.perfInfoConfig.PORT`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info port.	Data Type: String Range: NA Default Value: NA
`global.perfInfoConfig.perfInfoRequestMap`	This is a mandatory parameter, if the feature is enabled. This parameter defines the Perf-Info service request endpoint.	Data Type: String Range: NA Default Value: NA
`tlsVersionSupportForKubeApiServer.enabled`	This is an optional parameter. This parameter enables or disables TLS 1.3 support for establishing communication between Gateway Services and Kubernetes API server (Kube\u0002Api-Server). If this parameter is enabled, support for establishing communication with Kube\u0002Api-Server is provided through TLS 1.3, along with TLS 1.2 as configured in `kubeApiServerTlsVersion`. If this parameter is disabled, support for communication with Kube-Api-Server is provided only through TLS 1.2.	Data Type: Boolean Range: True or False Default Value: False
`tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`	This is a mandatory parameter. This parameter defines the supported TLS versions used by Gateway Services to communicate with the Kube-API-Server.	Data Type: String Range: TLS 1.2 and TLS 1.3 Default Value: TLS 1.3
`tlsVersionSupportForKubeApiServer.cipherSuites`	This is a mandatory parameter. This parameter indicates the Cipher suites that are compliant with the configured `tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`	Data Type: String Range: NA Default Value: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CH ACHA20 _POLY1305_SHA 256

Table 3-9 (Cont.) plmn-ingress-gateway

Name	Description	Details
`tlsVersionSupportForKubeApiServer.featureSecrets`	This is an optional parameter. This parameter indicates the list of all the secrets that are used for all the features of Gateway Services. These secrets are volume mounted during the pod deployment.	Data Type: String Range: NA Default Value: • ocegress -secret1 • ocegress -secret2 • ocegress -secret3
`overloadControlLocalDiscardEnabled`	This is an optional parameter. This parameter enables each pod independently to discard requests based on its local load. This parameter can have the following values: • true: No coherence-based token reservation is required. • false: Coherence is used for token reservations across pods.	Data Type: Boolean Range: true or false Default Value: false

3.1.9 n32-egress-gateway

This section includes information about the n32-egress-gateway parameters of the SEPP.

Table 3-10 n32-egress-gateway

Name	Description	Details
`cmName`	This is an optional parameter. Name of the configmap.	Data Type: String Range: NA Default Value: egressgateway
`serviceMeshCheck`	This is a mandatory parameter. Enabled when deployed in serviceMesh.	Data Type: Boolean Range: true false Default Value: false
`istioSidecarQuitUrl`	This is a mandatory parameter. The sidecar (istio quit url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/quitquitquit
`istioSidecarReadyUrl`	This is a mandatory parameter. The sidecar (istio ready url)when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/ready
`global.k8sResources.hpat.supportedVersions`	Kubernetes resource.	Data Type: String Range: NA Default Value: autoscaling/v1

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`global.k8sResources.pdb.supportedVersions`	Kubernetes resource PDB supported version.	Data Type: String Range: NA Default Value: policy/v1
`global.logStorage`	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
`global.crictlStorage`	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
`global.ephemeralStorageLimit`	This is an optional parameter. Ephemeral storage Limit.	Data Type: Integer Range: NA Default Value: 1024
`extraContainers`	This is a mandatory parameter. The attribute is used to control the usage of extra container(DEBUG tool). Allowed Values: DISABLED, ENABLED, USE_GLOBAL_VALUE If assigned with ENABLED or USE_GLOBAL_VALUE, then ensure "extraContainers Tpl" yaml chunk is defined at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: String Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
`prefix`	This is a optional parameter. Support for multiple egress instances. When set to some value then that value is used in the name of resources along with release name so that there is any clash between the instances. When the value of this flag is set to ' ' then the resources are prepended with release name only.When set to some value then that value will be used in the names of resources along with release name.	Data Type: String Range: NA Default Value: 'n32'
`sepp.removeUnusedProxyAfter`	This is an optional parameter. Time in minutes after which unsed proxy beans are removed. If this parameter is not added, then default value is picked up.	Data Type: Integer Range: NA Default Value: 30
`sepp.forwardProxy`	This is an optional parameter. Flag to enable sepp forward proxy.	Data Type: Boolean Range: NA Default Value: true

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
sepp.tlsConnectionMode	Set true only if sepp.forwardProxy is true,otherwise it wont have effect. For ASM this will be set to false.	Data Type: Boolean Range: true or false Default Value: true
serviceEgressGateway.port	This is a mandatory parameter. Egress Gateway port.	Data Type: Integer Range: NA Default Value: 8080
serviceEgressGateway.sslPort	This is a mandatory parameter. SSL Port.	Data Type: Integer Range: NA Default Value: 8442
serviceEgressGateway.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range: NA Default Value: 9094
deploymentEgressGateway.image	This is an optional parameter. Image name of Ingress gateway.	Data Type: String Range: NA Default Value: ocegress_gateway
deploymentEgressGateway.imageTag	This is an optional parameter. Image Tag name of ingress gateway.	Data Type: String Range: NA Default Value: helm-gateway-egress-tag
deploymentEgressGateway.pullPolicy	This is an optional parameter. Image Pull Policy.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
initContainersImage.name	This is an optional parameter. Image name of initContainer.	Data Type: String Range: NA Default Value: configurationinit
initContainersImage.tag	This is an optional parameter. Image tag name of initContainer.	Data Type: String Range: NA Default Value: helm-gateway-egress-tag
initContainersImage.pullPolicy	This is an optional parameter. Image Pull Policy.	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
updateContainersImage.name	This is an optional parameter. Image name of updateContainer	Data Type: String Range: NADefault Value: configurationupdate
updateContainersImage.tag	This is an optional parameter. Image tag name of updateContainer	Data Type: String Range: NA Default Value: helm-gateway-egress-tag

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`updateContainersImage.pullPolicy`	This is an optional parameter. Image Pull Policy	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`dbHookImage.name`	This is an optional parameter. Image name of dbHook	Data Type: String Range: NA Default Value: common_config_hook
`dbHookImage.tag`	This is an optional parameter. Image tag name of dbHook	Data Type: String Range: NA Default Value: helm-gateway-egress-tag
`dbHookImage.pullPolicy`	This is an optional parameter. Pull Policy of Image	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`initssl`	This is an optional parameter. Enabling it generates key and trust store for https support	Data Type: Boolean Range: True or False Default Value: true **Note:** • The default value will be true, if the user wants to deploy in non ASM mode. • The default value will be false, if the user wants to deploy in ASM mode.
`enableIncomingHttp`	This is an optional parameter. Enabling it for incoming http request	Data Type: Boolean Range: True or False Default Value: true **Note:** This value must be set to true always.
`enableIncomingHttps`	This is an optional parameter. Enabling it for incoming http request	Data Type: Boolean Range: True or False Default Value: false **Note:** This value must be set to false always.
`enableOutgoingHttps`	This is an optional parameter. Enabling it for incoming https request	Data Type: Boolean Range: True or False Default Value: true **Note:** • The default value will be true, if the user wants to deploy in non ASM mode. • The default value will be false, if the user wants to deploy in ASM mode.

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`httpsTargetOnly`	This is an optional parameter. This is global parameter which will be taken into consideration if route (under routeConfig section) based httpsTargetOnly parameter is not available. true: Select SbiRouting instances for https list only false: Run existing logic as per provided scheme. Note: double quotes to be enclosed for values of httpsTargetOnly	Data Type: Boolean Range: True or False Default Value: false
`httpRuriOnly`	This is an optional parameter. Global parameter is taken into consideration if route (under routeConfig section) based httpRuriOnly parameter is not available. true: Means change Scheme of RURI to http false: Keep scheme as is.	Data Type: Boolean Range: True or False Default Value: false
`sbiRouting.sbiRoutingDefaultScheme`	This is an optional parameter. Default scheme applicable when 3gpp-sbi-target apiroot header is missing	Data Type: String Range: NA Default Value: https
`sbiRouting.sbiRerouteEnabled`	This is an optional parameter. Set this flag to true if re-routing to multiple SCP instances is to be enabled.	Data Type: Boolean Range: True or False Default Value: true
`log.level.root`	This is an optional parameter. Log level for root logs	Data Type: ENUM Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
`log.level.egress`	This is an optional parameter. Log level for ingress logs	Data Type: ENUM Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
`log.level.oauth`	This is an optional parameter. Log level for oauth logs	Data Type: ENUM Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
`log.level.updateContainer`	This is an optional parameter. Log level for update container logs	Data Type: ENUM Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
`log.level.hook`	This is an optional parameter. Log level for hook	Data Type: ENUM Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
service.ssl.privateKey.k8SecretName	This is a mandatory parameter. Name of the privatekey secret	Data Type: StringRange: NADefault Value: ocsepp-n32-secret
service.ssl.privateKey.k8NameSpace	This is a mandatory parameter. Namespace of privatekey	Data Type: StringRange: NADefault Value: DEPLOYMENT_NAMESPACE
service.ssl.privateKey.rsa.fileName	This is a mandatory parameter. rsa private key file name	Data Type: StringRange: NADefault Value: rsa_private_key_pkcs1.pem
service.ssl.privateKey.ecdsa.fileName	This is a mandatory parameter. ecdsa private key file name	Data Type: StringRange: NADefault Value: ssl_ecdsa_private_key.pem
service.ssl.certificate.k8SecretName	This is a mandatory parameter. Name of the certificate secret	Data Type: StringRange: NADefault Value: ocsepp-n32-secret
service.ssl.certificate.k8NameSpace	This is a mandatory parameter. Namespace of certificate	Data Type: StringRange: NADefault Value: DEPLOYMENT_NAMESPACE
service.ssl.certificate.rsa.fileName	This is a mandatory parameter. rsa certificate key file name	Data Type: StringRange: NADefault Value: ocsepp.cer
service.ssl.certificate.ecdsa.fileName	This is a mandatory parameter. ecdsa certificate key file name	Data Type: StringRange: NADefault Value: ssl_ecdsa_certificate.crt
service.ssl.caBundle.k8SecretName	This is a mandatory parameter. Name of the caBundle secret	Data Type:String Range: NA Default Value:ocsepp-n32-secret
service.ssl.caBundle.k8NameSpace	This is a mandatory parameter. Namespace of private	Data Type: StringRange: NADefault Value: DEPLOYMENT_NAMESPACE
service.ssl.caBundle.fileName	This is a mandatory parameter. rsa private key file name	Data Type: StringRange: NADefault Value: caroot.cer
service.ssl.keyStorePassword.k8SecretName	This is a mandatory parameter. Name of the privatekey secret	Data Type:StringRange: NADefault Value: ocsepp-n32-secret
service.ssl.keyStorePassword.k8NameSpace	This is a mandatory parameter. Namespace of privatekey	Data Type: StringRange: NADefault Value: DEPLOYMENT_NAMESPACE
service.ssl.keyStorePassword.fileName	This is a mandatory parameter. File name that has password for keyStore	Data Type: StringRange: NADefault Value: key.txt
service.ssl.trustStorePassword.k8SecretName	This is a mandatory parameter. Name of the privatekey secret	Data Type: StringRange: NADefault Value: ocsepp-n32-secret
service.ssl.trustStorePassword.k8NameSpace	This is a mandatory parameter. Namespace of privatekey	Data Type: StringRange: NADefault Value: DEPLOYMENT_NAMESPACE
service.ssl.trustStorePassword.fileName	This is a mandatory parameter. File name that has password for trustStore	Data Type: StringRange: NADefault Value: trust.txt

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
service.ssl.initialAlgorithm	This is a mandatory parameter. Algorithm based on the certificate	Data Type: StringRange: NADefault Value: RSA256
service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to n32-egw specific Service	Data Type: String Range: NA Default Value:{}
service.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to n32-egw specific Services	Data Type: String Range: NA Default Value:{}
deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to n32-egw specific deployment	Data Type: String Range: NA Default Value:{}
deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to n32-egw specific deployment	Data Type: String Range: NA Default Value:{}
deDupeResponseHeader	This is an optional parameter. it is used for handling duplicate values in response headers. Multiple values can be provided with space. # Ex: content-type nettylatency requestmethod, RETAIN_LAST	Data Type: String Range: nettylatency, requestmethod, RETAIN_LAST Default Value: content-type, RETAIN_LAST
commonCfgClient.enabled	This is an optional parameter. Set it to true if persistent configuration needs to be enabled.	Data Type: Boolean Range: True or False Default Value: true
commonCfgServer.configServerSvcName	This is a mandatory parameter if commonCfgClient. enabled is set to true Service name of common configuration service to which the client tries to poll for configuration updates	Data Type: String Range: NA Default Value: config-mgr-svc
commonCfgServer.host	This is an optional parameter. No (It is needed if commonCfgServer.configServerSvcName is not available) Host name of Common configuration server to which client tries to poll for configuration updates. This value is picked up if commonCfgServer .configServer SvcName is not available	Data Type: String Range: NA Default Value: config-mgr-svc

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
commonCfgServer.port	This is a mandatory parameter if commonCfgClient. enabled is set to true Port of Common Configurationserver	Data Type: Integer Range: NA Default Value: 9090
commonCfgServer.pollingInterval	This is a mandatory parameter if commonCfgClient. enabled is set to true This is the interval between two subsequent polling requests from config client toserver	Data Type: Integer Range: NA Default Value: 5000
commonServiceName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. This is the common service name that is currently requesting for configuration updates from server	Data Type: string Range: NA Default Value: egw
enableSecondaryInstance	To enable secondary instance of config client enableSecondaryInstance must beset to true.	Data Type: Boolean Range: true or false Default Value: false
ingressServiceName	IngressServiceName must be set with the value of commonServiceName present in ingress values.yaml.	Data Type: string Range: NA Default Value: igw
ingressReleaseVersion	IngressReleaseVersion must be same as version in Chart.yaml of IngressGateway.	Data Type: string Range: NA Default Value: helm-gateway-ingress-tag
restoreBackupOnInstall	This is an optional parameter. This flag when enabled picks up the data from the backup table during installation of gateway	Data Type: Boolean Range: true or false Default Value: false
dbConfig.dbHost	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Hostname of Mysql in which the configuration must be stored	Data Type: String Range: NA Default Value: sepp-mysql-svc
dbConfig.dbPort	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Port of mysql	Data Type: Integer Range: NA Default Value: 3306
dbConfig.configFile	This is a mandatory parameter. (if commonCfgClient enabled is set to true) File name for initial configuration that must be stored in the db	Data Type: String Range: NA Default Value: defaultconfig.yaml

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
dbConfig.schemaFile	This is a mandatory parameter. (if commonCfgClient enabled is set to true) File name for json schema validation	Data Type: String Range: NA Default Value: defaultschema.json
dbConfig.secretName	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Secret name from which the db name, db password and db user name is picked	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
dbConfig.dbName	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Database name	Data Type: String Range: NA Default Value: seppdb
dbConfig.dbUNameLiteral	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Name of the Key configured for "DB Username" in Secret with following name: "<dbConfig.secretName>"	Data Type: String Range: NA Default Value: mysql-username
dbConfig.dbPwdLiteral	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Name of the Key configured for "DB Password" in Secret with following name: "<dbConfig.secretName>"	Data Type: String Range: NA Default Value: mysql-password
dbConfig.dbEngine	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
routesConfig[0].filterNameReqEntryargs.headers[0].headersList[0].defaultVal	This is an optional parameter This parameter defines the default value for custom headers to be added in incoming request	Data Type: String Range: NA Default Value: script:shm-02,x-exit-new-req
routesConfig[0].filterNameReqEntry.args.headers[0].headersList[0].source	This is an optional parameter This parameter defines the source for custom headers to be added	Data Type: String Range: NA Default Value: incomingReq
routesConfig[0].filterNameReqEntry.args.headers[0].headersList[0].sourceHeader	This is an optional parameter This parameter defines the source header for custom headers to be added in incoming request	Data Type: String Range: NA Default Value: x-current-user

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
routesConfig[0].filterNameReqExit.name	This is an optional parameter This parameter defines the custom header filter name in egress request	Data Type: String Range: NA Default Value: CustomReqHeaderExitFilter
routesConfig[0].filterNameReqExit.args.headers.methods	This is an optional parameter This parameter defines the method in egress request for adding custom header filter	Data Type: String Range: NA Default Value: ALL
routesConfig[0].filterNameReqExit.args.headers.headersList[0].headerName	This is an optional parameter This parameter defines the list of custom headers to be added in egress request	Data Type: String Range: NA Default Value: x-headeReq-2021
routesConfig[0].filterNameReqExit.args.headers.headersList[0].defaultVal	This is an optional parameter This parameter defines the default value for custom headers to be added in egress request	Data Type: Integer Range: NA Default Value: 0505
routesConfig[0].filterNameReqExit.args.headers.headersList[0].source	This is an optional parameter This parameter defines the source for custom headers to be added	Data Type: String Range: NA Default Value: incomingReq
routesConfig[0].filterNameReqExit.args.headers.headersList[0].sourceHeader	This is an optional parameter This parameter defines the source header for custom headers to be added in egress request	Data Type: String Range: NA Default Value: x-current-user
routesConfig[0].filterNameResEntry.name	This is an optional parameter This parameter defines the custom header filter name in incoming response	Data Type: String Range: NA Default Value: CustomResHeaderEntryFilter
routesConfig[0].filterNameResEntry.args.headers[0].methods	This is an optional parameter This parameter defines the method in incoming response for adding custom header filter	Data Type: String Range: NA Default Value: ALL
routesConfig[0].filterNameResEntry.args.headers[0].headersList[0].headerName	This is an optional parameter This parameter defines the list of custom headers to be added in incoming response	Data Type: String Range: NA Default Value: x-headeRes-3014
routesConfig[0].filterNameResEntry.args.headers[0].headersList[0].defaultVal	This is an optional parameter This parameter defines the default value for custom headers to be added in incoming response	Data Type: String Range: NA Default Value: pqr
routesConfig[0].filterNameResEntry.args.headers[0].headersList[0].source	This is an optional parameter This parameter defines the source for custom headers to be added	Data Type: String Range: NA Default Value: incomingRes

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
routesConfig[0].filterNameResEntry.args.headers[0].headersList[0].sourceHeader	This is an optional parameter This parameter defines the source header for custom headers to be added in incoming response	Data Type: String Range: NA Default Value: x-current-hooman
routesConfig[0].filterNameResExit.name	This is an optional parameter This parameter defines the custom header filter name in egress response	Data Type: String Range: NA Default Value: CustomResHeaderExitFilter
routesConfig[0].filterNameResExit.args.headers.methods	This is an optional parameter This parameter defines the method in egress response for adding custom header filter	Data Type: String Range: NA Default Value: ALL
routesConfig[0].filterNameResExit.args.headers.headersList[0].headerName	This is an optional parameter This parameter defines the list of custom headers to be added in egress response	Data Type: Range: NA Default Value: x-headeRes-2021
routesConfig[0].filterNameResExit.args.headers.headersList[0].defaultVal	This is an optional parameter This parameter defines the default value for custom headers to be added in egress response	Data Type: Integer Range: NA Default Value: 0909
routesConfig[0].filterNameResExit.args.headers.headersList[0].source	This is an optional parameter This parameter defines the source for custom headers to be added	Data Type: String Range: NA Default Value: incomingRes
routesConfig[0].filterNameResExit.args.headers.headersList[0].sourceHeader	This is an optional parameter This parameter defines the source header for custom headers to be added in egress response	Data Type: String Range: NA Default Value: x-current-hooman
routesConfig[0].filterName1.name	This is a mandatory parameter if routesConfig[0].metadata.sbiRoutingEnabled is true Provide filtername as "SBIRoutingFilter" If FilterName1 is not provided then it would be considered as direct Egress Gateway path and configured accordingly during deployment.	Data Type: String Range: NA Default Value: SbiRouting
routesConfig[0].filterName1.args.peerSetIdentifier	This is a mandatory parameter if routesConfig[0].metadata.sbiRoutingEnabled is true This flag maps to id of peerSetConfiguration	Data Type: String Range: NA Default Value: set0

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
routesConfig[0].filterName 1.args.customPeerSelectorE nabled	This is an optional parameter This flag allows the user to send request to a particular instance directly when enabled according to "ocalternaterouteattempt" header	Data Type: BooleanRange: True or FalseDefault Value: false
routesConfig[0].filterName 1.args.errorHandling.error CriteriaSet	This is a mandatory parameter, if the NF wants to enable SBI Rerouting Feature. This flag maps to the id of sbiRoutingErrorCriteriaSets configuration.	Data Type: String Range: NA Default Value: scp_direct2_criteria_1
routesConfig[0].filterName 1.args.errorHandling.actio nSet	This is a mandatory parameter, if the NF wants to enable SBI Rerouting Feature. This flag maps to the id of sbiRoutingErrorActionSets configuration	Data Type: String Range: NA Default Value: scp_direct2_action_1
routesConfig[0].filterName 1.args.errorHandling.prior ity	This is a mandatory parameter, if the NF wants to enable SBI Rerouting Feature. This maps the priority of execution for sbiRoutingErrorCriteriaSets & sbiRoutingErrorActionSets mapping	Data Type: integer Range: NA Default Value: 1
routesConfig[0].removeRequ estHeader[0].name	This is an optional parameter This field is used for removing a request header at route level. Additional header can be configured by adding a new element in the next line and so on. The value of "name" attribute denotes the name of the request header which is to be removed at route level. Add a new entry in next line for every header to be removed.	Data Type: String Range: NA Default Value: myheader1 myheader3

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
routesConfig[0].removeResponseHeader[0]0.name	This is an optional parameter This field is used for removing a responseheader at route level. Additional header can be configured by adding a new element in the next line and so on. The value of "name" attribute denotes the name of the request header which is to be removed at route level. Add a new entry in next line for every header to be removed.	Data Type: String Range: NA Default Value: myresponseheader1 myresponseheader3
dnsSrv.host	This is a mandatory parameter, if DnsSrv integration is required, else optional Host of DNS Alternate Route Service	Data Type: String Range: NA Default Value: 10.75.225.67
dnsSrv.alternateRouteSvcName	This is a mandatory parameter, if DnsSrv integration is required and Service Name is expected to be provided otherwise optional Service name of Alternate Route Service. If Service name is provided , then this parameter would be picked for integrating Egress Gateway with alternate route service. If IP or Fqdn is expected to be provided then update this parameter as blank and update above parameter accordingly. If this parameter is populated with data then above parameter would be ignored.	Data Type: String Range: NA Default Value: alternate-route
dnsSrv.port	This is a mandatory parameter, if DnsSrv integration is required, else optional. Port of DNS Alternate Route Service	Data Type: String Range: NA Default Value: 80
dnsSrv.scheme	This is a mandatory parameter, if DnsSrv integration is required, else optional. Scheme of request that need to be sent to alternate route service. By default it is http. Just gave configurable privilege for future.	Data Type: String Range: NA Default Value: http

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
dnsSrv.requestTimeout	This is a mandatory parameter, if DnsSrv integration is required, else optional. Duration for Egress Gateway to Alternate Route Service DNS SRV request query execution.	Data Type: Integer Range: NA Default Value: 1000 ms
dnsSrv.connectTimeout	This is a mandatory parameter, if DnsSrv integration is required, else optional. Duration for Egress Gateway to Alternate Route Service DNS SRV connection timeout.	Data Type: Integer Range: NA Default Value: 10000 ms
dnsSrv.fqdnSchemesForProbing	This is a mandatory parameter. • Probing is executed as part of the container probe. An empty list indicates no probing. • Probing sends or looks up requests to DNS SRV host for the configured FQDN and scheme. • Probing is done sequentially for FQDN scheme combination, adjust container probe time based on the number of FQDNs.	Data Type: string Range: NA Default Value: []
dnsSrv.backoffDelay	This is a mandatory parameter. Indicates the wait time between retry attempts when DNS service discovery fails.	Data Type: Integer Range: NA Default Value: 5000 ms
dnsSrv.errorCodeOnDNSResolutionFailure	This is a mandatory parameter, if DnsSrv integration is required, else optional. Currently, this value cannot be modified.	Data Type: Integer Range: NA Default Value: 425 ms
dnsSrv.errorDescriptionOnDNSResolutionFailure	This is an optional parameter. Error description for DNS resolution failure. Populated in ProblemDetails response in ProblemDetails.detail section. Currently, this value cannot be modified.	Data Type: String Range: NA Default Value: ""
dnsSrv.errorTitleOnDNSResolutionFailure	This is an optional parameter. Error title for DNS resolution failure. Populated in ProblemDetails response in ProblemDetails.title section. Currently, this value cannot be modified.	Data Type: String Range: NA Default Value: ""

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
dnsSrv.errorCauseOnDNSResolutionFailure	This is an optional parameter. Error cause for DNS resolution failure. Populated in ProblemDetails response in ProblemDetails.cause section. Currently, this value cannot be modified.	Data Type: String Range: NA Default Value: ""
jaegerTracingEnabled	This is an optional parameter. Enable jaeger tracing	Data Type: Boolean Range: True or False Default Value: false
openTracing.jaeger.udpSender.host	This is an optional parameter. Jaeger Host	Data Type: String Range: NA Default Value: occne-tracer-jaeger-agent.occne-infra
openTracing.jaeger.udpSender.port	This is an optional parameter. Jaeger Port	Data Type: Integer Range: NA Default Value: 6831
openTracing.jaeger.probabilisticSampler	This is an optional parameter. Trace capture in percentage	Data Type: Float Range: NA Default Value: 0.5
dnsRefreshDelay	This is an optional parameter. Dns Refresh Delay in milli-seconds	Data Type: Integer Range: NA Default Value: 10000 ms
resources.limits.cpu	This is an optional parameter. CPU Limit	Data Type: Integer Range: NA Default Value: 5
resources.limits.initServiceCpu	This is an optional parameter. Init Container CPU Limit	Data Type: Float Range: NA Default Value: 1
resources.limits.updateServiceCpu	This is an optional parameter. Update Container CPU Limit	Data Type: Float Range: NA Default Value: 1
resources.limits.memory	This is an optional parameter. Memory Limit	Data Type: String Range: NA Default Value: 5Gi
resources.limits.updateServiceMemory	This is an optional parameter. Update Container Memory Limit	Data Type:String Range: NA Default Value: 1Gi
resources.limits.initServiceMemory	This is an optional parameter. int Container Memory Limit	Data Type: String Range: NA Default Value: 1Gi
resources.requests.cpu	This is an optional parameter. CPU for requests	Data Type: Integer Range: NA Default Value: 5

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`resources.requests.initServiceCpu`	This is an optional parameter. Init Container CPU for requests	Data Type: Float Range: NA Default Value: 1
`resources.requests.updateServiceCpu`	This is an optional parameter. Update Container CPU for requests	Data Type:Float Range: NA Default Value: 1
`resources.requests.memory`	This is an optional parameter. Memory for requests	Data Type: String Range: NA Default Value: 5Gi
`resources.requests.updateServiceMemory`	This is an optional parameter. Update Container Memory for requests	Data Type: String Range: NA Default Value: 1Gi
`resources.requests.initServiceMemory`	This is an optional parameter. Init Container Memory for requests	Data Type: String Range: NA Default Value: 1Gi
`resources.target.averageCpuUtil`	This is an optional parameter. Resource Requirements(avg cpu utilisation)	Data Type: Integer Range: NA Default Value: 70
`minAvailable`	This is an optional parameter. Number of Pods must always be available, even during a disruption	Data Type: Integer Default Value: 1
`maxUnavailable`	This is an optional parameter. Number of Pods that will be unavailable during a disruption	Data Type: Integer Range: NA Default Value: 25%
`minReplicas`	This is an optional parameter. Min replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
`maxReplicas`	This is an optional parameter. Max replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
`connectionTimeout`	This is an optional parameter. Connection timeout in milliseconds	Data Type: Integer Range: NA Default Value: 60
`requestTimeout`	This is an optional parameter. Request Timeout in milli seconds	Data Type: Integer Range: NA Default Value: 1000 #ms
`gracefulCloseDelay`	This is an mandatory parameter. gracefulCloseDelay value should be positive value greater than request Timeout and lesser than jettyIdleTimeout. If gracefulCloseDelay is set to 0 then default value of 30000 ms will be considered internally.	Data Type: Integer Range: NA Default Value: 1500 ms

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
gracefulShutdown.gracePeriod	This is an optional parameter. Grace period to wait for active requests to be executed. If there are no active requests then this period is neglected. 's' in case of seconds and 'm' in case of minutes	Data Type: String Range: NA Default Value: 1m
gracefulShutdown.defaultErrorCode	This is a optional parameter Default error code returned at the time of Graceful shut down	Data Type: Integer Range: NA Default Value: 500
gracefulShutdown.errorDescription	This is an optional parameter. Graceful shut down Error description	Data Type: String Range: NA Default Value: Shutdown in progress
gracefulShutdown.errorTitle	This is an optional parameter. Graceful shut down error title	Data Type: String Range: NA Default Value: Graceful shutdown
gracefulShutdown.errorCause	This is an optional parameter. Graceful shut down error cause	Data Type: String Range: NA Default Value: Shutdown
egressRateLimiting.enabled	This is a mandatory parameter. This parameter enables Global Rate Limiting on Gateway.	Data Type: boolean Range: True or False Default Value: false
egressRateLimiting.duration	This is a mandatory parameter. This parameter defines theduration to decide how frequently to refill(in seconds)	Data Type:Integer Range: NA Default Value: 1
egressRateLimiting.bucketCapacity	This is a mandatory parameter. This parameter defines the Bucket size in which capacity to handle traffic burst is defined.	Data Type: Integer Range: NA Default Value: 7500
egressRateLimiting.refillRate	This is a mandatory parameter. This parameter defines the number of tokens to be added to refill the bucket	Data Type: Integer Range: NA Default Value: 7500
egressRateLimiting.errorCodeOnRateLimit	This is a mandatory parameter. This parameter defines the configurable error code to be returned	Data Type: Integer Range: NA Default Value: 429
nettyIdleTimeout	This is an optional parameter. Netty Idle Timeout in milli seconds	Data Type: Integer Range: NA Default Value: 120000000
nfFqdn	This is a mandatory parameter. NF FQDN	Data Type:Integer Range: NA Default Value: sepp2.inter.oracle.com

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
messageCopy.enabled	This is an optional parameter. This parameter enables or disables the Message feed feature at the Ingress Gateway.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.copyPayload	This is an optional parameter. This parameter specifies whether to copy the message payload in the feed towards Data Director or not. true: the complete payload message is copied. false: Only the header information is copied.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.topicName	This is an optional parameter. Name of the topic to which Ingress Gateway send the payloads.	Data Type:String Range: NA Default Value:message.copy
messageCopy.ackRequired	This is a mandatory parameter. This parameter specifies if we wait for any acknowledgement from DD.	Data Type: Boolean Range: True or False Default Value:False
messageCopy.retryOnFailure	This is a mandatory parameter. This parameter specifies how many times SEPP should retry if message was not sent to DD successfully.	Data Type: Integer Range: NA Default Value: 0
messageCopy.threadPoolConfigurations.coreSize	This is an optional parameter. core Size for thread pool configuration for message feed thread For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8
messageCopy.threadPoolConfigurations.maxSize	This is an optional parameter. max Size for thread pool configuration for message feed thread For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8
messageCopy.threadPoolConfigurations.queueCapacity	This is an optional parameter. queue capacity for thread pool configuration message feed thread For performance enhancement, set the value as 3000.	Data Type: Integer Range: NA Default Value: 1000
messageCopy.security.enabled	This is a mandatory parameter. Security mode enabled for message feed feature	Data Type: Boolean Range: True or False Default Value:False
messageCopy.security.protocol	This is a conditional parameter. It is used for message feed feature when security is enabled between SEPP and Gateway.	Data Type: String Range: SASL_SSL or SSL Default Value: SASL_SSL

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`messageCopy.security.tlsVersion`	This is a mandatory parameter. TLS version details.	Data Type: String Range: TLSv1.2, TLSv1.3 Default Value: TLSv1.3
`kafka.bootstrapAddress`	This is an conditional parameter. List of comma- separated Kafka Nodes (to which messages should be copied if messageCopy feature is enabled).	Data Type: String Range: NA Default Value: <kafka-broker>:<port> Port = 9093 for SSL protocol Port = 9094 for SASL_SSL protocol
`messageCopy.security.saslConfiguration.username`	This is a mandatory parameter. username for DD Refer to DD guide for more details	Data Type: String Range: NA Default Value: test
`messageCopy.security.saslConfiguration.password.k8SecretName`	This is a mandatory parameter. Secret name for gateway on which feature enabled	Data Type: String Range: ocsepp-plmn-secret for PLMN Gateways and ocsepp-n32-secret for N32 Gateways Default Value: message-copy-secret
`messageCopy.security.saslConfiguration.password.k8NameSpace`	This is a mandatory parameter. Namespace where DD deployed Please refer to DD guide for more details	Data Type: String Range: Default Value:ocegress
`messageCopy.security.saslConfiguration.password.fileName`	This is a mandatory parameter. File used to create DD secrets Please refer to DD guide for more details	Data Type:String Range: NA Default Value: password.txt
`kafka.bootstrap-servers`	This is an conditional parameter. List of comma-separated DD Nodes IP address The port will change to 9092 if security is disabled	Data Type: String Range: NA Default Value: Default Value: <kafka-broker>:<port> Port = 9093 for SSL protocol Port = 9094 for SASL_SSL protocol
`clientDisabledExtension`	This is an optional parameter. Disables the extension sent by messages originated by clients (ClientHello).	**Data Type**: String **Range**: NA **Default Value**: ec_point_formats
`serverDisabledExtension`	This is an optional parameter. Disables the extension sent by messages originated by servers (ServerHello).	**Data Type**: String **Range**: NA **Default Value**: null

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`tlsNamedGroups`	This is an optional parameter. Provides a list of values sent in the supported_groups extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
`clientSignatureSchemes`	This is an optional parameter. Provides a list of values sent in the signature_algorithms extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
`service.ssl.tlsVersion`	This is a mandatory parameter. Indicates the TLS version.	**Data Type**: String **Range**: • TLSv1.2 , TLSv1.3 • TLSv1.2 • TLSv1.3 **Default Value**: TLSv1.2, TLSv1.3

`allowedCipherSuites`	This is an optional parameter.
	Indicates allowed Ciphers.
		Data Type: String
		Range: NA
		Default Values:
		`- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`
		`- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
		`- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256`
		`- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`
		`- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
		`- TLS_AES_256_GCM_SHA384`
		`- TLS_AES_128_GCM_SHA256`
		`- TLS_CHACHA20_POLY1305_SHA256`

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
cipherSuites	This is an optional parameter. Indicates supported cipher suites.	**Data Type**: String **Range**: NA **Default Values**: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 - TLS_CHACHA20_POLY1305_SHA256
healthCheckMonitoring.enabled	This is an optional parameter. Enables the support of health check API on the N32 Ingress gateway.	**Data Type**: Boolean **Range**: True or False **Default Value**: False
seppPeerHealthCheck	This is an optional parameter. Enables the health check monitoring feature on N32 Egress gateway.	**Data Type**: Boolean **Range**: True or False **Default Value**: False
seppPeerHealthCheckCodes	This is an optional parameter. Indicates the list of response codes that will be used to mark the peer as healthy.	**Data Type**: String **Range**: Valid Numerical code **Default Value**: 200, 204, 400, 401,403, 404, 501, and 503.
keybasedKafkaProducer	This is a mandatory parameter. This parameter when set to true, enables the functionality of message copy of same transaction into same Kafka partition.	**Data Type**: Boolean **Range**: True or False **Default Value**: False
podSecurityContext.runAsNonRoot	This is a mandatory parameter. Prevents pod from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
podSecurityContext.runAsUser	This is a mandatory parameter. Specifies that all processes in pod must run with the provided user ID.	Data Type: Integer Default Value: 10001

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`securityContext.enable`	This is a mandatory parameter. Enables security context for containers.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.readOnlyRootFilesystem`	This is a mandatory parameter. Mounts the mediation container's root filesystem as read-only.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.allowPrivilegeEscalation`	This is a mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the `no_new_privs` parameter gets configured on the container process. `allowPrivilegeEscalation` is always set to true when the container: • is run as privileged • has CAP_SYS_ADMIN	Data Type: Boolean Range: True or False Default Value: False
`containerSecurityContext.runAsNonRoot`	This is a mandatory parameter. Prevents containers from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
`containerSecurityContext.privileged`	This is a mandatory parameter. Provides containers' access to the host's resources and kernel capabilities.	Data Type: Boolean Range: True or False Default Value: False
`containerSecurityContext.runAsUser`	This is a mandatory parameter. Specifies that for any container in the pod, all processes must run with the provided user ID.	Data Type: Integer Range: Valid IDs for security context for user Default Value: 10001
`containerSecurityContext.capabilities.drop`	This is a mandatory parameter. Manages Linux capabilities for containers. Using Linux capabilities, you can grant certain privileges to a process without granting all the privileges of the root user.	Data Type: List of strings Range: Valid Linux capabilities Default Value: -all
`enablePodSecurityContext`	This is a mandatory parameter. Enables security context for pod.	Data Type: Boolean Range: True or False Default Value: True

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`egressRoutingMode`	This is a mandatory parameter. This parameter defines the routing mode (IPv4/IPv6) for the egress connections.	Data Type: String Range: IPv4, IPv6, IPv6_IPv4, and IPv4_IPv6. Default Value: In single stack mode, Default value: IPv4 In dual stack mode, Default value: IPv6_IPv4 (IPv6 preferred) Roaming Hub: Default value : IPv4 (do not change).
`checkAltRouteSvcReady`	This is a mandatory parameter. This parameter must be set to true if Alternate Route microservice is used for DNS SRV. If this flag is enabled, then Egress Gateway will be dependent on Alternate Route microservice to be up and running.	Data Type: Boolean Range: True or False Default Value: False
`tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`	This is a mandatory parameter. This parameter defines the supported TLS versions used by Gateway Services to communicate with the Kube-API-Server.	Data Type: String Range: TLS 1.2 and TLS 1.3 Default Value: TLS 1.3
`tlsVersionSupportForKubeApiServer.cipherSuites`	This is a mandatory parameter. This parameter indicates the Cipher suites that are compliant with the configured `tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion`	Data Type: String Range: NA Default Value: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CH ACHA20 _POLY1305_SHA 256
`tlsVersionSupportForKubeApiServer.featureSecrets`	This is an optional parameter. This parameter indicates the list of all the secrets that are used for all the features of Gateway Services. These secrets are volume mounted during the pod deployment.	Data Type: String Range: NA Default Value: • ocegress -secret1 • ocegress -secret2 • ocegress -secret3

Table 3-10 (Cont.) n32-egress-gateway

Name	Description	Details
`tlsVersionSupportForKubeApiServer.enabled`	This is an optional parameter. This parameter enables or disables TLS 1.3 support for establishing communication between Gateway Services and Kubernetes API server (Kube\u0002Api-Server). If this parameter is enabled, support for establishing communication with Kube\u0002Api-Server is provided through TLS 1.3, along with TLS 1.2 as configured in `kubeApiServerTlsVersion`. If this parameter is disabled, support for communication with Kube-Api-Server is provided only through TLS 1.2.	Data Type: Boolean Range: True or False Default Value: False

3.1.10 plmn-egress-gateway

This section includes information about the plmn-egress-gateway parameters of the SEPP.

Table 3-11 plmn-egress-gateway

Name	Description	Details
`cmName`	This is an optional parameter. Indicates the name of the configmap.	Data Type: String Range: NA Default Value: egressgateway
`serviceMeshCheck`	This is a mandatory parameter. Enabled when deployed in serviceMesh.	Data Type: Boolean Range: true or false Default Value: false
`istioSidecarQuitUrl`	This is a mandatory parameter. The sidecar (istio quit url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/quitquitquit Note: Port should be envoy admin port.
`istioSidecarReadyUrl`	This is a mandatory parameter. The sidecar (istio ready url)when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/ready Note: Port should be envoy admin port.
`global.k8sResources.hpat.supportedVersions`	Kubernetes resource	Data Type: String Range: NA Default Value: autoscaling/v1

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
`global.k8sResources.pdb.supportedVersions`	Kubernetes resource PDB supported version.	Data Type: String Range: NA Default Value: policy/v1
`global.logStorage`	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
`global.crictlStorage`	This is an optional parameter. Ephemeral storage configuration for log storage.	Data Type: Integer Range: NA Default Value: 32
`global.ephemeralStorageLimit`	This is an optional parameter. Ephemeral storage Limit.	Data Type: Integer Range: NA Default Value: 1024
`extraContainers`	This is a mandatory parameter. The attribute is used to control the usage of extra container(DEBUG tool). Allowed Values: DISABLED, ENABLED, USE_GLOBAL_VALUE If assigned with ENABLED or USE_GLOBAL_VALUE, then ensure "extraContainers Tpl" yaml chunk is defined at Service level or Global level in the parent chart based on the value assigned respectively.	Data Type: String Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
`prefix`	This is a mandatory parameter. When this parameter is set to specific value then that value will be used in the names of resources along with release name.	Data Type: String Range: NA Default Value: plmn
`routeConfigMode`	This is an optional parameter. Mode of route configuration for sbiRouting. Possible values are Helm, REST.	Data Type: String Range: Helm, REST Default Value: REST
`serviceEgressGateway.port`	This is a mandatory parameter. Indicates the Egress Gateway port.	Data Type: Integer Range: NA Default Value: 8080
`serviceEgressGateway.sslPort`	This is a mandatory parameter. SSL Port	Data Type: Integer Range: NA Default Value: 8442

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
`serviceEgressGateway.actuatorPort`	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It Cannot be same as service port.	Data Type: Integer Range: NA Default Value: 9094
`deploymentEgressGateway.image`	This is an optional parameter. Image name of ingress gateway	Data Type: String Range: NA Default Value: ocingress_gateway
`deploymentEgressGateway.imageTag`	This is an optional parameter. Image Tag name of ingress gateway.	Data Type: String Range: NA Default Value: helm-gateway-egress-tag
`deploymentEgressGateway.pullPolicy`	This is an optional parameter. Image Pull Policy	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`initContainersImage.name`	This is an optional parameter. Image name of initContainer	Data Type: String Range: NA Default Value: configurationinit
`initContainersImage.tag`	This is an optional parameter. Image tag name of initContainer	Data Type: String Range: NA Default Value: helm-gateway-egress-tag
`initContainersImage.pullPolicy`	This is an optional parameter. Image Pull Policy	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`updateContainersImage.name`	This is an optional parameter. Image name of updateContainer	Data Type: String Range: NA Default Value: configurationupdate
`updateContainersImage.tag`	This is an optional parameter. Image tag name of updateContainer	Data Type: String Range: NA Default Value: helm-gateway-egress-tag
`updateContainersImage.pullPolicy`	This is an optional parameter. Image Pull Policy	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`dbHookImage.name`	This is an optional parameter. Image name of dbHook	Data Type: String Range: NA Default Value: common_config_hook

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
`dbHookImage.tag`	This is an optional parameter. Image tag name of dbHook	Data Type: String Range: NA Default Value: helm-gateway-egress-tag
`dbHookImage.pullPolicy`	This is an optional parameter. Pull Policy of Image	Data Type: String Range: Always, IfNotPresent, Never Default Value: Always
`initssl`	This is an optional parameter. Enabling it generates key and trust store for https support	Data Type: Boolean Range: True or False Default Value: True **Note:** • The default value will be true, if the user wants to deploy in non ASM mode. • The default value will be false, if the user wants to deploy in ASM mode.
`enableIncomingHttp`	This is an optional parameter. Enabling it for incoming http request	Data Type: Boolean Range: True or False Default Value: true **Note:** This value must be set to true always.
`enableIncomingHttps`	This is an optional parameter. Enabling it for incoming https request	Data Type: Boolean Range: True or False Default Value: False **Note:** This value must be set to false always.
`enableOutgoingHttps`	This is an optional parameter. Enabling it for incoming https request	Data Type: Boolean Range: True or False Default Value: True **Note:** • The default value will be true, if the user wants to enable the outgoing request over HTTPs mode only. • The default value will be false, if the user wants to enable the outgoing request over HTTP mode. • For ASM mode, this value is set to false.

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
`httpsTargetOnly`	This is an optional parameter. This is global parameter which will be taken into consideration if route (under routeConfig section) based httpsTargetOnly parameter is not available. true: Select SbiRouting instances for https list only false: Run existing logic as per provided scheme. Note: double quotes to be enclosed for values of httpsTargetOnly.	Data Type: Boolean Range: True or False Default Value: false
`httpRuriOnly`	This is an optional parameter. Global parameter is taken into consideration if route (under routeConfig section) based httpRuriOnly parameter is not available. true: Means change Scheme of RURI to http false: Keep scheme as is.	Data Type: Boolean Range: True or False Default Value: false
`sbiRouting.sbiRoutingDefaultScheme`	This is an optional parameter. Default scheme applicable when3gpp-sbi-target apirootheader is missing	Data Type: String Range: NA Default Value: https
`sbiRouting.peerConfiguration[0].id`	This is a mandatory parameter. Peer identifier for the peer	Data Type: String Range: NA Default Value: peer1
`sbiRouting.peerConfiguration[0].host`	This is a mandatory parameter. First peer instance HTTP IP/ FQDN	Data Type: String Range: NA Default Value: <release-name>-plmn-ingress-gateway
`sbiRouting.peerConfiguration[0].port`	This is a mandatory parameter. First peer instance Port	Data Type: Integer Range: NA Default Value: 80
`sbiRouting.peerConfiguration[0].apiPrfix`	This is an optional parameter. First peer instance apiPrefix. Change this value to corresponding prefix if "/" is not expected to be provided. Applicable only for SCP with TLS enabled.	Data Type: String Range: NA Default Value: "/"
`sbiRouting.peerSetConfiguration[0].id[0]`	This is a mandatory parameter. (If route-level "metadata.sbiRoutingEnabled" flag is set to true) This is the peer set id that contains list of http and http instances.	Data Type: String Range: NA Default Value: set0

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
sbiRouting.peerSetConfiguration[0].id[0].httpConfiguration[0].priority	This is a mandatory parameter. (If route-level "metadata.sbiRoutingEnabled" flag is set to true) This denotes the priority of the http instance that request needs to be forwarded. Lower the priority, higher the preference.	Data Type: Integer Range: NA Default Value: 2
sbiRouting.peerSetConfiguration[0].id[0].httpConfiguration[0].peerIdentifier	This is a mandatory parameter. (If route-level "metadata.sbiRoutingEnabled" flag is set to true) This denotes the peer id that is present in the list of peers configured with unique ids.	Data Type: String Range: NA Default Value: peer1
headlessServiceEnabled	This is an optional parameter. Enabling this will make the service type default to ClusterIP.	Data Type: Boolean Range: True or False Default Value: false
log.level.root	This is an optional parameter. Log level for root logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.egress	This is an optional parameter. Log level for ingress logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: ERROR
log.level.oauth	This is an optional parameter. Log level for oauth logs.	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: WARN
log.level.updateContainer	This is an optional parameter. Log level for update container logs	Data Type: String Range: DEBUG/ INFO/ WARN/ ERROR Default Value: WARN
connectionTimeout	This is an optional parameter. Connection timeout in milliseconds	Data Type: Integer Range: NA Default Value: 2000
requestTimeout	This is an optional parameter. Request Timeout in milli seconds	Data Type: Integer Range: NA Default Value: 10000 #ms

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
gracefulCloseDelay	This is an mandatory parameter. gracefulCloseDelay value should be positive value greater than request Timeout and lesser than jettyIdleTimeout. If gracefulCloseDelay is set to 0 then default value of 30000 ms will be considered internally.	Data Type: Integer Range: NA Default Value: 30000 ms
service.ssl.privateKey.k8SecretName	This is a mandatory parameter. Name of the privatekey secret	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.privateKey.k8NameSpace	This is a mandatory parameter. Namespace of privatekey	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.privateKey.rsa.fileName	This is a mandatory parameter. rsa private key file name	Data Type: String Range: NA Default Value: rsa_private_key_pkcs1.pem
service.ssl.privateKey.ecdsa.fileName	This is a mandatory parameter. ecdsa private key file name	Data Type: String Range: NA Default Value: ssl_ecdsa_private_key.pem
service.ssl.certificate.k8SecretName	Name of the certificate secret	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.certificate.k8NameSpace	This is a mandatory parameter. Namespace of certificate	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.certificate.rsa.fileName	This is a mandatory parameter. rsa certificate key file name	Data Type: String Range: NA Default Value: ocsepp.cer
service.ssl.certificate.ecdsa.fileName	This is a mandatory parameter. ecdsa certificate key file name	Data Type: String Range: NA Default Value: ssl_ecdsa_certificate.crt
service.ssl.caBundle.k8SecretName	This is a mandatory parameter. Name of the caBundle secret	Data Type: String Range: NA Default Value: ocsepp-plmn-secret

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
service.ssl.caBundle.k8NameSpace	This is a mandatory parameter. Namespace of private	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.caBundle.fileName	This is a mandatory parameter. rsa private key file name	Data Type: String Range: NA Default Value: caroot.cer
service.ssl.keyStorePassword.k8SecretName	This is a mandatory parameter. Name of the privatekey secret	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.keyStorePassword.k8NameSpace	This is a mandatory parameter. Namespace of privatekey	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.keyStorePassword.fileName	This is a mandatory parameter. File name that has password for keyStore	Data Type: String Range: NA Default Value: key.txt
service.ssl.trustStorePassword.k8SecretName	This is a mandatory parameter. Name of the privatekey secret	Data Type: String Range: NA Default Value: ocsepp-plmn-secret
service.ssl.trustStorePassword.k8NameSpace	This is a mandatory parameter. Namespace of privatekey	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
service.ssl.trustStorePassword.fileName	This is a mandatory parameter. File name that has password for trustStore	Data Type: String Range: NA Default Value: trust.txt
service.ssl.initialAlgorithm	This is a mandatory parameter. Algorithm based on the certificate	Data Type: String Range: NA Default Value: RS256
service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to plmn-egw specific Service	Data Type: String Range: NA Default Value: { }
service.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to plmn-egw specific Services	Data Type: String Range: NA Default Value: { }

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
`deployment.customExtension.labels`	This is an optional parameter. Custom Labels that needs to be added to plmn-egw specific deployment	Data Type: String Range: NA Default Value: { }
`deployment.customExtension.annotations`	This is an optional parameter. Custom Annotations that needs to be added to plmn-egw specific deployment	Data Type: String Range: NA Default Value: { }
`deDupeResponseHeader`	This is an optional parameter. it is used for handling duplicate values in response headers. Multiple values can be provided with space. # Ex: content-type nettylatency requestmethod, RETAIN_LAST	Data Type: String Range: NA Default Value: content-type, RETAIN_LAST
`commonCfgClient.enabled`	This is an optional parameter. Set it to true if persistent configuration needs to be enabled.	Data Type: Boolean Range: true or false Default Value: true
`commonCfgServer.configServerSvcName`	This is a mandatory parameter if commonCfgClient. enabled is set to true Service name of common configuration service to which the client tries to poll for configuration updates	Data Type: String Range: NA Default Value: config-mgr-svc
`commonCfgServer.host`	This is an optional parameter. No (It is needed if commonCfgServer.configServerSvcName is not available) Host name of Common configuration server to which client tries to poll for configuration updates. This value is picked up if commonCfgServer .configServer SvcName is not available	Data Type: String Range: NA Default Value: config-mgr-svc
`commonCfgServer.port`	This is a mandatory parameter if commonCfgClient. enabled is set to true Port of Common Configurationserver	Data Type: Integer Range: NA Default Value: 9090
`commonCfgServer.pollingInterval`	This is a mandatory parameter if commonCfgClient. enabled is set to true This is the interval between two subsequent polling requests from config client toserver	Data Type: Integer Range: NA Default Value: 5000

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
commonServiceName	This is a Mandatory parameter if commonCfgClient.enabled is set to true. This is the common service name that is currently requesting for configuration updates from server	Data Type: String Range: NA Default Value: egw
enableSecondaryInstance	To enable secondary instance of config client enableSecondaryInstance must beset to true.	Data Type: Boolean Range: NA Default Value: false
ingressServiceName	IngressServiceName must be set with the value of commonServiceName present in ingress values.yaml.	Data Type: string Range: NA Default Value: igw
ingressReleaseVersion	IngressReleaseVersion must be same as version in Chart.yaml of IngressGateway.	Data Type: String Range: NA Default Value: helm-gateway-ingress-tag
restoreBackupOnInstall	This is an optional parameter. This flag when enabled picks up the data from the backup table during installation of gateway	Data Type: Boolean Range: true or false Default Value: false
dbConfig.dbHost	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Hostname of Mysql in which the configuration must be stored	Data Type: String Range: NA Default Value: sepp-mysql-svc
dbConfig.dbPort	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Port of mysql	Data Type: Integer Range: NA Default Value: 3306
dbConfig.configFile	This is a mandatory parameter. (if commonCfgClient enabled is set to true) File name for initial configuration that must be stored in the db	Data Type: String Range: NA Default Value: defaultconfig.yaml
dbConfig.schemaFile	This is a mandatory parameter. (if commonCfgClient enabled is set to true) File name for json schema validation	Data Type: String Range: NA Default Value: defaultschema.json
dbConfig.secretName	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Secret name from which the db name, db password and db user name is picked	Data Type: String Range: NA Default Value: ocsepp-mysql-cred

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
dbConfig.dbName	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Database name	Data Type: String Range: NA Default Value: seppdb
dbConfig.dbUNameLiteral	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Name of the Key configured for "DB Username" in Secret with following name: "<dbConfig.secretName>"	Data Type: String Range: NA Default Value: mysql-username
dbConfig.dbPwdLiteral	This is a mandatory parameter. (if commonCfgClient enabled is set to true) Name of the Key configured for "DB Password" in Secret with following name: "<dbConfig.secretName>"	Data Type: String Range: NA Default Value: mysql-password
dbConfig.dbEngine	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
globalretry.enabled	This is an optional parameter Can be set to true if Scp re-route feature (scpRerouteEnabled) is enabled.	Data Type: Boolean Range: true or false Default Value: false
globalretry.retries	This is a mandatory parameter if, "routesConfig[0].filterName2 .retries" is not defined Number of reroute to be attempted to alternate SCP instances and this property will be considered in the absence of "routesConfig[0].filterName2.retries" attribute at route level.	Data Type: Interger Range: NA Default Value: 2
routesConfig[0].id	This is a mandatory parameter. id of the route. Multiple routes can be configured in a similar way.	Data Type: Interger Range: NA Default Value: scp_via_proxy

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
routesConfig[0].uri	This is a mandatory parameter. Provide any dummy url, existing url can also left with existing value. Please note provided sample url does not make any impact (http or https) as url's will be constructed in the code.	Data Type: String Range: NA Default Value: http://request.uri
routesConfig[0].path	This is a mandatory parameter. Provide the path to be matched.	Data Type: String Range: NA Default Value: /**
routesConfig[0].order	This is a mandatory parameter. Provide the order of the execution of this route.	Data Type: Integer Range: NA Default Value: 1
routesConfig[0].metadata.httpRuriOnly	This is an optional parameter Provide true or false enclosed with double quotes. If "true" then change scheme of RURI to http , "false" then keep scheme as is.	Data Type: Boolean Range: true or false Default Value: false
routesConfig[0].metadata.httpsTargetOnly	This is an optional parameter Provide true or false enclosed with double quotes. If "true" then select SBI instances for https list only (if 3gpp sbi target root header is http), if "false" then run existing logic as per the provided scheme.	Data Type: Boolean Range: true or false Default Value: false
routesConfig[0].metadata.sbiRoutingEnabled	This is an optional parameter true: SbiRouting functionality is enabled false: SbiRouting functionality is disabled	Data Type: Boolean Range: true or false Default Value: false
routesConfig[0].filterName1.name	This is a mandatory parameter if routesConfig[0].metadata.sbiRoutingEnabled is true Provide filtername as "SBIRoutingFilter" If FilterName1 is not provided then it would be considered as direct Egress Gateway path and configured accordingly during deployment.	Data Type: String Range: NA Default Value: "SBIRoutingFilter"
routesConfig[0].filterName1.args.peerSetIdentifier	This is a mandatory parameter if routesConfig[0].metadata.sbiRoutingEnabled is true This flag maps to id of peerSetConfiguration	Data Type: String Range: NA Default Value: set0

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
routesConfig[0].filterName1.args.customPeerSelectorEnabled	This is an optional parameter This flag allows the user to send request to a particular instance directly when enabled according to "ocalternaterouteattempt" header	Data Type: Boolean Range: true or false Default Value: false
routesConfig[0].removeRequestHeader[0].name	This is an optional parameter This field is used for removing a request header at route level. Additional header can be configured by adding a new element in the next line and so on. The value of "name" attribute denotes the name of the request header which is to be removed at route level. Add a new entry in next line for every header to be removed.	Data Type: String Range: NA Default Value: NA
routesConfig[0].removeResponseHeader[0]0.name	This is an optional parameter This field is used for removing a responseheader at route level. Additional header can be configured by adding a new element in the next line and so on. The value of "name" attribute denotes the name of the request header which is to be removed at route level. Add a new entry in next line for every header to be removed.	Data Type: String Range: NA Default Value: NA
dnsSrv.host	This is a mandatory parameter, If DnsSrv integration is required, else optional Host of DNS Alternate Route Service	Data Type: String Range: NA Default Value: NA

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
dnsSrv.alternateRouteSvcName	This is a mandatory parameter, if DnsSrv integration is required and Service Name is expected to be provided otherwise optional Service name of Alternate Route Service. If Service name is provided , then this parameter would be picked for integrating Egress Gateway with alternate route service. If IP or Fqdn is expected to be provided then update this parameter as blank and update above parameter accordingly. If this parameter is populated with data then above parameter would be ignored.	Data Type: String Range: NA Default Value: alternate-route
dnsSrv.port	This is a mandatory parameter, If DnsSrv integration is required, else optional. Port of DNS Alternate Route Service.	Data Type: Integer Range: NA Default Value: 80
dnsSrv.scheme	This is a mandatory parameter, If DnsSrv integration is required, else optional. Scheme of request that need to be sent to alternate route service. By default it is http. Just gave configurable privilege for future.	Data Type: String Range: NA Default Value: http
dnsSrv.connectTimeout	This is a mandatory parameter, If DnsSrv integration is required, else optional. Duration for Egress Gateway to Alternate Route Service DNS SRV connection timeout.	Data Type: Integer Range: NA Default Value: 10000
dnsSrv.requestTimeout	This is a mandatory parameter, If DnsSrv integration is required, else optional. Duration for Egress Gateway to Alternate Route Service DNS SRV request query execution.	Data Type: Integer Range: NA Default Value: 1000

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
dnsSrv.fqdnSchemesForProbing	This is a mandatory parameter. • Probing is executed as part of the container probe. An empty list indicates no probing. • Probing sends or looks up requests to DNS SRV host for the configured FQDN and scheme. • Probing is done sequentially for FQDN scheme combination, adjust container probe time based on the number of FQDNs.	Data Type: string Range: NA Default Value: []
dnsSrv.backoffDelay	This is a mandatory parameter. BackoffDelay is used for backoff during DNS SRV failures.	Data Type: Integer Range: NA Default Value: 5000
dnsSrv.errorCodeOnDNSResolutionFailure	This is a mandatory parameter, If DnsSrv integration is required, else optional. Currently, this value cannot be modified.	Data Type: Integer Range: NA Default Value: 425
dnsSrv.errorDescriptionOnDNSResolutionFailure	This is an optional parameter. Error Description for DNS resolution failure. Populated in ProblemDetails response in ProblemDetails.detail section. Currently, this value cannot be modified.	Data Type: String Range: NA Default Value: ""
dnsSrv.errorTitleOnDNSResolutionFailure	This is an optional parameter. Error title for DNS resolution failure. Populated in ProblemDetails response in ProblemDetails.title section. Currently, this value cannot be modified.	Data Type: String Range: NA Default Value: ""
dnsSrv.errorCauseOnDNSResolutionFailure	This is an optional parameter. Error cause for DNS resolution failure. Populated in ProblemDetails response in ProblemDetails.cause section. Currently, this value cannot be modified.	Data Type: String Range: NA Default Value: ""
dnsRefreshDelay	This is an optional parameter. Dns Refresh Delay in milli-seconds	Data Type: Integer Range: NA Default Value: 10000
resources.limits.cpu	This is an optional parameter. CPU Limit	Data Type: Integer Range: NA Default Value: 5

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
resources.limits.initServiceCpu	This is an optional parameter. Init Container CPU Limit	Data Type: Float Range: NA Default Value: 1
resources.limits.updateServiceCpu	This is an optional parameter. Update Container CPU Limit	Data Type: Float Range: NA Default Value: 1
resources.limits.memory	This is an optional parameter. Memory Limit	Data Type: String Range: NA Default Value: 5Gi
resources.limits.updateServiceMemory	This is an optional parameter. Update Container Memory Limit	Data Type: String Range: NA Default Value: 1Gi
resources.limits.initServiceMemory	This is an optional parameter. int Container Memory Limit	Data Type: String Range: NA Default Value: 1Gi
resources.requests.cpu	This is an optional parameter. CPU for requests	Data Type: Integer Range: NA Default Value: 1
resources.requests.initServiceCpu	This is an optional parameter. Init Container CPU for requests	Data Type: Integer Range: NA Default Value: 1
resources.requests.updateServiceCpu	This is an optional parameter. Update Container CPU for requests	Data Type: Integer Range: NA Default Value: 1
resources.requests.memory	This is an optional parameter. Memory for requests	Data Type: String Range: NA Default Value: 5Gi
resources.requests.updateServiceMemory	This is an optional parameter. Update Container Memory for requests	Data Type: String Range: NA Default Value: 1Gi
resources.requests.initServiceMemory	This is an optional parameter. Init Container Memory for requests	Data Type: String Range: NA Default Value: 1Gi

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
`resources.target.averageCpuUtil`	This is an optional parameter. Resource Requirements(avg cpu utilisation)	Data Type: Integer Range: NA Default Value: 70
`maxUnavailable`	Number of Pods that will be unavailable during a disruption	Data Type: String Range: NA Default Value: 25%
`minReplicas`	This is an optional parameter. Min replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
`maxReplicas`	This is an optional parameter. Max replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 10
`gracefulShutdown.gracePeriod`	This is an optional parameter. Grace period to wait for active requests to be executed. If there are no active requests then this period is neglected. 's' in case of seconds and 'm' in case of minutes	Data Type: String Range: NA Default Value: 1m
`gracefulShutdown.defaultErrorCode`	This is a optional parameter Default error code returned at the time of Graceful shut down	Data Type: Integer Range: NA Default Value: 500
`gracefulShutdown.errorDescription`	This is an optional parameter. Graceful shut down Error description	Data Type: String Range: NA Default Value: Shutdown in progress
`gracefulShutdown.errorTitle`	This is an optional parameter. Graceful shut down error title	Data Type: String Range: NA Default Value: Graceful shutdown
`gracefulShutdown.errorCause`	This is an optional parameter. Graceful shut down error cause	Data Type: String Range: NA Default Value: Shutdown
`egressRateLimiting.enabled`	This is a mandatory parameter. This parameter enables Global Rate Limiting on Gateway.	Data Type: boolean Range: True or False Default Value: false

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
egressRateLimiting.duration	This is a mandatory parameter. This parameter defines theduration to decide how frequently to refill(in seconds)	Data Type: Integer Range: NA Default Value: 1
egressRateLimiting.bucketCapacity	This is a mandatory parameter. This parameter defines the Bucket size in which capacity to handle traffic burst is defined.	Data Type: Integer Range: NA Default Value: 7500
egressRateLimiting.refillRate	This is a mandatory parameter. This parameter defines the number of tokens to be added to refill the bucket	Data Type: Integer Range: NA Default Value: 7500
egressRateLimiting.errorCodeOnRateLimit	This is a mandatory parameter. This parameter defines the configurable error code to be returned	Data Type: Integer Range: NA Default Value: 429
nettyIdleTimeout	This is an optional parameter. Netty Idle Timeout in milli seconds	Data Type: Integer Range: NA Default Value: 120000
nfFqdn	This is a mandatory parameter. NF FQDN	Data Type: Integer Range: NA Default Value: sepp2.inter.oracle.com
jaegerTracingEnabled	This is an optional parameter. Enable jaeger tracing	Data Type: Boolean Range: True or False Default Value: false
openTracing.jaeger.udpSender.host	This is an optional parameter. Jaeger Host	Data Type: String Range: NA Default Value: occne-tracer-jaeger-agent.occne-infra
openTracing.jaeger.udpSender.port	This is an optional parameter. Jaeger Port	Data Type: Integer Range: NA Default Value: 6831
openTracing.jaeger.probabilisticSampler	This is an optional parameter. Trace capture in percentage	Data Type: Float Range: NA Default Value: 0.5
messageCopy.enabled	This is an optional parameter. This parameter enables or disables the Message feed feature at the Ingress Gateway.	Data Type: Boolean Range: True or False Default Value: False

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
messageCopy.copyPayload	This is an optional parameter. This parameter specifies whether to copy the message payload in the feed towards Data Director or not. true: the complete payload message is copied. false: Only the header information is copied.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.topicName	This is an optional parameter. Name of the topic to which Ingress Gateway send the payloads.	Data Type: String Range: NA Default Value: message.copy
messageCopy.ackRequired	This is a mandatory parameter. This parameter specifies if we wait for any acknowledgement from DD.	Data Type: Boolean Range: True or False Default Value: False
messageCopy.retryOnFailure	This is a mandatory parameter. This parameter specifies how many times SEPP should retry if message was not sent to DD successfully.	Data Type: Integer Range: NA Default Value: 0
messageCopy.threadPoolConfigurations.coreSize	This is an optional parameter. core Size for thread pool configuration for message feed thread For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8
messageCopy.threadPoolConfigurations.maxSize	This is an optional parameter. max Size for thread pool configuration for message feed thread For performance enhancement, set the value as16.	Data Type: Integer Range: NA Default Value: 8
messageCopy.threadPoolConfigurations.queueCapacity	This is an optional parameter. queue capacity for thread pool configuration message feed thread For performance enhancement, set the value as 3000.	Data Type: Integer Range: NA Default Value: 1000
messageCopy.security.enabled	This is a mandatory parameter. Security mode enabled for message feed feature	Data Type: Boolean Range: True or False Default Value: False
messageCopy.security.protocol	This is a conditional parameter. It is used for message feed feature when security is enabled between SEPP and Gateway.	Data Type: String Range: SASL_SSL or SSL Default Value: SASL_SSL

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
messageCopy.security.tlsVersion	This is a mandatory parameter. TLS version details.	Data Type: String Range: TLSv1.2, TLSv1.3 Default Value: TLSv1.3
kafka.bootstrapAddress	This is an conditional parameter. List of comma- separated Kafka Nodes (to which messages should be copied if messageCopy feature is enabled).	Data Type: String Range: NA Default Value: <kafka-broker>:<port> Port = 9093 for SSL protocol Port = 9094 for SASL_SSL protocol
messageCopy.security.saslConfiguration.username	This is a mandatory parameter. username for DD Refer to DD guide for more details	Data Type: String Range: NA Default Value: test
messageCopy.security.saslConfiguration.password.k8SecretName	This is a mandatory parameter. Secret name for gateway on which feature enabled	Data Type: String Range: ocsepp-plmn-secret for PLMN Gateways and ocsepp-n32-secret for N32 Gateways Default Value: message-copy-secret
messageCopy.security.saslConfiguration.password.k8NameSpace	This is a mandatory parameter. Namespace where DD deployed Please refer to DD guide for more details	Data Type: String Range: NA Default Value: ocegress
messageCopy.security.saslConfiguration.password.fileName	This is a mandatory parameter. File used to create DD secrets Please refer to DD guide for more details	Data Type: String Range: NA Default Value: password.txt
kafka.bootstrap-servers	This is an conditional parameter. List of comma-separated DD Nodes IP address The port will change to 9092 if security is disabled	Data Type: String Range: NA Default Value: Default Value: <kafka-broker>:<port> Port = 9093 for SSL protocol Port = 9094 for SASL_SSL protocol
configureDefaultRoute	This is a mandatory parameter. This parameter is used to configure default route in the plmn-egress-gateway for direct routing.	Data Type: Boolean Range: True or False Default Value: True
sbiRoutingConfigMode	This is a mandatory parameter. This parameter is used to enable or disable the egress rate limiting per egress rate limiting list on Ingress Gateway	Data Type: String Default Value: REST

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
routeConfigMode	This is a mandatory parameter. This parameter is used to configure in which all the routes should be operated.	Data Type: String Default Value: REST
clientDisabledExtension	This is an optional parameter. Disables the extension sent by messages originated by clients (ClientHello).	**Data Type**: String **Range**: NA **Default Value**: ec_point_formats
serverDisabledExtension	This is an optional parameter. Disables the extension sent by messages originated by servers (ServerHello).	**Data Type**: String **Range**: NA **Default Value**: null
tlsNamedGroups	This is an optional parameter. Provides a list of values sent in the supported_groups extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
clientSignatureSchemes	This is an optional parameter. Provides a list of values sent in the signature_algorithms extension. These are comma-separated values.	**Data Type**: String **Range**: NA **Default Value**: null
service.ssl.tlsVersion	This is a mandatory parameter. Indicates the TLS version.	**Data Type**: String **Range**: • TLSv1.2 , TLSv1.3 • TLSv1.2 • TLSv1.3 **Default Value**: TLSv1.2, TLSv1.3
allowedCipherSuites	This is an optional parameter. Indicates allowed Ciphers.	**Data Type**: String **Range**: NA **Default Values**: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 - TLS_CHACHA20_POLY1305_SHA256

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
cipherSuites	This is an optional parameter. Indicates supported cipher suites.	**Data Type**: String **Range**: NA **Default Values**: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS_AES_128_GCM_SHA256 - TLS_CHACHA20_POLY1305_SHA256
defaultRouteRetryProfile	This is an optional parameter. This parameter is used for enabling default retry feature.	Data Type: Boolean Range: True or False Default Value: False
keybasedKafkaProducer	This is a mandatory parameter. This parameter when set to true, enables the functionality of message copy of same transaction into same Kafka partition.	**Data Type**: Boolean **Range**: True or False **Default Value**: False
podSecurityContext.runAsNonRoot	This is a mandatory parameter. Prevents pod from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
podSecurityContext.runAsUser	This is a mandatory parameter. Specifies that all processes in pod must run with the provided user ID.	Data Type: Integer Default Value: 10001
securityContext.enable	This is a mandatory parameter. Enables security context for containers.	Data Type: Boolean Range: True or False Default Value: True
containerSecurityContext.readOnlyRootFilesystem	This is a mandatory parameter. Mounts the mediation container's root filesystem as read-only.	Data Type: Boolean Range: True or False Default Value: True

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
containerSecurityContext.allowPrivilegeEscalation	This is a mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the no_new_privs parameter gets configured on the container process. allowPrivilegeEscalation is always set to true when the container: • is run as privileged • has CAP_SYS_ADMIN	Data Type: Boolean Range: True or False Default Value: False
containerSecurityContext.runAsNonRoot	This is a mandatory parameter. Prevents containers from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
containerSecurityContext.privileged	This is a mandatory parameter. Provides containers' access to the host's resources and kernel capabilities.	Data Type: Boolean Range: True or False Default Value: False
containerSecurityContext.runAsUser	This is a mandatory parameter. Specifies that for any container in the pod, all processes must run with the provided user ID.	Data Type: Integer Range: Valid IDs for security context for user Default Value: 10001
containerSecurityContext.capabilities.drop	This is a mandatory parameter. Manages Linux capabilities for containers. Using Linux capabilities, you can grant certain privileges to a process without granting all the privileges of the root user.	Data Type: List of strings Range: Valid Linux capabilities Default Value: -all
enablePodSecurityContext	This is a mandatory parameter. Enables security context for pod.	Data Type: Boolean Range: True or False Default Value: True
egressRoutingMode	This is a mandatory parameter. This parameter defines the routing mode (IPv4/IPv6) for the egress connections.	Data Type: String Range: IPv4, IPv6, IPv6_IPv4, and IPv4_IPv6 Default Value: SEPP/Roaming Hub: In single stack mode, Default value: IPv4 In dual stack mode, Default value : IPv6_IPv4 (IPv6 preferred)

Table 3-11 (Cont.) plmn-egress-gateway

Name	Description	Details
checkAltRouteSvcReady	This is a mandatory parameter. This parameter must be set to true if Alternate Route microservice is used for DNS SRV. If this flag is enabled, then Egress Gateway will be dependent on Alternate Route microservice to be up and running.	Data Type: Boolean Range: True or False Default Value: False
tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion	This is a mandatory parameter. This parameter defines the supported TLS versions used by Gateway Services to communicate with the Kube-API-Server.	Data Type: String Range: TLS 1.2 and TLS 1.3 Default Value: TLS 1.3
tlsVersionSupportForKubeApiServer.cipherSuites	This is a mandatory parameter. This parameter indicates the Cipher suites that are compliant with the configured tlsVersionSupportForKubeApiServer.kubeApiServerTlsVersion	Data Type: String Range: NA Default Value: • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CH ACHA20 _POLY1305_SHA 256
tlsVersionSupportForKubeApiServer.featureSecrets	This is an optional parameter. This parameter indicates the list of all the secrets that are used for all the features of Gateway Services. These secrets are volume mounted during the pod deployment.	Data Type: String Range: NA Default Value: • ocegress -secret1 • ocegress -secret2 • ocegress -secret3
tlsVersionSupportForKubeApiServer.enabled	This is an optional parameter. This parameter enables or disables TLS 1.3 support for establishing communication between Gateway Services and Kubernetes API server (Kube\u0002Api-Server). If this parameter is enabled, support for establishing communication with Kube\u0002Api-Server is provided through TLS 1.3, along with TLS 1.2 as configured in kubeApiServerTlsVersion. If this parameter is disabled, support for communication with Kube-Api-Server is provided only through TLS 1.2.	Data Type: Boolean Range: True or False Default Value: False

3.1.11 nrf-client

This section includes information about the nrf-client parameters of the SEPP.

Table 3-12 nrf-client

Name	Description	Details
nrfclient.nrf-client.configmapApplicationConfig.profile	This is a mandatory parameter. It contains configuration parameters that goes into nrf-client's config map. Note: See configmap table for configurable parameters	Data Type: String Range: NA Default Value: [appcfg] primaryNrfApiRoot= ocnrf-ingressgateway:80 nrfScheme=http retryAfterTime=PT120S nrfClientType=SEPP nrfClientSubscribeTypes= appProfiles= [{"nfInstanceId":"9faf1b bc-6e4a-4454-a507- aef01a101a06","nfType":" SEPP","nfStatus":"REGIST ERED","fqdn":"ocsepp- plmn-ingress- gateway.DEPLOYMENT_NAMES PACE","plmnList": [{"mcc": "333","mnc": "222"},{"mcc": "444","mnc": "555"}, {"mcc":"444","mnc":"55"}],"capacity":500,"locali ty":"delhi","priority":1 ,"nfSetIdList": ["set001.seppset.5gc.mnc 444.mcc555","set001.sepp set.5gc.mnc222.mcc333"]}] registrationRetryInterva l=5000 subscriptionRetryInterva l=5000 discoveryRetryInterval=5 000 renewalTimeBeforeExpiry= 3600 validityTime=30 enableSubscriptionAutoRe newal=true nfHeartbeatRate=80 acceptAdditionalAttribut es=false retryForCongestion=5 supportedDataSetId=

Table 3-13 nrf-client-nfdiscovery

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfdiscovery.extraContainers	This is an optional parameter. This attribute is used to control the usage of extra container when DEBUG tool is ENABLED.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
nrfclient.nrf-client.nrf-client-nfdiscovery.image	This is a mandatory parameter. NRF Client Microservice image name	Data Type: String Range: NA Default Value: nrf-client
nrfclient.nrf-client.nrf-client-nfdiscovery.imageTag	This is a mandatory parameter. NRF Client Microservice image tag	Data Type: String Range: NA Default Value: helm_nrfclient_tag
nrfclient.nrf-client.nrf-client-nfdiscovery.extraContainers	This is an optional parameter. This attribute is used to control the usage of extra container when DEBUG tool is ENABLED.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
nrfclient.nrf-client.nrf-client-nfdiscovery.dbHookImage.name	This is a mandatory parameter. Image name of dbHook	Data Type: String Range: NA Default Value: common_config_hook
nrfclient.nrf-client.nrf-client-nfdiscovery.dbHookImage.tag	This is a mandatory parameter. Image tag name of dbHook	Data Type: String Range: NA Default Value: helm_nrf_client_db_hook_tag
nrfclient.nrf-client.nrf-client-nfdiscovery.dbHookImage.pullPolicy	This is a mandatory parameter. Indicates if the image needs to be pulled or not	Data Type: ENUM Range: Always, IfNotPresent, Never Default Value: IfNotPresent
nrfclient.nrf-client.nrf-client-nfdiscovery.global.logStorage	This is an optional parameter. Log storage for ephemeral storage request	Data Type: Integer Range: NA Default Value: 32
nrfclient.nrf-client.nrf-client-nfdiscovery.global.crictlStorage	This is an optional parameter. Critical storage for ephemeral storage request	Data Type: Integer Range: NA Default Value: 32
nrfclient.nrf-client.nrf-client-nfdiscovery.global.ephemeralStorageLimit	This is an optional parameter. Ephemeral storage allocation limits	Data Type: Integer Range: NA Default Value: 1024
nrfclient.nrf-client.nrf-client-nfdiscovery.envJaegerSamplerParam	This is an Conditional Parameter. Note: You must customize this parameter only when NRF client services are enabled. Trace capture in percentage	Data Type: Integer Range: NA Default Value: '1'

Table 3-13 (Cont.) nrf-client-nfdiscovery

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfdiscovery.envJaegerSamplerType	This is an Conditional Parameter. Note: You must customize this parameter only when NRF client services are enabled. Trace Sampler type	Data Type: String Range: NA Default Value: ratelimiting
nrfclient.nrf-client.nrf-client-nfdiscovery.envJaegerServiceName	This is an Conditional Parameter. Note: You must customize this parameter only when NRF client services are enabled. Jaeger Service Name	Data Type: String Range: NA Default Value: nrf-client-nfdiscovery
nrfclient.nrf-client.nrf-client-nfdiscovery.cpuRequest	This is a mandatory parameter. Maximum cpu limit to which it can be requested	Data Type: Integer Range: NA Default Value: 1
nrfclient.nrf-client.nrf-client-nfdiscovery.cpuLimit	This is a mandatory parameter. Maximum CPU limit for nrf-client discovery service.	Data Type: Integer Range: NA Default Value: 1
nrfclient.nrf-client.nrf-client-nfdiscovery.memoryRequest	This is a mandatory parameter. Amount of memory requested.	Data Type: String Range: NA Default Value: 2Gi
nrfclient.nrf-client.nrf-client-nfdiscovery.memoryLimit	This is a mandatory parameter. Memory limit for nrf-client discovery service.	Data Type: String Range: NA Default Value: 2Gi
nrfclient.nrf-client.nrf-client-nfdiscovery.minReplicas	This is a mandatory parameter. Min replicas to scale to maintain an average CPU utilisation.	Data Type: Integer Range: NA Default Value: 2
nrfclient.nrf-client.nrf-client-nfdiscovery.maxReplicas	This is a mandatory parameter. Max replicas to scale to maintain an average CPU utilisation.	Data Type: Integer Range: NA Default Value: 2
nrfclient.nrf-client.nrf-client-nfdiscovery.averageCpuUtil	This is a mandatory parameter. CPU utilisation limit for autoscaling (creating HPA).	Data Type: Integer Range: NA Default Value: 70
nrfclient.nrf-client.nrf-client-nfdiscovery.upgradeStrategy	This is a mandatory parameter. This parameter indicates the update strategy used in nrf-client discovery service.	Data Type: String Range: NA Default Value: RollingUpdate
nrfclient.nrf-client.nrf-client-nfdiscovery.maxUnavailable	This is an optional parameter. Number of replicas that can go down during a disruption.	Data Type: String Range: NA Default Value: 25%
nrfclient.nrf-client.nrf-client-nfdiscovery.cacheDiscoveryResults	This is a mandatory parameter. Set to true if the discovery results should be cached.	Data Type: Boolean Range: NA Default Value: false
nrfclient.nrf-client.nrf-client-nfdiscovery.envDiscoveryServicePort	This is a mandatory parameter. Discovery Service Port used for subscribing to management Service.	Data Type: Integer Range: NA Default Value: 5910

Table 3-13 (Cont.) nrf-client-nfdiscovery

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfdiscovery.envManagementServicePort	This is a mandatory parameter. Management Service Port used to send subscriptions to the Management Service.	Data Type: Integer Range: NA Default Value: 5910
nrfclient.nrf-client.nrf-client-nfdiscovery.istioExcludePorts	Ports to be added in the "excludeInboundPort" and "excludeOutboundPort" ports in ASM. Add actuator prometheus here for oso read of metrics as comma separated values.	Data Type: Integer Range: NA Default Value: 53
nrfclient.nrf-client.nrf-client-nfdiscovery.hookRestartPolicy	This is a mandatory parameter. Restart Policy for hooks	Data Type: String Range: NA Default Value: Never
nrfclient.nrf-client.nrf-client-nfdiscovery.metricPrefix	This is an optional parameter. A prefix that shall be added to all the metric names.By default, this shall contain the value configured in the global section metricPrefix.	Data Type: String Range: NA Default Value: ""
nrfclient.nrf-client.nrf-client-nfdiscovery.metricSuffix	This is an optional parameter. A suffix that shall be added to all the metric names.By default, this shall contain the value configured in the global section metricSuffix.	Data Type: String Range: NA Default Value: ""
nrfclient.nrf-client.nrf-client-nfdiscovery.istioSidecarQuitUrl	This is an conditional parameter. The sidecar (istio quit url) when deployed in serviceMesh. This value shall be considered only when serviceMeshCheck is true.	Data Type: String Range: NA Default Value: http://127.0.0.1:15000/quitquitquit
nrfclient.nrf-client.nrf-client-nfdiscovery.istioSidecarReadyUrl	This is an conditional parameter. The sidecar (istio ready url) when deployed in serviceMesh. This value shall be considered only when serviceMeshCheck is true.	Data Type: String Range: NA Default Value: http://127.0.0.1:15000/ready
nrfclient.nrf-client.nrf-client-nfdiscovery.serviceMeshCheck	This is an optional parameter. Flag to enable aspen service mesh.	Data Type: String Range: NA Default Value: false
nrfclient.nrf-client.nrf-client-nfdiscovery.nfProfileConfigMode	This is an optional parameter. Flag to switch between "HELM" based or "REST" based nfProfile configuration.	Data Type: String Range: NA Default Value: HELM
nrfclient.nrf-client.nrf-client-nfdiscovery.commonCfgClient.enabled	This is an optional parameter. Flag to enable/disable dynamic logging using common configuration service.	Data Type: Boolean Range: True or False Default Value: true

Table 3-13 (Cont.) nrf-client-nfdiscovery

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfdiscovery.commonCfgServer.configServerSvcName	This is an optional parameter. Service name of common configuration service to which the client tries to poll for configuration updates.	Data Type: String Range: NA Default Value: 'config-mgr-svc'
nrfclient.nrf-client.nrf-client-nfdiscovery.commonCfgServer.host	This is an optional parameter. The Host name of the Nf Configuration Service name or the common config service.This attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: 'config-mgr-svc'
nrfclient.nrf-client.nrf-client-nfdiscovery.commonCfgServer.port	This is an optional parameter. The port of the Nf Configuration Service name or the common config service.This attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: 9090
nrfclient.nrf-client.nrf-client-nfdiscovery.commonCfgServer.pollingInterval	This is an optional parameter. The interval at which the discovery service shall poll the configuration service to check for updates in msThis attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: Integer Range: NA Default Value: 5000
nrfclient.nrf-client.nrf-client-nfdiscovery.dbConfig.dbHost	This is a mandatory parameter. Specifies the Hostname of MySQL that is used to store configurations.	Data Type: String Range: NA Default Value: sepp-mysql-svc
nrfclient.nrf-client.nrf-client-nfdiscovery.dbConfig.dbPort	This is a mandatory parameter. Specifies the port number of MySQL.	Data Type: String Range: NA Default Value: 3306
nrfclient.nrf-client.nrf-client-nfdiscovery.dbConfig.secretName	This is a mandatory parameter. The database secretThis attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
nrfclient.nrf-client.nrf-client-nfdiscovery.dbConfig.dbName	This is a mandatory parameter. The database name which will be used to store the common configuraiton. This attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: seppdb

Table 3-13 (Cont.) nrf-client-nfdiscovery

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfdiscovery.dbConfig.dbUNameLiteral	This is a mandatory parameter. The db literal name that shall be used as per the secrets configured.This attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: mysql-username
nrfclient.nrf-client.nrf-client-nfdiscovery.dbConfig.dbPwdLiteral	This is a mandatory parameter. The db password literal name that shall be used as per the secrets configured. This attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: mysql-password
nrfclient.nrf-client.nrf-client-nfdiscovery.dbConfig.dbEngine	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
nrf-client-nfdiscovery.startupProbe.initialDelaySeconds	This is a mandatory parameter.Tells the kubelet that it should wait second before performing the first probe	Data Type: Integer Range: NA Default Value: 30
nrf-client-nfdiscovery.startupProbe.timeoutSeconds	This is a mandatory parameter. Number of seconds after which the probe times out	Data Type: Integer Range: NA Default Value: 3
nrf-client-nfdiscovery.startupProbe.periodSeconds	This is a mandatory parameter. Specifies that the kubelet should perform a readiness probe every xx seconds	Data Type: Integer Range: NA Default Value: 10
nrf-client-nfdiscovery.startupProbe.successThreshold	This is a mandatory parameter. Minimum consecutive successes for the probe to be considered successful after having failed	Data Type: Integer Range: NA Default Value: 1
nrf-client-nfdiscovery.startupProbe.failureThreshold	This is a mandatory parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up	Data Type: Integer Range: NA Default Value: 6
nrfclient.nrf-client.nrf-client-nfdiscovery.deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to nrf-client-nfdiscovery specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.nrf-client.nrf-client-nfdiscovery.deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to nrf-client-nfdiscovery specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA

Table 3-13 (Cont.) nrf-client-nfdiscovery

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfdiscovery.service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to nrf-client-nfdiscovery specific Service.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.nrf-client.nrf-client-nfdiscovery.service.customExtension.anotations	This is an optional parameter. Custom Annotations that needs to be added to nrf-client-nfdiscovery specific Services.	**Data Type**: String **Default Value**: null **Range**: NA

Table 3-14 nrf-client-nfmanagement

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfmanagement.image	This is a mandatory parameter. NRF Client Microservice image name	Data Type: String Range: NA Default Value: nrf-client
nrfclient.nrf-client.nrf-client-nfmanagement.imageTag	This is a mandatory parameter. NRF Client Microservice image tag	Data Type: String Range: NA Default Value: helm_nrfclient_tag
nrfclient.nrf-client.nrf-client-nfmanagement.extraContainers	This is an optional parameter. This attribute is used to control the usage of extra container when DEBUG tool is ENABLED.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
nrfclient.nrf-client.nrf-client-nfmanagement.dbHookImage.name	This is a mandatory parameter. Image name of dbHook	Data Type: String Range: NA Default Value: common_config_hook
nrfclient.nrf-client.nrf-client-nfmanagement.dbHookImage.tag	This is a mandatory parameter. Image tag name of dbHook	Data Type: String Range: NA Default Value: helm_nrf_client_db_hook_tag
nrfclient.nrf-client.nrf-client-nfmanagement.dbHookImage.pullPolicy	This is a mandatory parameter. Indicates if the image needs to be pulled or not	Data Type: ENUM Range: Always, IfNotPresent, Never Default Value: IfNotPresent
nrfclient.nrf-client.nrf-client-nfmanagement.global.logStorage	This is an optional parameter. Log storage for ephemeral storage request.	Data Type: Integer Range: NA Default Value: 32
nrfclient.nrf-client.nrf-client-nfmanagement.global.crictlStorage	This is an optional parameter. Critical storage for ephemeral storage request.	Data Type: Integer Range: NA Default Value: 32
nrfclient.nrf-client.nrf-client-nfmanagement.global.ephemeralStorageLimit	This is an optional parameter. Ephemeral storage allocation limits	Data Type: Integer Range: NA Default Value: 1024

Table 3-14 (Cont.) nrf-client-nfmanagement

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfmanagement.envJaegerSamplerParam	This is an Conditional Parameter. Note: You must customize this parameter only when NRF client services are enabled. Trace capture in percentage	Data Type: String Range: NA Default Value: '1'
nrfclient.nrf-client.nrf-client-nfmanagement.envJaegerSamplerType	This is an Conditional Parameter. Note: You must customize this parameter only when NRF client services are enabled. Trace Sampler type	Data Type: String Range: NA Default Value: ratelimiting
nrfclient.nrf-client.nrf-client-nfmanagement.envJaegerServiceName	This is an Conditional Parameter. Note: You must customize this parameter only when NRF client services are enabled. Jaeger Service Name	Data Type: String Range: NA Default Value: nrf-client-nfmanagement
nrfclient.nrf-client.nrf-client-nfmanagement.enablePDBSupport	This is an optional parameter. This flag is to enable and disable Pod Disruption Budget feature.If its enabled, nrf-client-nfmanagement.replicas should be set to 2.	Data Type: Boolean Range: True or False Default Value: false
nrfclient.nrf-client.nrf-client-nfmanagement.replicas	This is a mandatory parameter. Indicates the number of pods, which needs to be created as part of deployment.	Data Type: Integer Range: NA Default Value: 1
nrfclient.nrf-client.nrf-client-nfmanagement.cpuRequest	This is a mandatory parameter. Maximum cpu limit to which it can be requested	Data Type: Integer Range: NA Default Value: 1
nrfclient.nrf-client.nrf-client-nfmanagement.cpuLimit	This is a mandatory parameter. maximum cpu limit	Data Type: Integer Range: NA Default Value: 1
nrfclient.nrf-client.nrf-client-nfmanagement.memoryRequest	This is a mandatory parameter. The amount of memory requested	Data Type: String Range: NA Default Value: 1Gi
nrfclient.nrf-client.nrf-client-nfmanagement.memoryLimit	This is a mandatory parameter. Memory limit for nrf-client nfmanagement service	Data Type: String Range: NA Default Value: 1Gi
nrfclient.nrf-client.nrf-client-nfmanagement.hookRestartPolicy	This is a mandatory parameter. Restart Policy for hooks	Data Type: String Range: NA Default Value: Never
nrfclient.nrf-client.nrf-client-nfmanagement.metricPrefix	This is an optional parameter. A prefix that shall be added to all the metric names.By default, this shall contain the value configured in the global section metricPrefix	Data Type: String Range: NA Default Value: ""

Table 3-14 (Cont.) nrf-client-nfmanagement

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfmanagement.metricSuffix	This is an optional parameter. A suffix that shall be added to all the metric names.By default, this shall contain the value configured in the global section metricSuffix	Data Type: String Range: NA Default Value: ""
nrfclient.nrf-client.nrf-client-nfmanagement.istioExcludePorts	Ports to be added in the "excludeInboundPort" and "excludeOutboundPort" ports in ASM. Add actuator prometheus here for oso read of metrics as comma separated values.	Data Type: Integer Range: NA Default Value: 53
nrfclient.nrf-client.nrf-client-nfmanagement.istioSidecarQuitUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar quit URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to explicitly shutdown the sidecar container.	Data Type: String Range: NA Default Value: http://127.0.0.1:15000/quitquitquit
nrfclient.nrf-client.nrf-client-nfmanagement.istioSidecarReadyUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar ready URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to check the readiness of the sidecar container during initialization process.	Data Type: String Range: NA Default Value: http://127.0.0.1:15000/ready
nrfclient.nrf-client.nrf-client-nfmanagement.serviceMeshCheck	This is an optional parameter.Flag to enable aspen service mesh.	Data Type: String Range: NA Default Value: false
nrfclient.nrf-client.nrf-client-nfmanagement.nfProfileConfigMode	This is an optional parameter. Flag to switch between "HELM" based or "REST" based nfProfile configuration	Data Type: String Range: NA Default Value: HELM
nrfclient.nrf-client.nrf-client-nfmanagement.commonCfgClient.enabled	This is an optional parameter. Set it to true if persistent configuration needs to be enabled.	Data Type: Boolean Range: True or False Default Value: true
nrfclient.nrf-client.nrf-client-nfmanagement.commonCfgServer.configServerSvcName	This is an optional parameter. Service name of common configuration service to which the client tries to poll for configuration updates	Data Type: String Range: NA Default Value: config-mgr-svc

Table 3-14 (Cont.) nrf-client-nfmanagement

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfmanagement.commonCfgServer.host	This is an optional parameter. The Host name of the Nf Configuration Service name or the common config service.This attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: config-mgr-svc
nrfclient.nrf-client.nrf-client-nfmanagement.commonCfgServer.port	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) Port of Common Configuration server	Data Type: Integer Range: NA Default Value: 9090
nrfclient.nrf-client.nrf-client-nfmanagement.commonCfgServer.pollingInterval	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) This is the interval between two subsequent polling requests from config client to server	Data Type: Integer Range: NA Default Value: 5000
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.dbHost	This is a mandatory parameter. Specifies the Hostname of MySQL that is used to store configurations.	Data Type: String Range: NA Default Value: sepp-mysql-svc
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.dbPort	This is a mandatory parameter. Specifies the port number of MySQL.	Data Type: String Range: NA Default Value: 3306
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.secretName	This is a mandatory parameter. Specifies the database secret from which the db name, db password and db user name is picked.	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.dbName	This is a mandatory parameter. Specifies the database name to be used to store the common configuration.	Data Type: String Range: NA Default Value: seppdb
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.leaderPodDbName	This is a mandatory parameter. Name of the database	Data Type: String Range: NA Default Value: seppdb
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.networkDbName	This is a mandatory parameter. Name of the database	Data Type: String Range: NA Default Value: seppdb
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.dbUNameLiteral	This is a mandatory parameter. Specifies the database literal name that shall be used as per the <dbConfig.secretName>.	Data Type: Range: NA Default Value: mysql-username

Table 3-14 (Cont.) nrf-client-nfmanagement

Name	Description	Details
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.dbPwdLiteral	This is a mandatory parameter. Specifies the database password literal name that shall be used as per the <dbConfig.secretName>.	Data Type: String Range: NA Default Value: mysql-password
nrfclient.nrf-client.nrf-client-nfmanagement.dbConfig.dbEngine	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
nrf-client-nfmanagement.startupProbe.initialDelaySeconds	This is a mandatory parameter. Tells the kubelet that it should wait second before performing the first probe	Data Type: Integer Range: NA Default Value: 20
nrf-client-nfmanagement.startupProbe.timeoutSeconds	This is a mandatory parameter. Number of seconds after which the probe times out	Data Type: Integer Range: NA Default Value: 3
nrf-client-nfmanagement.startupProbe.periodSeconds	This is a mandatory parameter. Specifies that the kubelet should perform a readiness probe every xx seconds	Data Type: Integer Range: NA Default Value: 10
nrf-client-nfmanagement.startupProbe.successThreshold	This is a mandatory parameter. Minimum consecutive successes for the probe to be considered successful after having failed	Data Type: Integer Range: NA Default Value: 1
nrf-client-nfmanagement.startupProbe.failureThreshold	This is a mandatory parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up	Data Type: Integer Range: NA Default Value:10
nrfclient.nrf-client.nrf-client-nfmanagement.deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to nrf-client-nfmanagement specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.nrf-client.nrf-client-nfmanagement.service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to nrf-client-nfmanagement specific Service.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.nrf-client.nrf-client-nfmanagement.service.customExtension.anotations	This is an optional parameter. Custom Annotations that needs to be added to nrf-client-nfmanagement specific Services.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.nrf-client.nrf-client-nfmanagement.deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to nrf-client-nfmanagement specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA

nrf-client Global Parameters

Table 3-15 nrf-client Global Parameters

Parameter	Description	Details
nfName	This is a mandatory parameter nfName is used as a prefix in service names of nrf client's service and other services it connects to.	Data Type: String Range: NA Default Value: sepp
nrfClientNfDiscoveryEnable	This is a mandatory parameter Global control to enable or disable deployment of NF Discovery service. Enable it if on demand discovery of NF is required.	Data Type: Boolean Range: True or False Default Value: true
nrfClientNfManagementEnable	This is a mandatory parameter. Global control to enable or disable deployment of NF Management service.	Data Type: Boolean Range: True or False Default Value: true
alternateRouteServiceEnable	This is a mandatory parameter. Global parameter to mention if alternate-route service is available (deployed) or not.	Data Type: Boolean Range: True or False Default Value: false
altServiceHTTP2Enabled	This is a mandatory parameter. enable HTTP2 support for alternate service requests.	Data Type: Boolean Range: True or False Default Value: true
altServiceReqTimeout	This is a mandatory parameter. http timeout value. Unit : milliseconds	Data Type: Integer Range: NA Default Value: 3000
altServiceLookupInterval	This is a mandatory parameter. Alternate service lookup interval	Data Type: Integer Range: NA Default Value: 3000
envJaegerAgentHost	This is a mandatory parameter. Jaeger tracing host	Data Type: String Range: NA Default Value: ' '
envJaegerAgentPort	This is a mandatory parameter. Jaeger tracing port	Data Type: Integer Range: NA Default Value: 6831
nrfClientNodePort	This is a mandatory parameter. Provide value for NodePort	Data Type: Integer Range: NA Default Value: 0
vendor	This is a mandatory parameter. Vendor name	Data Type: String Range: NA Default Value: Oracle
applicationName	This is a mandatory parameter. Application name	Data Type: String Range: NA Default Value: nrf-client
metricPrefix	This is a mandatory parameter. Prefix for Metrics	Data Type: String Range: NA Default Value: " "

Table 3-15 (Cont.) nrf-client Global Parameters

Parameter	Description	Details
metricSuffix	This is a mandatory parameter. Suffix for Metrics	Data Type: String Range: NA Default Value: " "
nrfClientCommonServicePort	This is a mandatory parameter. Common service port	Data Type: Integer Range: NA Default Value: 9091
prometheusScrapingConfig.enabled	This is a mandatory parameter. flag to enable or disable Prometheus scraping	Data Type: Boolean Range: True or False Default Value: true
prometheusScrapingConfig.path	This is a mandatory parameter. Path for Prometheus scraping	Data Type: String Range: NA Default Value: /actuator/prometheus
configServerEnable	This is a mandatory parameter. Flag to enable or Disable Config server If nrfclientDisable mode is set/ Roaming-Hub mode is set, set the value to false	Data Type: Boolean Range: True or False Default Value: true
configServerFullNameOverride	This is a mandatory parameter. Config-Server Service full name. Shall be used as {{ ReleaseName }}-configServerFullNameOverride	Data Type: String Range: NA Default Value: ocpm-config
envMysqlHost	This is a mandatory parameter. MySQL Host name	Data Type: String Range: NA Default Value: sepp-mysql-svc
envMysqlPort	This is a mandatory parameter. MySQL Port number	Data Type: String Range: NA Default Value: 3306
dbCredSecretName	This is a mandatory parameter. MySQL Secret name	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
appinfoServiceEnable	This is a mandatory parameter. flag to enable or disable appinfo service. **Note**: For the Roaming hub mode, the value must be set to false.	Data Type: Boolean Range: True or False Default Value: true
performanceServiceEnable	This is a mandatory parameter. flag to enable or disable performance service	Data Type: Boolean Range: True or False Default Value: true
deploymentNrfClientService.envNfNamespace	This is an optional parameter. namespace of Services to be monitored by performance service.If no services are to be monitored, envNfNamespace can be left blank	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE

Table 3-15 (Cont.) nrf-client Global Parameters

Parameter	Description	Details
deploymentNrfClientService.envNfType	This is an optional parameter. Name of Service to be monitored by performance service. If no services are to be monitored, envNfType can be left blank	Data Type: String Range: NA Default Value: sepp
deploymentNrfClientService.envConsumeSvcName	This is an optional parameter. Name of consumer Service to be monitored by performance service.	Data Type: String Range: NA Default Value: nsepp-telescopic:ocsepp-release-plmn-ingress-gateway
deploymentNrfClientService.envEgressGatewayFullnameOverride	This is a mandatory parameter. Egress gateway Host.	Data Type: String Range: NA Default Value: plmn-egress-gateway
deploymentNrfClientService.envEgressGatewayPort	This is a mandatory parameter. Egress gateway port number	Data Type: Integer Range: NA Default Value: 8080
deploymentNrfClientService.nodeSelectorEnabled	This is a mandatory parameter. Flag to enable or disable node selector.	Data Type: Boolean Range: True or False Default Value: false
deploymentNrfClientService.nodeSelectorKey	This is a mandatory parameter. NodeSelector key configuration at the microservice level when helm Based Configuration Node Selector Api Version is set to v1 then this configuration is used. And this configuration does not depend on nodeSelection flag, once configured this is used for all microservices.	Data Type: String Range: NA Default Value: cnf
deploymentNrfClientService.nodeSelectorValue	This is a mandatory parameter. NodeSelector Value configuration at the global level when helmBasedConfigu rationNodeSelectorApiVersion is set to v1 then this configuration is used. And this configuration does not depend on nodeSelection flag, once configured this is used for all microservices.	Data Type: String Range: NA Default Value: ocsepp
privilegedDbCredSecretName	This is a mandatory parameter. K8s Secret containing Database/ user/password for DB Hooks for creating tables	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
releaseDbName	This is a mandatory parameter MySQL Release DB Name	Data Type: String Range: NA Default Value: seppdb

Table 3-15 (Cont.) nrf-client Global Parameters

Parameter	Description	Details
leaderPodDbName	This is a mandatory parameter. (if multipod is supported for NRF client) Specifies the database name for LeaderPodDb database. This database is unique per site	Data Type: String Range: NA Default Value: seppdb
networkDbName	This is a mandatory parameter. (if multipod is supported for NRF client) Specifies the network database name.	Data Type: String Range: NA Default Value: seppdb

Config Map Configuration

Table 3-16 Config Map nrf-client Configuration

Parameter	Description
configmapApplicationConfig.profile.primaryNrfApiRoot	Primary NRF Hostname and Port
configmapApplicationConfig.profile.nrfScheme	Scheme of primary and secondary NRF http or https.
configmapApplicationConfig.profile.retryAfterTime	Default downtime(in Duration) of an NRF detected to be unavailable.
configmapApplicationConfig.profile.nrfClientType	The NfType of the NF registering
configmapApplicationConfig.profile.nrfClientSubscribeTypes	The NFType for which the NF wants to subscribe to the NRF.
configmapApplicationConfig.profile.appProfiles	The NfProfile of the NF to be registered with NRF.
configmapApplicationConfig.profile.registrationRetryInterval	Retry Interval after a failed autonomous registration request.
configmapApplicationConfig.profile.subscriptionRetryInterval	Retry Interval after a failed autonomous subscription request.
configmapApplicationConfig.profile.discoveryRetryInterval	Retry Interval after a failed autonomous discovery request.
configmapApplicationConfig.profile.renewalTimeBeforeExpiry	Time Period(seconds) before the Subscription Validity time expires.
configmapApplicationConfig.profile.validityTime	The default validity time(days) for subscriptions.
configmapApplicationConfig.profile.enableSubscriptionAutoRenewal	Enable Renewal of Subscriptions automatically.
configmapApplicationConfig.profile.nfHeartbeatRate	This value specifies the rate at which the NF shall heartbeat with the NRF. The value shall be configured in terms of percentage(1-100). if the heartbeatTimer is 60s, then the NF shall heartbeat at nfHeartBeatRate * 60/100.

Table 3-16 (Cont.) Config Map nrf-client Configuration

Parameter	Description
`configmapApplicationConfig.profile.discoveryRefreshInterval`	This attribute defines the maximum ValidityPeriod at which the discovery results shall be refreshed. The ValidityPeriod received in the discovery response shall be capped at this value. If ValidityPeriod received in discovery results is 60s. The validityPeriod shall be capped to 10s as per configuration. If ValidityPeriodn received in discovery results is 5s. No capping shall be applied and valdiityPeriod shall be considered as 5s. Unit : seconds
`configmapApplicationConfig.profile.discoveryDurationBeforeExpiry`	This attributes defines the rate at which the NF shall resend discovery requests to NRF. The value shall be configured in terms of percentage(1-100). if the discovery ValidityPeriod is 10s(after applying the capped value of discoveryRefreshInterval), then the discovery requests shall be sent at discoveryDurationBeforeExpiry * 10/100.
`configmapApplicationConfig.profile.acceptAdditionalAttributes`	Enable additionalAttributes as part of 29.510 Release 15.5.
`configmapApplicationConfig.profile.retryForCongestion`	The duration(seconds) after which nrf-client should retry to a NRF server found to be congested.
`configmapApplicationConfig.profile.supportedDataSetId`	The data-set value to be used in queryParams for NFs autonomous/on-demand discovery.
`configmapApplicationConfig.profile.useAlternateScpOnAlternateRouting`	Enable use SCP on alternate routing service.
`configmapApplicationConfig.profile.requestTimeoutGracePeriod`	The grace period at nrf-client for which it shall wait for a response from the NRF. This value shall be added to value configured at configmapApplicationConfig.profile.requestTimeout. Unit : seconds NOTE: The setting support for *2s* (means in seconds) or *50ms* (means in milliseconds) format since Release 1.6.x

3.1.12 config-server

This section includes information about the config-server parameters of the SEPP.

Table 3-17 config-server

Name	Description	Details
`nrfclient.config-server.extraContainers`	This is an optional parameter. This attribute is used to control the usage of extra container when DEBUG tool is ENABLED.	Data Type: Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value:
`nrfclient.config-server.enabled`	This is a mandatory parameter. flag to enable or disable config-server	Data Type: Boolean Range: True or False Default Value: true

Table 3-17 (Cont.) config-server

Name	Description	Details
nrfclient.config-server.image	This is a mandatory parameter. config-server microservice image name.	Data Type: String Range: NA Default Value: occnp/oc-config-server
nrfclient.config-server.imageTag	This is a mandatory parameter.config-server Microservice image tag	Data Type: String Range: NA Default Value: helm_nrfclient_config_server_tag
nrfclient.config-server.fullnameOverride	This is a mandatory parameter. Full name to be used for configuration server service	Data Type: String Range: NA Default Value: occnp-config-server
nrfclient.config-server.installedChartVersion	This is a mandatory parameter. Chart version to be read by hooks	Data Type: String Range: NA Default Value: ''
nrfclient.config-server.envJaegerServiceName	This is an Conditional Parameter Note: You must customize this parameter only when NRF client services are enabled. Jaeger Service Name	Data Type: String Range: NA Default Value: occne-tracer-jaeger-agent.occne-infra
nrfclient.config-server.nfInstanceId	This is an Conditional Parameter This is the NfInstanceId of NF that will get deployed. This shall be used in the profile being registered.	Data Type: String Range: NA Default Value: 9faf1bbc-6e4a-4454-a507-aef01a101a06
nrfclient.config-server.envMysqlDatabase	This is a mandatory parameter. MySQL Database to be used.	Data Type: String Range: NA Default Value: seppdb
nrfclient.config-server.replicas	This is a mandatory parameter. Indicates the number of pods, which needs to be created as part of deployment.	Data Type: Integer Range: NA Default Value: 2
nrfclient.config-server.minReplicas	This is a mandatory parameter. Min replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 2
nrfclient.config-server.maxReplicas	This is a mandatory parameter. Max replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: NA Default Value: 2
nrfclient.config-server.averageCpuUtil	This is a mandatory parameter. CPU utilisation limit for autoscaling (creating HPA)	Data Type: Integer Range: NA Default Value: 70

Table 3-17 (Cont.) config-server

Name	Description	Details
nrfclient.config-server.dbConfig.dbEngine	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
nrfclient.config-server.global.serviceMeshEnabled	This is an optional parameter.Flag to enable aspen service mesh.	Data Type: Boolean Range: True or False Default Value: false
nrfclient.config-server.global.istioSidecarQuitUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar quit URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to explicitly shutdown the sidecar container.	Data Type: String Range: NA Default Value: http://127.0.0.1:15020/quitquitquit
nrfclient.config-server.global.istioSidecarReadyUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar ready URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to check the readiness of the sidecar container during initialisation process.	Data Type: String Range: NA Default Value: http://127.0.0.1:15020/healthz/ready
nrfclient.config-server.global.logStorage	This is an optional parameter. Log storage for ephemeral storage request	Data Type: Integer Range: NA Default Value: 32
nrfclient.config-server.global.crictlStorage	This is an optional parameter. Critical storage for ephemeral storage request	Data Type: Integer Range: NA Default Value: 32
nrfclient.config-server.resources.limits.cpu	This is an optional parameter. CPU Limit for config-server service	Data Type: Range: Default Value: 1
nrfclient.config-server.resources.limits.memory	This is an optional parameter. Memory Limit for config-server service	Data Type: Range: Default Value: 1Gi
nrfclient.config-server.resources.limits.ephemeralStorage	This is an optional parameter. Ephemeral storage allocation limits	Data Type: Range: Default Value: 1Gi
nrfclient.config-server.resources.requests.cpu	This is an optional parameter. Requested CPU usage for config-server pod to come up	Data Type: Range: Default Value: 1

Table 3-17 (Cont.) config-server

Name	Description	Details
nrfclient.config-server.resources.requests.memory	This is an optional parameter. Requested memory usage for config-server pod to come up	Data Type: Range: Default Value: 1Gi
nrfclient.config-server.maxUnavailable	This is an optional parameter. Number of replicas that can go down during a disruption	Data Type: String Range: NA Default Value: 25%
nrfclient.config-server.servicePcfConfig.type	This is a mandatory parameter. Kubernetes service type for exposing config-server deployment	Data Type: String Range: NA Default Value: NodePort
nrfclient.config-server.service.customExtension.anotations	This is an optional parameter. Custom Annotations that needs to be added to config server specific Services.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.config-server.deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to config server specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.config-server.deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to config server specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.config-server.service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to config server specific Service.	**Data Type**: String **Default Value**: null **Range**: NA

3.1.13 appinfo

This section includes information about the appinfo parameters of the SEPP.

Table 3-18 appinfo

Parameter	Description	Details
nrfclient.appinfo.serviceMeshCheck	This is an optional parameter. Flag to enable aspen service mesh.	Data Type: Boolean Range: True or False Default Value: false
nrfclient.appinfo.istioSidecarQuitUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar quit URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to explicitly shutdown the sidecar container.	Data Type: String Range: NA Default Value: http://127.0.0.1:15020/quitquitquit

Table 3-18 (Cont.) appinfo

Parameter	Description	Details
nrfclient.appinfo.istioSidecarReadyUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar ready URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to check the readiness of the sidecar container during initialization process.	Data Type: String Range: NA Default Value: http://127.0.0.1:15020/ready
nrfclient.appinfo.extraContainers	This is an optional parameter. This attribute is used to control the usage of extra container when DEBUG tool is ENABLED.	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
nrfclient.appinfo.enabled	This is a mandatory paramenet Flag to enable or disable appinfo service	Data Type: Boolean Range: True or False Default Value: true
nrfclient.appinfo.image	This is a mandatory parameter. Name of the docker image of app info service	Data Type: String Range: NA Default Value: occnp/oc-app-info
nrfclient.appinfo.imageTag	This is a mandatory parameter. Tag of the image of app info service	Data Type: String Range: NA Default Value: helm_nrfclient_app_info_tag
nrfclient.appinfo.imagePullPolicy	This is a mandatory parameter. Indicates if the image needs to be pulled or not.	Data Type: ENUM Range: Always, IfNotPresent, Never Default Value: Always
nrfclient.appinfo.dbHookImage.name	This is a mandatory parameter. Image name of dbHook	Data Type: Range: Default Value: common_config_hook
nrfclient.appinfo.dbHookImage.tag	This is a mandatory parameter. Image tag name of dbHook	Data Type: String Range: NA Default Value: helm_nrf_client_db_hook_tag
nrfclient.appinfo.dbHookImage.pullPolicy	This is a mandatory parameter. Indicates if the image needs to be pulled or not	Data Type: ENUM Range: Always, IfNotPresent, Never Default Value: Always
nrfclient.appinfo.replicas	This is a mandatory parameter. Indicates the number of pods, which needs to be created as part of deployment.	Data Type: Integer Range: NA Default Value: 2

Table 3-18 (Cont.) appinfo

Parameter	Description	Details
nrfclient.appinfo.minReplicas	This is a mandatory parameter. Min replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: Default Value: 2
nrfclient.appinfo.maxReplicas	This is a mandatory parameter. Max replicas to scale to maintain an average CPU utilisation	Data Type: Integer Range: Default Value: 2
nrfclient.appinfo.prometheusUrl	This is a mandatory parameter. Prometheus server k8s service URL Information	Data Type: String Default Value: http://occne-kube-prom-stack-kube-prometheus.occne-infra:80/clustername/prometheus Note: The user must configure the actual name of the cluster in place of /clustername.
nrfclient.appinfo.alertmanagerUrl	This is a mandatory parameter. Alert manager k8s service URL Information	Data Type: String Default Value: http://occne-kube-prom-stack-kube-prometheus.occne-infra:80/clustername/alertmanager Note: The user must configure the actual name of the cluster in place of /clustername.
nrfclient.appinfo.global.logStorage	This is an optional parameter. Log storage for ephemeral storage request	Data Type: Range: Default Value: 32
nrfclient.appinfo.global.crictlStorage	This is an optional parameter. Critical storage for ephemeral storage request	Data Type: Range: Default Value: 32
nrfclient.appinfo.resources.limits.cpu	This is an optional parameter. CPU Limit for app info pod	Data Type: Range: Default Value: 1
nrfclient.appinfo.resources.limits.memory	This is an optional parameter. Memory Limit for app info pod	Data Type: Range: Default Value: 2Gi
nrfclient.appinfo.resources.limits.ephemeralStorage	This is an optional parameter. Ephemeral storage allocation limits	Data Type: Range: Default Value: 1Gi
nrfclient.appinfo.resources.requests.cpu	This is an optional parameter. Requested CPU usage for app info pod to come up	Data Type: Range: Default Value: 1
nrfclient.appinfo.resources.requests.memory	This is an optional parameter. Requested memory usage for app info pod to come up	Data Type: Range: Default Value: 1Gi
nrfclient.appinfo.resources.maxUnavailable	This is an optional parameter. Number of replicas that can go down during a disruption	Data Type: Range: Default Value: 25%

Table 3-18 (Cont.) appinfo

Parameter	Description	Details
nrfclient.appinfo.serviceAccountName	This is an optional parameter. Name of Service account	Data Type: Range: Default Value: ' '
nrfclient.appinfo.commonServiceName	This is an optional parameter. This is the common service name that is currently requesting for configuration updates from server	Data Type: String Range: NA Default Value: app-info
nrfclient.appinfo.log.level.appinfo	This is an optional parameter. Identifies log level of app info	Data Type: ENUM Range: INFO, DEBUG, ERROR Default Value: INFO
nrfclient.appinfo.commonCfgClient.enabled	This is an optional parameter. Set it to true if persistent configuration needs to be enabled.	Data Type: Boolean Range: True or False Default Value: true
nrfclient.appinfo.commonCfgServer.configServerSvcName	This is an optional parameter. Service name of common configuration service to which the client tries to poll for configuration updates	Data Type: String Range: NA Default Value: config-mgr-svc
nrfclient.appinfo.commonCfgServer.host	This is an optional parameter. The Host name of the Nf Configuration Service name or the common config service.This attribute shall be configured only if commonCfgClient.enabled is set to true.	Data Type: String Range: NA Default Value: config-mgr-svc
nrfclient.appinfo.commonCfgServer.port	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) Port of Common Configuration server	Data Type: Integer Range: NA Default Value: 9090
nrfclient.appinfo.commonCfgServer.pollingInterval	This is the interval between two subsequent polling requests from configuration client to server	Data Type: Integer Range: NA Default Value: 5000
nrfclient.appinfo.commonCfgServer.connectionTimeout	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) This is the limit for connection to be established between config client and server	Data Type: Integer Range: NA Default Value: 10000 #ms
nrfclient.appinfo.dbConfig.dbHost	This is a mandatory parameter. Specifies the Hostname of MySQL that is used to store configurations.	Data Type: String Range: NA Default Value: sepp-mysql-svc

Table 3-18 (Cont.) appinfo

Parameter	Description	Details
`nrfclient.appinfo.dbConfig.dbPort`	This is a mandatory parameter. Specifies the port number of MySQL.	Data Type: Integer Range: NA Default Value: 3306
`nrfclient.appinfo.dbConfig.secretName`	This is a mandatory parameter. Specifies the database secret from which the db name, db password and db user name is picked.	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
`nrfclient.appinfo.dbConfig.dbName`	This is a mandatory parameter. Specifies the database name to be used to store the common configuration.	Data Type: String Range: NA Default Value: seppdb
`nrfclient.appinfo.dbConfig.dbUNameLiteral`	This is a mandatory parameter. Specifies the database literal name that shall be used as per the <dbConfig.secretName>.	Data Type: String Range: NA Default Value: mysql-username
`nrfclient.appinfo.dbConfig.dbPwdLiteral`	This is a mandatory parameter. Specifies the database password literal name that shall be used as per the <dbConfig.secretName>.	Data Type: String Range: NA Default Value: mysql-password
`nrfclient.appinfo.dbConfig.dbEngine`	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: ENUM Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
`nrfclient.appinfo.core_services.sepp`	This is an optional parameter. Specifies the list of SEPP services to be monitored.	Data Type: String Range: NA Default Value: [ ]

Table 3-18 (Cont.) appinfo

Parameter	Description	Details
`nrfclient.appinfo.infraServices`	This is a conditional parameter. Specifies the URI for the health check of InfraServices that need to be monitored. Examples: http://mysql- cluster-db- monitor-svc.vzw1- cndbtier:8080 / actuator/ health http://mysql- cluster-db-replication- svc.vzw1- cndbtier/ actuator/ health Uncomment this parameter and set this parameter to an empty array if any one of following conditions is true: • Deploying on OCCNE 1.4 or lower version • Not deploying on OCCNE • Do not wish to monitor infra services such as db-monitor service	Data Type: String Range: NA Default Value: [ ]
`nrfclient.appinfo.service.customExtension.labels`	This is an optional parameter. Custom Labels that needs to be added to appinfo specific Service.	**Data Type**: String **Default Value**: null **Range**: NA
`nrfclient.appinfo.service.customExtension.anotations`	This is an optional parameter. Custom Annotations that needs to be added to appinfo specific Services.	**Data Type**: String **Default Value**: null **Range**: NA
`nrfclient.appinfo.deployment.customExtension.labels`	This is an optional parameter. Custom Labels that needs to be added to appinfo specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
`nrfclient.appinfo.deployment.customExtension.annotations`	This is an optional parameter. Custom Annotations that needs to be added to appinfo specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA

3.1.14 Pre-install hook

This section includes information about the Pre-install hook parameters of the SEPP.

Table 3-19 Pre-install hook

Parameter	Description	Details
`pre-install-hook.image.repository`	This is a mandatory parameter. Repository location of image	Data Type: String Range: NA Default Value: reg-1

Table 3-19 (Cont.) Pre-install hook

Parameter	Description	Details
`pre-install-hook.image.name`	This is a mandatory parameter. Name of image	Data Type: String Range: NA Default Value: ocsepp-pre-install-hook
`pre-install-hook.image.tag`	This is a mandatory parameter. Tag of image	Data Type: String Range: NA Default Value: helm-tag
`pre-install-hook.image.pullPolicy`	This is a mandatory parameter. This setting indicates if the image needs to be pulled or not	Data Type: String Range: NA Default Value: Always

3.1.15 update-db

This section includes information about the update-db parameters of the SEPP.

Table 3-20 update-db

Parameter	Description	Details
`update-db.serviceMeshCheck`	Enabled when deployed in serviceMesh.	Data Type: Boolean Range: NA Default Value: false
`update-db.istioSidecarQuitUrl`	This is a mandatory parameter. The sidecar (istio quit url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/quitquitquit
`update-db.istioSidecarReadyUrl`	This is a mandatory parameter. The sidecar (istio ready url)when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Range: NA Default value: http://127.0.0.1:15020/ready
`update-db.image.repository`	This is a mandatory parameter. Repository location of image	Data Type: String Range: NA Default Value: reg-1
`update-db.image.name`	This is a mandatory parameter. Name of image	Data Type: String Range: NA Default Value: ocsepp-update-db
`update-db.image.tag`	This is a mandatory parameter. Tag of image	Data Type: String Range: NA Default Value: helm-tag
`update-db.image.pullPolicy`	This is a mandatory parameter.. This setting indicates if the image needs to be pulled or not.	Data Type: String Range: NA Default Value: Always

Table 3-20 (Cont.) update-db

Parameter	Description	Details
`update-db.hookAlerts.prometheus.fqdn`	This is a mandatory parameter. This parameter defines the fqdn for prometheus service. Incorrect value may result in timeout failures during install, upgrade or rollback.	Data Type: String Range: NA Default Value: occne-kube-prom-stack-kube-prometheus. Format : servicename.namespace
`update-db.hookAlerts.prometheus.port`	This is a mandatory parameter.. This parameter defines the port number for prometheus service. Incorrect value may result in timeout failures during install, upgrade or rollback.	Data Type: Integer Range: NA Default Value: 80
`update-db.hookAlerts.prometheus.pathToFetchAlertManagerEndPoint`	This is a mandatory parameter. This parameter defines the endpoint for prometheus actuator service.	Data Type: String Range: NA Default Value: /clustername/prometheus/api/v1/alertmanagers **Note**: The user must configure the actual name of the cluster in place of /clustername.
`update-db.hookAlerts.alertManagerContainerPort`	This is a mandatory parameter. This parameter defines the alert manager container port number.	Data Type: Integer Range: NA Default Value: 9093
`update-db.hookAlerts.customAlertExpiryEnabled`	This is a mandatory parameter. Following variable indicates, alert expiry occurs according to resolve_timeout value of AlertManager and upgrade/rollback hooks shall clear the alerts as applicable. If it is set to true, auto alert clear shall occur after customAlertExpiryDuration value and upgrade/rollback hooks may not clear the alerts.	Data Type: Boolean Range: true or false Default Value: false
`update-db.hookAlerts.customAlertExpiryDuration`	This is a mandatory parameter. The custom duration (in minutes) post which Alert gets auto cleared, applicable only when customAlertExpiryEnabled is set to true.	Data Type: Integer Range: NA Default Value: 60

3.1.16 perf-info

This section includes information about the perf-info of the SEPP.

Table 3-21 perf-info

Parameter	Description	Details
nrfclient.perf-info.image	This is a mandatory parameter. perf-info microservice image name.	Data Type: String Range: NA Default Value: occnp/oc-perf-info
nrfclient.perf-info.imageTag	This is a mandatory parameter. perf-info microservice image tag name.	Data Type: String Range: NA Default Value: helm_nrfclient_perf_info_tag
nrfclient.perf-info.serviceMeshCheck	This is an optional parameter. Flag to enable aspen service mesh.	Data Type: String Range: true or false Default Value: false
nrfclient.perf-info.istioSidecarQuitUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar quit URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to explicitly shutdown the sidecar container.	Data Type: String Range: NA Default Value: http://127.0.0.1:15020/quitquitquit
nrfclient.perf-info.istioSidecarReadyUrl	This is an conditional parameter. Applicable only when serviceMeshCheck parameter is set to true. Specifies the sidecar ready URL (envoy container quite URL) if deployed with serviceMesh. This URL is needed to check the readiness of the sidecar container during initialization process.	Data Type: String Range: NA Default Value: http://127.0.0.1:15020/ready
nrfclient.perf-info.dbHookImage.name	This is a mandatory parameter. Image name of dbHook	Data Type: String Range: NA Default Value: common_config_hook
nrfclient.perf-info.dbHookImage.tag	This is a mandatory parameter. Image tag name of dbHook	Data Type: String Range: NA Default Value: helm_nrf_client_db_hook_tag
nrfclient.perf-info.dbHookImage.pullPolicy	This is a mandatory parameter. Indicates if the image needs to be pulled or not	Data Type: ENUM Range: Always, IfNotPresent, Never Default Value: Always
nrfclient.perf-info.extraContainers	This is an optional parameter Flag to enable addition of container configuration under extraContainersTpl to all the deployments under perf-info umbrella. This parameter is used for debug container template	Data Type: ENUM Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE

Table 3-21 (Cont.) perf-info

Parameter	Description	Details
nrfclient.perf-info.service_namespace	This is a mandatory parameter. Namespace in which perf-info will be deployed.	Data Type: String Range: NA Default Value: DEPLOYMENT_NAMESPACE
nrfclient.perf-info.envMysqlDatabase	This is a mandatory parameter. MySQL Database to be used.	Data Type: String Range: NA Default Value: seppdb
nrfclient.perf-info.replicas	This is a mandatory parameter. Replicas for perf Info - This is exact value without scaling	Data Type: Integer Range: NA Default Value: 2
nrfclient.perf-info.imagepullPolicy	This is a mandatory parameter. Indicates if the image needs to be pulled or not	Data Type: ENUM Range: Always, IfNotPresent, Never Default Value: Always
nrfclient.perf-info.service.port	This is a mandatory parameter. Kubernetes service port for exposing perf-info deployment	Data Type: Integer Range: NA Default Value: 5905
nrfclient.perf-info.global.logStorage	This is an optional parameter. Log storage for ephemeral storage request	Data Type: Integer Range: NA Default Value: 32
nrfclient.perf-info.global.crictlStorage	This is an optional parameter. Critical storage for ephemeral storage request	Data Type: Integer Range: NA Default Value: 32
nrfclient.perf-info.resources.limits.ephemeralStorage	This is an optional parameter. Ephemeral Storage allocation limits	Data Type: String Range: NA Default Value: 1Gi
nrfclient.perf-info.resources.limits.cpu	This is an optional parameter. CPU Limit for perf-info service	Data Type: Integer Range: NA Default Value: 2
nrfclient.perf-info.resources.limits.memory	This is an optional parameter. Memory Limit for perf-info service	Data Type: String Range: NA Default Value: 4Gi
nrfclient.perf-info.resources.requests.cpu	This is an optional parameter. CPU Requested for perf-info service	Data Type: Range: NA Default Value: 2
nrfclient.perf-info.resources.requests.memory	This is an optional parameter. Memory Requested for perf-info service	Data Type: Range: NA Default Value: 200Mi
nrfclient.perf-info.maxUnavailable	This is an optional parameter. Number of replicas that can go down during a disruption	Data Type: Range: NA Default Value: '25%'
nrfclient.perf-info.affinity	This is an Optional Parameter Pod Affinity configurations	Data Type: String Range: NA Default Value:

Table 3-21 (Cont.) perf-info

Parameter	Description	Details
nrfclient.perf-info.commonCfgClient.enabled	This is an optional parameter. Set it to true if persistent configuration needs to be enabled.	Data Type: Boolean Range: true or false Default Value: true
nrfclient.perf-info.commonCfgServer.configServerSvcName	This is an optional parameter. Service name of common configuration service to which the client tries to poll for configuration updates	Data Type: String Range: NA Default Value: 'config-mgr-svc'
nrfclient.perf-info.commonCfgServer.host	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) Host name of Common configuration server to which client tries to poll for configuration updates. This value is picked up if commonCfgServer.configServerSvcName is not available	Data Type: String Range: NA Default Value: config-mgr-svc
nrfclient.perf-info.commonCfgServer.port	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) Port of Common Configuration server	Data Type: Integer Range: NA Default Value: 9090
nrfclient.perf-info.commonCfgServer.pollingInterval	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) This is the interval between two subsequent polling requests from config client to server	Data Type: Integer Range: NA Default Value: 5000
nrfclient.perf-info.commonCfgServer.connectionTimeout	This is a mandatory parameter. (Applicable only if commonCfgClient.enabled is set to true) This is the limit for connection to be established between config client and server	Data Type: Integer Range: NA Default Value: 10000
nrfclient.perf-info.commonServiceName	This is a mandatory parameter. This is the common service name that is currently requesting for configuration updates from server	Data Type: String Range: NA Default Value: perf-info
nrfclient.perf-info.log.level.perfinfo	This is an optional parameter. Log level for perf-info service	Data Type: ENUM Range: NA Default Value: INFO

Table 3-21 (Cont.) perf-info

Parameter	Description	Details
nrfclient.perf-info.dbConfig.dbHost	This is a mandatory parameter. Specifies the Hostname of MySQL that is used to store configurations.	Data Type: String Range: NA Default Value: sepp-mysql-svc
nrfclient.perf-info.dbConfig.dbPort	This is a mandatory parameter. Specifies the port number of MySQL.	Data Type: Integer Range: NA Default Value: 3306
nrfclient.perf-info.dbConfig.secretName	This is a mandatory parameter. Specifies the database secret from which the db name, db password and db user name is picked.	Data Type: String Range: NA Default Value: ocsepp-mysql-cred
nrfclient.perf-info.dbConfig.dbName	This is a mandatory parameter. Specifies the database name to be used to store the common configuration.	Data Type: String Range: NA Default Value: seppdb
nrfclient.perf-info.dbConfig.dbUNameLiteral	This is a mandatory parameter. Specifies the database literal name that shall be used as per the <dbConfig.secretName>.	Data Type: String Range: NA Default Value: mysql-username
nrfclient.perf-info.dbConfig.dbPwdLiteral	This is a mandatory parameter. Specifies the database password literal name that shall be used as per the <dbConfig.secretName>.	Data Type: String Range: NA Default Value: mysql-password
nrfclient.perf-info.dbConfig.dbEngine	This mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
nrfclient.perf-info.overloadManager.enabled	This is a mandatory parameter. Specifies whether to enable or disable overload reporting.	Data Type: Boolean Range: true or false Default Value: false
nrfclient.perf-info.overloadManager.nfType	This is a mandatory parameter. Specifies the NF type that is used to query configuration from common configuration server.	Data Type: String Range: NA Default Value: sepp
nrfclient.perf-info.overloadManager.ingressGatewaySvcName	This is a mandatory parameter. Specifies the names of backend services	Data Type: String Range: NA Default Value: n32-ingress-gateway
nrfclient.perf-info.overloadManager.ingressGatewayPort	This is a mandatory parameter. Specifies the port number of Ingress Gateway	Data Type: Integer Range: NA Default Value: 80
nrfclient.perf-info.ingress.enabled	This is a mandatory parameter. Ingress flag control	Data Type: Boolean Range: NA Default Value: false

Table 3-21 (Cont.) perf-info

Parameter	Description	Details
nrfclient.perf-info.configmapPerformance.prometheus	This is a mandatory parameter. Prometheus server k8s service URL Information	Data Type: String Range: NA Default Value: http: http://prometheus-server.prometheus:5802/<clustername>
nrfclient.perf-info.tagNamespace	This is a mandatory parameter. Specifies the Kubernetes namespace.	Data Type: String Range: NA Default Value: namespace **Note**: In OCI deployment, the value must be k8Namespace.
nrfclient.perf-info.tagContainerName	This is a mandatory parameter. Specifies the tag used for specifying name of the container.	Data Type: String Range: NA Default Value: container
nrfclient.perf-info.tagServiceName	This is a mandatory parameter. Specifies the tag used for specifying name of the service.	Data Type: String Range: NA Default Value: service
probeValidationByPass.enabled	This is an optional parameter. It is used to bypass the startup probe failure during upgrade.	Data Type: Boolean Range: NA Default Value: True
nrfclient.perf-info.deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to perf-info specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.perf-info.deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to perf-info specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.perf-info.service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to perf-info specific Service.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.perf-info.service.customExtension.anotations	This is an optional parameter. Custom Annotations that needs to be added to perf-info specific Services.	**Data Type**: String **Default Value**: null **Range**: NA
nrfclient.perf-info.capacityConfig.overall	This is a mandatory parameter. Overall capacity for all services defined for NF.	Data Type: Integer Default Value: 100 Range: NA
nrfclient.perf-info.capacityConfig.serviceLevel	This is a mandatory parameter. Service level capacity for a particular NF.	Data Type: Integer Default Value: Empty Range: NA
nrfclient.perf-info.capacityConfig.default	This is a mandatory parameter. Default value considered if overall capacity is not defined.	Data Type: Integer Default Value: 100 Range: NA

3.1.17 mediation

nf-mediation parameters

This section includes information about the nf-mediation parameters of the SEPP.

Table 3-22 nf-mediation parameters

Parameter	Description	Details
nf-mediation.istioSidecarQuitUrl	This is a mandatory parameter Field to define the URL that is used for quitting service mesh sidecar. This URL is used to quit the istio sidecar after successful completion of hook job. The reference variable &sidecarQuitUrl should not be changed, however, the value http://127.0.0.1:15020/quitquitquit can be changed. Applicable only when serviceMeshEnabled is set to true.	Data Type: &sidecarQuitUrl"http://127.0.0.1:15000/quitquitquit" Range: NA Default Value: http://127.0.0.1:15020/quitquitquit
nf-mediation.istioSidecarReadyUrl	This is a mandatory parameter Field to define the URL that is used for checking the service mesh sidecar status and start application when the status is ready. The reference variable &sidecarReadyUrl should not be changed, however, the value "http://127.0.0.1:15020/ready can be changed.Applicable only when serviceMeshEnabled isset to true.	Data Type: &sidecarReadyUrl "http://127.0.0.1:15000/ready" Range: NA Default Value: "http://127.0.0.1:15020/ready
nf-mediation.global.imageRepository	This is a mandatory parameter. user need to set imageRepository to the repository where the images are kept.	Data Type: string Range: NA Default Value: reg-1
nf-mediation.global.serviceMeshEnabled	This is an optional parameter.Flag to enable aspen service mesh.	Data Type: Boolean Range: true or false Default Value: false
nf-mediation.global.database.dbHost	This is a mandatory parameter. DB Connection Service IP Or Hostname. DB Service FQDN	Data Type: string Range: Valid IPv4 address as per RFC 791 or Valid FQDN Default Value: "sepp-mysql-svc"
nf-mediation.global.database.dbPort	This is a mandatory parameter. DB Service Port	Data Type: integer Range: Valid port value Default Value: 3306

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
nf-mediation.global.database.dbAppUserSecretName	This is a mandatory parameter K8s Secret containing Database/user/password for all services of SCP interacting with DB.	Data Type: string Range: NA Default Value: 'ocsepp-mysql-cred
nf-mediation.global.database.dbPrivilegedUserSecretName	This is a mandatory parameter Name of the Kubernetes secret object containing the Database username and password for an admin user.	Data Type: string Range: NA Default Value: 'ocsepp-mysql-cred'
nf-mediation.global.database.createUser	This is a mandatory parameter This parameter can enable or disable the automatic database and application user creation.	Data Type: Boolean Range: true false Default Value: true
nf-mediation.global.database.sqlQueryLimit	This is a mandatory parameter Database query limit value	Data Type: Integer Range: NA Default Value: 1000
nf-mediation.global.database.dbName	This is a mandatory parameter.It is the name of SEPP database.	Data Type: string Range: NA Default Value: seppdb
nf-mediation.global.database.seppBackupDbName	This is a mandatory parameter.It is the name of SEPP Backup database. Defines backupdb name where backup will be created during upgrade	Data Type: string Range: NA Default Value: seppbackupdb
nf-mediation.global.databaseEngine	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
nf-mediation.global.hookJob.weight.mediation	This is a mandatory parameter. This parameter decides the pre-hook sequence of Mediation service (In Preinstall, Pre upgrade and Pre rollback)	Data Type: Integer Range: NA Default Value: 8
nf-mediation.global.hookJob.postHookJobsWeights.mediation	This is a mandatory parameter. This parameter decides the post-hook sequence of Mediation service (In Post install, Post upgrade and Post rollback)	Data Type: Integer Range: NA Default Value: 8
nf-mediation.global.upgradeLimit	This is a mandatory parameter. limit of upgrade versions to be supported	Data Type: Integer Range: NA Default Value: 3

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
`nf-mediation.global.rollbackLimit`	This is a mandatory parameter. limit of rollback versions to be supported	Data Type: Integer Range: NA Default Value: 3
`nf-mediation.global.mediation.port.servicePort`	This is a Mandatory parameter This parameter defines the Http Port for mediation service	Data Type: Integer Range: NA Default Value: 9090
`nf-mediation.global.mediation.port.serviceHttpsPort`	This is a Mandatory parameter This parameter defines the Https Port for mediation service	Data Type: Integer Range: NA Default Value: 9091
`nf-mediation.global.mediation.port.containerPort`	This is a Mandatory parameter This parameter defines the container http Port for mediation service	Data Type: Integer Range: NA Default Value: 9090
`nf-mediation.global.mediation.port.containerHttpsPort`	This is a Mandatory parameter This parameter defines the container https Port for mediation service	Data Type: Integer Range: NA Default Value: 9091
`nf-mediation.global.mediation.port.commonServicePort`	This is a Mandatory parameter This parameter defines the port number for prometheus actuator service	Data Type: Integer Range: NA Default Value: 8091
`nf-mediation.global.securityContext`	This is an optional parameter A security context defines privilege and access control settings for a pod.	Data Type: string Range: NA Default Value: {}
`nfmediation.global.enableContainerSecurityContext`	This is a Mandatory parameter. Enables security context for mediation containers.	Data Type: Boolean Range: true or false Default Value: true
`nfmediation.global.containerSecurityContext.readOnlyRootFilesystem`	This is a Mandatory parameter. Mounts the mediation container's root filesystem as read-only.	Data Type: Boolean Range: true or false Default Value: false
`nfmediation.global.containerSecurityContext.allowPrivilegeEscalation`	This is a Mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the no_new_privs parameter gets configured on the container process. `allowPrivilegeEscalation` parameter is always set to true when the container: • is run as privileged. • has CAP_SYS_ADMIN	Data Type: Boolean Range: true or false Default Value: false

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
nfmediation.global.containerSecurityContext.runAsNonRoot	This is a Mandatory parameter. Prevents mediation containers from starting as root user.	Data Type: Boolean Range: true or false Default Value: true
nfmediation.global.containerSecurityContext.privileged	This is a Mandatory parameter. Provides mediation containers' access to the hosts resources and kernel capabilities.	Data Type: Boolean Range: true or false Default Value: false
nfmediation.global.containerSecurityContext.runAsUser	This is a Mandatory parameter. Specifies that for any mediation container in the pod, all processes must run with the provided user ID.	Data Type: Integer Range: Valid IDs for security context for user Default Value: 1012
nfmediation.global.containerSecurityContext.capabilities.add	This is a Mandatory parameter. Manages Linux capabilities for containers. Using Linux capabilities, you can grant certain privileges to a process without granting all the privileges of the root user.	Data Type: List of strings Range: Valid Linux capabilities Default Value: -all
nf-mediation.imageDetails.image	This is a mandatory parameter. Indicates the Image name of mediation.	Data Type: string Range: Name components may contain lowercase letters, digits, and separators. A separator is defined as a period, one or two underscores, or one or more dashes. A name component may not start or end with a separator. Default Value: mediation/ocmed-nfmediation
nf-mediation.imageDetails.tag	This is a mandatory parameter. Indicates the Image tag of mediation.	Data Type: string Range: valid ASCII that may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters. Default Value: nf_mediation_tag
nf-mediation.imageDetails.pullPloicy	This is a mandatory parameter. Indicates if the image has to be pulled.	Data Type: string Range: Always, IfNotPresent, Never Default Value: Always

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
nf-mediation.targetCpuForScaling.averageCpuUtil	This is an optional parameter. A new replica will be created if this much CPU utilisation is reached. This parameter is used in HPA	Data Type: Integer Range: NA Default Value: 70. # %
nf-mediation.maxPdbUnavailable	This is an optional parameter. determine the maximum number of pods that can remain unavailable during a voluntary disruption. For example, if maxPdbUnavailable is 25%, the evictions are allowed until not more than 25% of the desired replicas are unhealthy.	Data Type: string Range: NA Default Value: 25%
nf-mediation.upgradeStrategy	This is an optional parameter. Specifies the strategy used during upgrade process. The only supported upgradeStrategy is rollingUpgrade.	Data Type: string Range: RollingUpdate Default Value: RollingUpdate
nf-mediation.maxUnavailable	This is an optional parameter. parameter determines the number of pods that are unavailable during the update. Maximum number of unavailable should be 0.Since maximum number of replicas for mediation microservice is 1	Data Type: integer Range: Default Value: 0
nf-mediation.maxSurge	This is an optional parameter. The number of pods that can be created above the desired amount of pods during an update	Data Type: integer Range: Default Value: 1
nf-mediation.log.level	This is an mandatory parameter. Enables desired level of logging for the service.	Data Type: string Range: N/A Default Value: ERROR
nf-mediation.minreplicas	This is a mandatory parameter Indicates the minimum replica count of the mediation microservice.	Data Type: integer Range: N/A Default Value: 2
nf-mediation.maxreplicas	This is a mandatory parameter Indicates the maximum replica count of the mediation microservice.	Data Type: integer Range: N/A Default Value: 2
nf-mediation.jaegerTracingEnabled	This is an optional parameter. Enables Jaeger traces for mediation.	Data Type: Boolean Range: true false Default Value: false
nf-mediation.bodyInTraceEnabled	This is an optional parameter. Enables body traces for mediation.	Data Type: Boolean Range: true false Default Value: false

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
nf-mediation.openTracing.jaeger.udpSender.host	This is an optional parameter Indicates the host details of jaeger server.	Data Type: string Range: N/A Default Value: "jaeger-agent.cne-infra"
nf-mediation.openTracing.jaeger.udpSender.port	This is an optional parameter Indicates the port details of Jaeger server.	Data Type: integer Range: 0 - 65535 Default Value: 6831
nf-mediation.openTracing.jaeger.logSpans	This is an optional parameter Enables Jaeger log spans.	Data Type: Boolean Range: true false Default Value: false
nf-mediation.openTracing.jaeger.probabilisticSamplingRate	This is an optional parameter Indicates the sampling rate for Jaeger	Data Type: string Range: 0-1 Default Value: 0.1
nf-mediation.ruleMetricsEnable	This is an optional parameter Enables pegging of rule based metrics	Data Type:Boolean Range: True or False Default value: false
nf-mediation.nfInstanceId	This is an optional parameter This is the instance ID of Mediation	Data Type: String Range: NA Default Value: IWF1
nf-mediation.MediationMode	This is an optional parameter This parameter defines the mode of Mediation service	Data Type: String Range: NA Default Value: NFMediation
opentracingHost	This is an optional parameter. IP address for Jaeger-Agent This parameter comes into picture only if jaegerTracingEnabled parameter is enabled.	Data Type: string Range: valid IP adress Default Value: 10.75.157.169
opentracingPort	This is an optional parameter node port of Jaeger-Agent	Data Type: Integer Range: valid port Default Value: 32460
nf-mediation.server.maxConnections	This is a mandatory parameter This parameter defines the maximum connection created by tomcat server for mediation service	Data Type: Integer Range: Default Value: 10000
nf-mediation.server.queueSize	This is a mandatory parameter This parameter defines the request queue size for tomcat server for mediation service	Data Type: Integer Range: NA Default Value: 100
nf-mediation.server.maxThreads	This is a mandatory parameter This parameter defines the maximum threads for processing the requests created by tomcat server for mediation service	Data Type: Integer Range: NA Default Value: 200

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
nf-mediation.server.spareThreads	This is a mandatory parameter This parameter defines the spare threads for processing the requests created by tomcat server for mediation service	Data Type: Integer Range: NA Default Value: 20
nf-mediation.undertowMaxConcurrentStream	This is a mandatory parameter Maximum number of concurrent streams	Data Type: Integer Range: NA Default Value: 1000
nf-mediation.undertowMaxQueuedReadBuffers	This is a mandatory parameter Maximum number of buffers that will be used before reads are paused in framed protocols	Data Type: Integer Range: NA Default Value: 200
nf-mediation.undertowQueuedFramesHighWaterMark	This is a mandatory parameter Maximum numbers of frames that can be queued before reads are suspended	Data Type: Integer Range: NA Default Value: 1000
nf-mediation.undertowQueuedFramesLowWaterMark	This is a mandatory parameter The point at which reads will resume again after hitting the high water mark	Data Type: Integer Range: NA Default Value: 200
nf-mediation.settingsMaxDownstreamConcurrentStreams	This is a mandatory parameter Maximum number of down cuncurrent streams	Data Type: Integer Range: NA Default Value: 999
nf-mediation.commonCPJCConnectFailureThreshold	This is a mandatory parameter This is one of the common jetty client parameter. Connection failure threshold value	Data Type: integer Range: NA Default Value:10
nf-mediation.commonCPJCMaxConcurrentPushedStreams	This is a mandatory parameter This is one of the common jetty client parameter. Maximum no of Concurrent Pushed Streams	Data Type: integer Range: NA Default Value:1000
nf-mediation.commonCPJCConnectTimeout	This is a conditional parameter. This is one of the common jetty client parameter. This is the limit for connection to be established between client and server.	Data Type: integer Range: NA Default Value:10000
nf-mediation.commonCPJCmaxRequestsQueuedPerDestination	This is a mandatory parameter This is one of the common jetty client parameter. Maximum Requests Queued Per Destination	Data Type: integer Range: NA Default Value:1024

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
nf-mediation.commonCPJCmaxConnectionsPerDestination	This is a mandatory parameter This is one of the common jetty client parameter. Maximum Connections Per Destination	Data Type: integer Range: NA Default Value: 4
nf-mediation.commonCPJCMaxConnectionsPerIp	This is a mandatory parameter This is one of the common jetty client parameter. Maximum Connections Per IP	Data Type: integer Range: NA Default Value: 4
nf-mediation.commonCPJCRrequestTimeout	This is a conditional parameter. This is one of the common jetty client parameter. This is the limit for the configuration for request timeout	Data Type: integer Range: NA Default Value:10000
nf-mediation.commonCPJCDNSRefreshDelay	This is a conditional parameter. This is one of the common jetty client parameter. This is the value for DNS Refresh Delay.	Data Type: integer Range: NA Default Value:15000
nf-mediation.commonCPJCPingDelayDuration	This is a conditional parameter. This is one of the common jetty client parameter. This is the value for Ping delay duration.	Data Type: integer Range: NA Default Value: 0
nf-mediation.downstream.idleTimeout	This is a mandatory parameter The Idle Timeout setting in the TCP profile specifies the length of time that a connection is idle before the connection is eligible for deletion. If no traffic flow is detected within the idle session timeout, the session will be deleted.	Data Type: integer Range: NA Default Value: 600000(sec)
nf-mediation.downstream.tcpKeepalive.count	This is a mandatory parameter used to adjust the count of TCP Keep-Alive packets.	Data Type: Integer Range: NA Default Value: 10
nf-mediation.downstream.tcpKeepalive.enabled	This is a mandatory parameter This parameter Enables TCP Keep alive functionality	Data Type: Boolean Range: true or false Default Value: true
nf-mediation.downstream.tcpKeepalive.interval	This is a mandatory parameter used to adjust the frequency at which TCP Keep-Alive packets are sent to a remote host for connection validation	Data Type: integer Range: NA Default Value: 500 (sec)

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
nf-mediation.downstream.tcpKeepalive.time	This is a mandatory parameter The Keep Alive Interval setting is used to adjust the frequency at which TCP Keep-Alive packets are sent to a remote host for connection validation.	Data Type: integer Range: NA Default Value: 1000 (sec)
nf-mediation.downstream.tcpKeepalive.probes	This is a mandatory parameter This parameter defines the maximum number of unacknowledged keepalive packets that the system will send before considering the connection dead.	Data Type: Integer Range: NA Default Value: 10
nf-mediation.extraContainers	This is a mandatory parameter. Spawns debug container along with application container in the pod. This debug container is used for debugging purposes.	Data Type: string Range: DISABLED, ENABLED, USE_GLOBAL_VALUE Default Value: USE_GLOBAL_VALUE
nf-mediation.service.loadBalancer.addressPool	This is a mandatory parameter. To request the assignment of public IP from a specific IP pool using metallb.universe.tf/address-pool annotation to mediation service.	Data Type: String Range: NA Default Value: signaling1
nf-mediation.service.customExtension.labels	Optional field to configure service specific labels applicable to "Service" Resource Type.	Data Type: <string_label_1_key>:<string_label_1_value> <string_label_2_key>:<string_label_2_value> Range: K8s label object syntax Default Value: customExtension: labels:{} annotations: {}
nf-mediation.service.customExtension.annotations	Optional field to configure service specific annotations applicable to "Service" Resource Type.	Data Type: <string_annotation_1_key>:<string_annotation_1_value> <string_annotation_2_key>:<string_annotation_2_value> Range: K8s annotations object syntax Default Value: customExtension: labels:{} annotations: {}

Table 3-22 (Cont.) nf-mediation parameters

Parameter	Description	Details
`nf-mediation.deployment.customExtension.labels`	Optional field to configure service specific labels applicable to "Deployment" Resource Type.	Data Type: <string_label_1_key>:<string_label_1_value> <string_label_2_key>:<string_label_2_value> Range: K8s label object syntax Default Value: customExtension: labels:{} annotations: {}
`nf-mediation.deployment.customExtension.annotations`	Optional field to configure service specific annotations applicable to "Deployment" Resource Type.	Data Type: <string_annotation_1_key>:<string_annotation_1_value> <string_annotation_2_key>:<string_annotation_2_value> Range: K8s annotations object syntax Default Value: customExtension: labels:{} annotations: {}
`nf-mediation.sidecarPortExclusion.inBound`	This is an optional parameter. This is used to exclude ports on mediation microservice.	Data Type: integer Range: valid port value Default Value: 8091

mediationConfig

This section includes information about the mediation config parameters of the SEPP.

Table 3-23 mediationConfig parameters

Parameter	Description	Details
`mediationConfig.ruleApi.enabled`	This is a mandatory parameter This flag is used to enable or disable the CNC Console or REST API based rules configurations feature implementation. If the value is true, mediation microservice uses the rules from the CNC Console or REST APIs based rules setup. If the value is false, mediation microservice uses the rules from the config map based rules setup.	Data Type: boolean Range: NA Default Value: true

Table 3-23 (Cont.) mediationConfig parameters

Parameter	Description	Details
mediationConfig.idleTimeout	This is a mandatory parameter. This indicates the maximum duration that (milliseconds) a connection can be idle for (that is, without traffic of bytes in either direction).	Data Type: integer Range: NA Default Value: 720000 ms

3.1.18 coherence-svc

This section includes information about the coherence-svc parameters of the SEPP.

Table 3-24 coherence-svc

Parameter	Description	Details
coherence-svc.global.asm.serviceMeshCheck	This is a mandatory parameter. This flag is used to enable or disable ASM for all services. ASM setup: When serviceMeshCheck is enabled signature validation of certificate is skipped. There is no need to configure the certificate or the secret.	Data Type: boolean Range: True or False Default Value: false
coherence-svc.global.asm.istioSidecarQuitUrl	This is a mandatory parameter. This indicates the sidecar (istio quit url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Default Value: " "
coherence-svc.global.asm.istioSidecarReadyUrl	This is a mandatory parameter. This indicates the sidecar (istio ready url) when deployed in serviceMesh. Port should be modified envoy admin port.	Data Type: String Default Value: "http://127.0.0.1:15000/ready"
coherence-svc.replicaCount	This is a mandatory parameter. This indicates the maximum replicas to scale to maintain an average CPU utilisation	Data Type: Integer Default Value: 1
coherence-svc.clusterName	This is a mandatory parameter. Name of Cluster	Data Type: Integer Default Value: SEPPCoherenceCluster
coherence-svc.image.repository	This is a mandatory parameter. Repo location of image	Data Type: Integer Default Value: reg-1
coherence-svc.image.name	This is a mandatory parameter. Name of image	Data Type: String Default Value: ocsepp-coherence-svc
coherence-svc.image.tag	This is a mandatory parameter.Tag of image	Data Type: String Default Value: helm-tag

Table 3-24 (Cont.) coherence-svc

Parameter	Description	Details
coherence-svc.image.pullPolicy	This is a mandatory parameter. This setting indicates if the image needs to be pulled or not	Data Type: String Default Value: Always
coherence-svc.service.port	This is a mandatory parameter. This is the ocsepp-pn32f-cache-svc service Port number	Data Type: Integer Default Value: 9070
coherence-svc.service.actuatorPort	This is a mandatory parameter. ActuatorPort is used for prometheus port and probes.It Cannot be same as service port.	Data Type: Integer Default Value: 9090
coherence-svc.log.root	This is a mandatory parameter. This indicates the Root log level value	Data Type: String Default Value: ERROR
coherence-svc.log.sepp	This is a mandatory parameter. This indicates the SEPP specific log level	Data Type: String Default Value: ERROR
coherence-svc.resources.limits.ephemeralStorage	This is an optional parameter. This indicates the pods use ephemeral local storage for scratch space, caching, and logs.	Data Type: Integer Default Value: 1Gi
coherence-svc.resources.limits.cpu	This is a mandatory parameter. Resource Requirements(limit of cpu)	Data Type: Integer Default Value: 1
coherence-svc.resources.limits.memory	This is a mandatory parameter. Resource Requirements(limit of memory)	Data Type: String Default Value: 2Gi
coherence-svc.resources.requests.ephemeralStorage	This is an optional parameter. Pods and containers can require ephemeral storage for their operation.	Data Type: String Default Value: 78Mi
coherence-svc.resources.requests.cpu	This is a mandatory parameter. Resource Requirements(requested cpu)	Data Type: Integer Default Value: 1
coherence-svc.resources.requests.memory	This is a mandatory parameter. Resource Requirements(requested memory)	Data Type: String Default Value: 2Gi
coherence-svc.resources.target.averageCpuUtil	This is a mandatory parameter. Resource Requirements(avg cpu utilisation)	Data Type: Integer Default Value: 50
coherence-svc.coherence.port	This is a mandatory parameter. This is coherence service port number.	Data Type: Integer Default Value: 8070
service.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to coherence specific Services.	**Data Type**: String **Default Value**: null **Range**: NA

Table 3-24 (Cont.) coherence-svc

Parameter	Description	Details
`deployment.customExtension.labels`	This is an optional parameter. Custom Labels that needs to be added to coherence specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
`deployment.customExtension.annotations`	This is an optional parameter. Custom Annotations that needs to be added to coherence specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
`service.customExtension.labels`	This is an optional parameter. Custom Labels that needs to be added to coherence specific Service.	**Data Type**: String **Default Value**: null **Range**: NA

3.1.19 alternate-route service

This section includes information about the alternate-route service parameters of the SEPP.

Table 3-25 Alternate Route Service

Parameter	Description	Details
`alternate-route.logStorage`	This is an optional parameter. It is the sum of "50M Logging space requirement of infrastructure (based on kubectl configuration - default log file size if 10M and it maintains max 5 copies)" and "5Kb as infra space". resources.request.ephemeral-storage will be set as 110% of the sum (logStorage + crictlStorage)	**Data Type**: Integer **Default Value**: 70MB **Range**: NA
`alternate-route.crictlStorage`	This is an optional parameter. It is the disk space usage of a pod that can be collected by running the command crictl stats `` `crictl ps | grep dummy | cut -d" " -f1` `` in the node on which the pod is running. To know the pod details, run the `kubectl get pods -o wide` command. resources.request.ephemeral-storage will be set as 110% of the sum (logStorage + crictlStorage)	**Data Type**: Integer **Default Value**: 1MB **Range**: NA
`alternate-route.nodeSelection`	This is a mandatory parameter. Specifies whether Kubernetes assigns the alternate-route pod to the node that match with the specified node labels. If the value is set to USE_GLOBAL_VALUE, then the pod uses the configuration from `nodeSelection` parameter in the Global Parameters section. If the value is set to ENABLED, then the nodeSelector is applied to the deployments. If the value is set to DISABLED, then the nodeSelector is not applied to any deployments.	**Data Type**: String **Default Value**: USE_GLOBAL_VALUE **Range**: ENABLED, DISABLED, USE_GLOBAL_VALUE

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
`alternate-route.helmBasedConfigurationNodeSelectorApiVersion`	This is a mandatory parameter. Indicates the supported Node Selector API Version. **Note**: Only v1 is supported.	**Data Type**: String **Default Value**: v1 **Range**: NA
`alternate-route.nodeSelector.nodeKey`	This is a mandatory parameter. nodeSelector: Use this configuration to apply nodeSelector to Configuration service pods. nodeKey: Key of the node label. **Note**: This is a read-only parameter. It is configured only for config client.	**Data Type**: String **Default Value**: ' ' **Range**: NA
`alternate-route.nodeSelector.nodeValue`	This is a mandatory parameter. Indicates the value of the node label. **Note**: This is a read-only parameter. It is configured only for config client.	**Data Type**: String **Default Value**: "" **Range**: NA
`alternate-route.tolerationsSetting`	This is an optional parameter. Specifies whether Kubernetes assigns the toleration to the `alternate-route` pod. If the value is set to USE_GLOBAL_VALUE, then the pod uses the configuration from the `global.tolerations` parameter configured in the Global Parameters section. If the value is set to ENABLED, then the toleration is applied to the pod that is defined in the tolerations in the `alternate-route` pod. If the value is set to DISABLED, then the toleration is not applied to the pod that is defined in the tolerations in the `alternate-route` pod.	**Data Type**: String **Default Value**: USE_GLOBAL_VALUE **Range**: ENABLED, DISABLED, USE_GLOBAL_VALUE

`alternate-route.tolerations`	This is an optional parameter.
	Defines the toleration values. Following is an example to define the configuration:
	`tolerations:`
	`- key: "exampleKey"`
	`operator: "Equal"`
	`value: "value1"`
	`effect: "NoSchedule"`
		Data Type: String
		Default Value: []
		Range: NA

`alternate-route.maxUnavailable`	This is a mandatory parameter. Indicates the maximum allowed unavailable pods during pod disruption. This parameter uses the same value of the reference variable, `maxPdbUnavailable` present in the Global Parameters section. **Note**: By default the global configured value is used. The reference variable must be replaced with absolute value, in case the microservice value needs to be changed.	**Data Type**: String **Default Value**: *maxPdbUnavailableRef **Range**: NA

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
`alternate-route.deploymentDnsSrv.name`	This is an optional parameter. Indicates the full image path.	**Data Type**: String **Default Value**: alternate_route **Range**: NA
`alternate-route.deploymentDnsSrv.tag`	This is an optional parameter. Indicates the tag image in docker repository. This parameter uses the same value of the reference variable, `gwTag` present in the Global Parameters section. **Note**: This is a read-only parameter and must not be changed.	**Data Type**: String **Default Value**: *gwTagRef **Range**: NA
`alternate-route.deploymentDnsSrv.pullPolicy`	This is an optional parameter. Indicates if the image need to be pulled. This parameter uses the same value of the reference variable, `imagePullPolicy` present in the Global Parameters section. **Note**: This is a read-only parameter and must not be changed.	**Data Type**: String **Default Value**: *imagePullPolicyRef **Range**: Always, IfNotPresent, Never
`alternate-route.dbHookImage.name`	This is an optional parameter. Indicates the common configuration hook image.	**Data Type**: String **Default Value**: common_config_hook **Range**: NA
`alternate-route.dbHookImage.tag`	This is an optional parameter. Indicates the common configuration hook image tag. This parameter uses the same value of the reference variable, `gwTag` present in the Global Parameters section. **Note**: This is a read-only parameter and must not be changed.	**Data Type**: String **Default Value**: *gwTagRef **Range**: NA
`alternate-route.dbHookImage.pullPolicy`	This is an optional parameter. Indicates the common configuration hook image pull policy. **Note**: This is a read-only parameter and must not be changed.	**Data Type**: String **Default Value**: *imagePullPolicyRef **Range**: NA
`alternate-route.minAvailable`	This is an optional parameter. Indicates the number of pods must always be available, even during a disruption.	**Data Type**: Integer **Default Value**: 2 **Range**: NA
`alternate-route.minReplicas`	This is an optional parameter. Indicates the minimum number of pods that will be deployed.	**Data Type**: Integer **Default Value**: 2 **Range**: NA
`alternate-route.maxReplicas`	This is an optional parameter. Indicates the maximum number of pods that will be scaled up.	**Data Type**: Integer **Default Value**: 2 **Range**: NA

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
alternate-route.startupProbe.initialDelaySeconds	This is an optional parameter. Indicates the configurable wait time (in seconds) before performing the first readiness probe by Kubelet. **Note**: Do not change the default value. If you see delays in pod to come up and probe is killing the pod then you must tune these parameters.	**Data Type**: Integer **Default Value**: 30 **Range**: NA
alternate-route.startupProbe.periodSeconds	This is an optional parameter. Indicates the time interval (in seconds) for every readiness probe check. **Note**: Do not change the default value. If you see delays in pod to come up and probe is killing the pod then you must tune these parameters.	**Data Type**: Integer **Default Value**: 10 **Range**: NA
alternate-route.startupProbe.timeoutSeconds	This is an optional parameter. Indicates the number of seconds after which the probe times out. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 15 **Range**: NA
alternate-route.startupProbe.successThreshold	This is an optional parameter. Indicates the minimum consecutive successes for the probe to be considered successful after having failed. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 1 **Range**: NA
alternate-route.startupProbe.failureThreshold	This is an optional parameter. When a pod starts and the probe fails, Kubernetes indicates failure threshold time before giving up. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 6 **Range**: NA
alternate-route.readinessProbe.initialDelaySeconds	This is an optional parameter. Indicates the configurable wait time (in seconds) before performing the first readiness probe by Kubelet. **Note**: Do not change the default value. If you see delays in pod to come up and probe is killing the pod then you must tune these parameters.	**Data Type**: Integer **Default Value**: 30 **Range**: NA
alternate-route.readinessProbe.periodSeconds	This is an optional parameter. Indicates the time interval (in seconds) for every readiness probe check. **Note**: Do not change the default value. If you see delays in pod to come up and probe is killing the pod then you must tune these parameters.	**Data Type**: Integer **Default Value**: 10 **Range**: NA
alternate-route.readinessProbe.timeoutSeconds	This is an optional parameter. Indicates the number of seconds after which the probe times out. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 15 **Range**: NA
alternate-route.readinessProbe.successThreshold	This is an optional parameter. Indicates the minimum consecutive successes for the probe to be considered successful after having failed. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 1 **Range**: NA

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
`alternate-route.readinessProbe.failureThreshold`	This is an optional parameter. When a pod starts and the probe fails, Kubernetes indicates failure threshold time before giving up. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 3 **Range**: NA
`alternate-route.livenessProbe.initialDelaySeconds`	This is an optional parameter. Indicates the configurable wait time (in seconds) before performing first liveness probe by Kubelet. **Note**: Do not change the default value. If you see delays in pod to come up and probe is killing the pod then you must tune these parameters.	**Data Type**: Integer **Default Value**: 30 **Range**: NA
`alternate-route.livenessProbe.periodSeconds`	This is an optional parameter. Indicates the time interval ((in seconds) for every liveness probe check. **Note**: Do not change the default value. If you see delays in pod to come up and probe is killing the pod then you must tune these parameters.	**Data Type**: Integer **Default Value**: 15 **Range**: NA
`alternate-route.livenessProbe.timeoutSeconds`	This is an optional parameter. Indicates the number of seconds after which the probe times out. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 15 **Range**: NA
`alternate-route.livenessProbe.successThreshold`	This is an optional parameter. Indicates the minimum consecutive successes for the probe to be considered successful after having failed. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 1 **Range**: NA
`alternate-route.livenessProbe.failureThreshold`	This is an optional parameter. When a pod starts and the probe fails, Kubernetes tries failure threshold times before giving up. **Note**: Do not change the default value.	**Data Type**: Integer **Default Value**: 3 **Range**: NA
`alternate-route.dbConfig.dbHost`	This is a mandatory parameter. Indicates the hostname of database connection in which the common configuration must be stored. This is the MySQL primary DB connection service IP or hostname (`mysql.primary.host`) present in the Global Parameters section.	**Data Type**: String **Default Value**: *mySqlHostRef **Range**: NA
`alternate-route.dbConfig.dbPort`	This is a mandatory parameter. Indicates the port of database connection. This is the MySQL primary DB connection service port (`mysql.primary.port`) present in the Global Parameters section.	**Data Type**: String **Default Value**: *mySqlPortRef **Range**: NA
`alternate-route.dbConfig.secretName`	This is a mandatory parameter. Indicates the secret name from which the DB name, DB password and db user name is picked for common configuration. This is the privileged user secret name used by DB hooks for creating tables (`database.privilegedUserSecretName`) present in the Global Parameters section.	**Data Type**: String **Default Value**: *privilegedSecretNameRef **Range**: NA

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
`alternate-route.dbConfig.dbName`	This is a mandatory parameter. Indicates the name of common configuration database. This is the database name to be used for common configuration (`database.commonConfigDbName`) present in the Global Parameters section.	**Data Type**: String **Default Value**: *dbNameRef **Range**: NA
`alternate-route.dbConfig.dbEngine`	This is a mandatory parameter. Defines the MySQL engine that is used to store information in the MySQL database.	Data Type: String Range: NDBCLUSTER or InnoDB Default Value: NDBCLUSTER Note: NDBCLUTER must be used when using cnDBTier.
`alternate-route.staticVirtualFqdns.name`	This is an optional parameter. Indicates the name of the virtual FQDN or FQDN.	**Data Type**: String **Default Value**: NA **Range**: NA
`alternate-route.staticVirtualFqdns.alternateFqdns.target`	This is a mandatory parameter, if "`alternate-route.staticVirtualFqdns.name`" is defined. Indicates the name of the alternate FQDN mapped to above virtual FQDN.	**Data Type**: String **Default Value**: NA **Range**: NA
`alternate-route.staticVirtualFqdns.alternateFqdns.port`	This is a mandatory parameter, if "`alternate-route.staticVirtualFqdns.name`" is defined. Indicates the port of the alternate FQDN.	**Data Type**: Integer **Default Value**: 5060 **Range**: NA
`alternate-route.staticVirtualFqdns.alternateFqdns.priority`	This is a mandatory parameter, if "`alternate-route.staticVirtualFqdns.name`" is defined. Indicates the priority of the alternate FQDN.	**Data Type**: Integer **Default Value**: 10 **Range**: NA
`alternate-route.dnsSrvEnabled`	This is an optional parameter. Indicates the attribute to enable or disable the DNS-SRV query to DNS Server.	**Data Type**: Boolean **Default Value**: true **Range**: false, true
`alternate-route.dnsSrvFqdnSetting.enabled`	This is an optional parameter. Indicates the flag to enable the usage of custom patterns for the FQDN while triggering DNS-SRV query.	**Data Type**: Boolean **Default Value**: false **Range**: false, true
`alternate-route.dnsSrvFqdnSetting.pattern`	This is an optional parameter. Indicates the pattern of the FQDN used to format the incoming FQDN and Scheme while triggering the DNS-SRV query. • The value must be in sync with the format used for configuring FQDN's of SRV records in DNS. • If the flag "`dnsSrvFqdnSetting.enabled`" is set to false, then the default value is used for forming the FQDN while sending a DNS-SRV query to DNS. This default value is in accordance with the standards of DNS-SRV. It is recommended that this pattern must be used for configuring the SRV records in DNS.	**Data Type**: String **Default Value**: "_{scheme}._tcp.{fqdn}." **Range**: NA

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
alternate-route.resources.limits.cpu	This is an optional parameter. Indicates the maximum amount of CPU that Kubernetes will allow the nrfconfiguration service container to use. It is the maximum CPU resource allocated to nrfconfiguration deployment.	**Data Type**: Integer **Default Value**: 2 **Range**: NA
alternate-route.resources.limits.commonHooksCpu	This is an optional parameter. Indicates the maximum amount of CPU that Kubernetes will allow the common hooks container to use.	**Data Type**: Integer **Default Value**: 1 **Range**: NA
alternate-route.resources.limits.memory	This is an optional parameter. Indicates the maximum memory that Kubernetes will allow the nrfconfiguration service container to use. It is the maximum memory allocated to nrfconfiguration deployment.	**Data Type**: Integer **Default Value**: 4Gi **Range**: NA
alternate-route.resources.limits.commonHooksMemory	This is an optional parameter. Indicates the maximum amount of memory that Kubernetes will allow the common hooks container to use.	**Data Type**: Integer **Default Value**: 1Gi **Range**: NA
alternate-route.resources.requests.cpu	This is an optional parameter. Indicates the amount of CPU that the system will guarantee for the nrfconfiguration service container, and Kubernetes will use this value to decide on which node to place the pod. It is the maximum CPU resource allocated to nrfconfiguration deployment.	**Data Type**: Integer **Default Value**: 2 **Range**: NA
alternate-route.resources.requests.memory	This is an optional parameter. Indicates the memory that the system will guarantee for the nrfconfiguration, Kubernetes will use this value to decide on which node to place the pod. It is the maximum memory for requests allocated to nrfconfiguration deployment.	**Data Type**: Integer **Default Value**: 2Gi **Range**: NA
alternate-route.resources.target.averageCpuUtil	This is an optional parameter. Indicates the target CPU utilization after which Horizontal Pod Autoscaler will be triggered.	**Data Type**: Integer **Default Value**: 80 **Range**: NA
alternate-route.gracePeriodSeconds	This is a mandatory parameter. It is the grace period for pod to wait for inflight requests to be completed. If there are no inflight requests, then this period is ignored. If there are pending requests even after this period is elapsed, then the pod will be forcefully shutdown. **Unit**: seconds.	**Data Type**: Integer **Default Value**: 60 **Range**: NA
alternateRouteServiceEnable	This is a mandatory parameter. This parameter is used to enable the deployment for alternate-route-service.	Data Type: Boolean Range: True or False Default Value: False
dnsSrvFqdnSetting.enabled	This is an optional parameter. This parameter is used to enable or disable the usage of custom patterns for the FQDN while triggering DNS-SRV query.	Data Type: Boolean Range: True or False Default Value: True

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
dnsSrvFqdnSetting.pattern	This is an optional parameter. This parameter is the default custom pattern for DNS SRV record to be resolved.	Data Type: String Default Value: _{scheme}._tcp.{fqdn}.
dnsSrvEnabled	This is a mandatory parameter. This parameter is used to enable the sending of DNS SRV queries to core-dns.	Data Type: Boolean Range: True or False Default Value: True
ports.actuatorPort	This is a Mandatory parameter (for ASM and non ASM Setups). ActuatorPort is used for prometheus port and probes. It cannot be same as service port.	Data Type: Integer Range: NA Default Value: 9094
service.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to alternate-route specific Service.	**Data Type**: String **Default Value**: null **Range**: NA
service.customExtension.anotations	This is an optional parameter. Custom Annotations that needs to be added to alternate-route specific Services.	**Data Type**: String **Default Value**: null **Range**: NA
deployment.customExtension.labels	This is an optional parameter. Custom Labels that needs to be added to alternate-route specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
deployment.customExtension.annotations	This is an optional parameter. Custom Annotations that needs to be added to alternate-route specific Deployment.	**Data Type**: String **Default Value**: null **Range**: NA
enablePodSecurityContext	This is a mandatory parameter. Enables security context for pod.	Data Type: Boolean Range: True or False Default Value: True
podSecurityContext.runAsNonRoot	This is a mandatory parameter. Prevents pod from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
podSecurityContext.runAsUser	This is a mandatory parameter. Specifies that all processes in pod must run with the provided user ID.	Data Type: Integer Default Value: 10001
securityContext.enable	This is a mandatory parameter. Enables security context for containers.	Data Type: Boolean Range: True or False Default Value: True
containerSecurityContext.readOnlyRootFilesystem	This is a mandatory parameter. Mounts the mediation container's root filesystem as read-only.	Data Type: Boolean Range: True or False Default Value: True

Table 3-25 (Cont.) Alternate Route Service

Parameter	Description	Details
containerSecurityContext.allowPrivilegeEscalation	This is a mandatory parameter. Controls if a process can obtain more privileges than its primary process. This boolean data type controls whether the no_new_privs parameter gets configured on the container process. allowPrivilegeEscalation is always set to true when the container: • is run as privileged • has CAP_SYS_ADMIN	Data Type: Boolean Range: True or False Default Value: False
containerSecurityContext.runAsNonRoot	This is a mandatory parameter. Prevents containers from starting as root user.	Data Type: Boolean Range: True or False Default Value: True
containerSecurityContext.privileged	This is a mandatory parameter. Provides containers' access to the host's resources and kernel capabilities.	Data Type: Boolean Range: True or False Default Value: False
containerSecurityContext.runAsUser	This is a mandatory parameter. Specifies that for any container in the pod, all processes must run with the provided user ID.	Data Type: Integer Range: Valid IDs for security context for user Default Value: 10001
containerSecurityContext.capabilities.drop	This is a mandatory parameter. Manages Linux capabilities for containers. Using Linux capabilities, you can grant certain privileges to a process without granting all the privileges of the root user.	Data Type: List of strings Range: Valid Linux capabilities Default Value: -all

3.1.20 Timer Parameters

The following is the consolidated list of SEPP Timer Parameters:

PN32F

Table 3-26 PN32F

Parameter Name	Description	Default Value	Data Type
cacheRefreshTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database.	30,000 (ms)	Integer
cacheRefreshInitTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database at Init time.	5000 (ms)	Integer

Table 3-26 (Cont.) PN32F

Parameter Name	Description	Default Value	Data Type
securityCacheRefreshTimeout	This is a mandatory parameter (If Security Countermeasure feature is enabled). Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration.	30,000 (ms)	Integer
securityCacheRefreshInitTimeout	This is a mandatory parameter (If Security Countermeasure feature is enabled). Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration at the Init time when Application comes up.	50,000 (ms)	Integer
topologyhidingCacheRefreshTimeout	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration.	30,000 (ms)	Integer
topologyhidingCacheRefreshInitTimeout	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration at the Init time when Application comes up.	50,000 (ms)	Integer

Table 3-26 (Cont.) PN32F

Parameter Name	Description	Default Value	Data Type
topologyhidingHistoryUpdateTimeout	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. This is the Time for the old entries to be removed from cache. Entries older than topologyhidingHistoryRefreshSeconds are purged.	30,000 (ms)	Integer
topologyhidingHistoryRefreshSeconds	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. This value represents the Time until old Topology Hiding feature entries are kept in cache.	60 (sec)	Integer
connectionTimeout	This is a mandatory parameter. This is Jetty Client Settings. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	60 (ms)	Integer
dnsRefreshDelay	This is a mandatory parameter. This is Jetty Client Settings. This value represents the Time taken to refresh the DNS entries for a destination	10,000 (ms)	Integer

Table 3-26 (Cont.) PN32F

Parameter Name	Description	Default Value	Data Type
requestTimeout	This is a mandatory parameter. This is Jetty Client Settings. Request timeout is the maximum time that can be taken to process HTTP request after the connection is established. Sum of time to process request plus ConnectionTimeout and should always be greater than Connection Timeout.	1100 (ms)	Integer
mediationRequestTimeout	This is a mandatory parameter (If Mediation feature is enabled). Time to wait for the response from mediation microservice.	400 (ms)	Integer
nrfDiscoveryCacheRefreshTimeout	This is a mandatory parameter (If Cat 3 - Previous Location Check feature is enabled). This parameter defines the timer value when UDR Discovery request will be triggered if coherence map containing UDR Profile information is empty. After this timer expiry, UDR Discovery request will be initiated by NRF Client towards NRF.	30000 (ms) Note: In ATS setup, set the value as 10.	Integer
nrfDiscoveryCacheRefreshInitTimeout	This is a mandatory parameter (If Cat 3 - Previous Location Check feature is enabled). This parameter defines the timer value after which UDR Discovery request will be triggered at SEPP INIT Time. After this timer expiry, UDR Discovery request will be initiated by NRF Client towards NRF.	5000 (ms)	Integer

Table 3-26 (Cont.) PN32F

Parameter Name	Description	Default Value	Data Type
evictSanHeaderCacheDelay	This is a mandatory parameter. This parameter defines the timer value after which San Header Cache gets cleared out and updated with new N32F Context (if added).	50000 (ms) Note: In ATS setup, set the value as 100.	Integer
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	30000 ms	Integer

CN32F

Table 3-27 CN32F

Parameter Name	Description	Default Value	Data Type
cacheRefreshTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database.	30,000 (ms)	Integer
cacheRefreshInitTimeout	This is a mandatory parameter. Timeout configured for updating PN32F cache with N32F Context details present in SEPP database at Init time.	5000 (ms)	Integer
securityCacheRefreshTimeout	This is a mandatory parameter (If Security Countermeasure feature is enabled). Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration.	30,000 (ms)	Integer

Table 3-27 (Cont.) CN32F

Parameter Name	Description	Default Value	Data Type
`securityCacheRefreshInitTimeout`	This is a mandatory parameter (If Security Countermeasure feature is enabled). Timeout configured for updating PN32F cache with SEPP Features details for loading their Database configuration at the Init time when Application comes up.	50,000 (ms)	Integer
`topologyhidingCacheRefreshTimeout`	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration.	30,000 (ms)	Integer
`topologyhidingCacheRefreshInitTimeout`	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. Timeout configured for updating PN32F cache with Topology Hiding feature configuration for loading their Database configuration at the Init time when Application comes up.	50,000 (ms)	Integer
`topologyhidingHistoryUpdateTimeout`	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. This is the Time for the old entries to be removed from cache. Entries older than topologyhidingHistoryRefreshSeconds are purged.	30,000 (ms)	Integer

Table 3-27 (Cont.) CN32F

Parameter Name	Description	Default Value	Data Type
topologyhidingHistoryRefreshSeconds	This is a mandatory parameter (If Topology hiding feature is enabled). This is Topology Hiding Settings. This value represents the Time until old Topology Hiding feature entries are kept in cache.	60 (sec)	Integer
connectionTimeout	This is a mandatory parameter. This is Jetty Client Settings. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	60 (ms)	Integer
dnsRefreshDelay	This is a mandatory parameter. This is Jetty Client Settings. This value represents the Time taken to refresh the DNS entries for a destination	10,000 (ms)	Integer
requestTimeout	This is a mandatory parameter This is Jetty Client Settings. Request timeout is the maximum time that can be taken to process HTTP request after the connection is established. Sum of time to process request plus ConnectionTimeout and should always be greater than Connection Timeout.	.	Integer
mediationRequestTimeout	This is a mandatory parameter (If Mediation feature is enabled). Time to wait for the response from mediation microservice.	900 (ms)	Integer

Table 3-27 (Cont.) CN32F

Parameter Name	Description	Default Value	Data Type
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	30000 ms	Integer

Update DB

Table 3-28 Update DB

Parameter Name	Description	Default Value	Data Type
customAlertExpiryDuration	This is a mandatory parameter (applicable only when customAlertExpiryEnabled is set to true). This timer indicates, alert expiry occurs according to resolve_timeout value of AlertManager and upgrade/rollback hooks shall clear the alerts as applicable. If it is set to true, auto alert clear shall occur after customAlertExpiryDuration value and upgrade/rollback hooks may not clear the alerts. The custom duration (in minutes) post which Alert gets auto cleared, applicable only when customAlertExpiryEnabled is set to true	60 (Min)	Integer

NRF Client

Table 3-29 NRF Client

Parameter Name	Description	Default Value	Data Type
`nrf-client-nfdiscovery.commonCfgServer.pollingInterval`	This is a mandatory parameter (applicable only when commonCfgClient.enabled is set to true). The interval at which the discovery service shall poll the configuration service to check for updates in ms This attribute shall be configured only if commonCfgClient.enabled is set to true.	5000 (ms)	Integer
`nrf-client-nfmanagement.commonCfgServer.pollingInterval`	This is a mandatory parameter (applicable only when commonCfgClient.enabled is set to true). The interval at which the management service shall poll the configuration service to check for updates in ms This attribute shall be configured only if commonCfgClient.enabled is set to true.	5000 (ms)	Integer

App Info

Table 3-30 App Info

Parameter Name	Description	Default Value	Data Type
`commonCfgServer.pollingInterval`	This is a mandatory parameter (applicable only when commonCfgClient.enabled is set to true). This is the interval between two subsequent polling requests from config client to server	5000 (ms)	Integer

Table 3-30 (Cont.) App Info

Parameter Name	Description	Default Value	Data Type
commonCfgServer.connectionTimeout	This is a mandatory parameter (applicable only when commonCfgClient.enabled is set to true). This is the limit for connection to be established between config client and server	10000 (ms)	Integer

Perf Info

Table 3-31 Perf Info

Parameter Name	Description	Default Value	Data Type
commonCfgServer.pollingInterval	This is a mandatory parameter (Applicable only if commonCfgClient.enabled is set to true). This is the interval between two subsequent polling requests from config client toserver	5000 (ms)	Integer
commonCfgServer.connectionTimeout	This is a mandatory parameter (Applicable only if commonCfgClient.enabled is set to true). This is the limit for connection to be established between config client and server	10000 (ms)	Integer

Config Manager Service

Table 3-32 Config Manager Service

Parameter Name	Description	Default Value	Data Type
readinessProbe.initialDelaySeconds	This is a mandatory parameter. This value Tells the kubelet that it should wait second before performing the first probe. Probes start running after initialDelaySeconds after container is started.	30 (sec)	Integer

Table 3-32 (Cont.) Config Manager Service

Parameter Name	Description	Default Value	Data Type
readinessProbe.timeoutSeconds	This is a mandatory parameter. This value tells the Number of seconds after which the probe times out.	3 (sec)	Integer
readinessProbe.periodSeconds	This is a mandatory parameter. This value specifies that the kubelet should perform a liveness probe every xx seconds.	10 (sec)	Integer
livenessProbe.initialDelaySeconds	This is a mandatory parameter. This value tells the kubelet that it should wait second before performing the first probe.	180 (sec)	Integer
livenessProbe.timeoutSeconds	This is a mandatory parameter. Number of seconds after which the probe times out.	3 (sec)	Integer
livenessProbe.periodSeconds	This is a mandatory parameter. This value specifies that the kubelet should perform a liveness probe every xx seconds.	15 (sec)	Integer
dbCheckRefreshTimeout	This is a mandatory parameter. This value represents time interval that checks whether Database connectivity with Service is healthy or not.	30000 ms	Integer

Mediation

Table 3-33 Mediation

Parameter Name	Description	Default Value	Data Type
commonCPJCConnectTimeout	This is a conditional parameter. This is one of the common jetty client parameter. This is the limit for connection to be established between client and server.	10000	Integer
commonCPJCRrequestTimeout	This is a conditional parameter. This is one of the common jetty client parameter. This is the limit for the configuration for request timeout	10000	Integer
commonCPJCDNSRefreshDelay	This is a conditional parameter. This is one of the common jetty client parameter. This is the value for DNS Refresh Delay.	15000	Integer
commonCPJCPingDelayDuration	This is a conditional parameter. This is one of the common jetty client parameter. This is the value for Ping delay duration.	0	Integer
downstream.idleTimeout	This is a mandatory parameter. The Idle Timeout setting in the TCP profile specifies the length of time that a connection is idle before the connection is eligible for deletion. If no traffic flow is detected within the idle session timeout, the session will be deleted. This timer is for jetty client.	600000 (sec)	Integer
downstream.tcpKeepalive.interval	This is a mandatory parameter. Used to adjust the frequency at which TCP Keep-Alive packets are sent to a remote host for connection validation	500 (sec)	Integer

Table 3-33 (Cont.) Mediation

Parameter Name	Description	Default Value	Data Type
downstream.tcpKeepalive.time	This is a mandatory parameter. The Keep Alive Interval setting is used to adjust the frequency at which TCP Keep-Alive packets are sent to a remote host for connection validation.	1000 (sec)	Integer

PLMN Egress Gateway

Table 3-34 PLMN Egress Gateway

Parameter Name	Description	Default Value	Data Type
connectionTimeout	This is an optional parameter. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	60 (ms)	Integer
requestTimeout	This is an optional parameter. The configuration for request timeout for the call from Egress Gateway to the producer NF.	1000 (ms)	Integer
gracefulCloseDelay	This is a mandatory parameter. gracefulCloseDelay value should be positive value greater than requestTimeout and lesser than jettyIdleTimeout. # if gracefulCloseDelay is set to 0 then default value of 30000 ms will be considered internally	2000 (ms)	Integer
dnsRefreshDelay	This is an optional parameter. This is Jetty Client Settings. This value represents the Time taken to refresh the DNS entries for a destination	10000 (ms)	Integer

Table 3-34 (Cont.) PLMN Egress Gateway

Parameter Name	Description	Default Value	Data Type
gracefulShutdown.gracePeriod	This is an optional parameter. Grace period to wait for active requests to be executed. If there are no active requests then this period is neglected. 's' in case of seconds and 'm' in case of minutes	1 (min)	Integer
jettyIdleTimeout	This is a mandatory parameter. Used for clearing out idle connections on Jetty Client. Note: Jetty Idle timeout provides a waiting period before cleaning up the TCP socket when the client has sent a GOAWAY but the server never responded with GOAWAY. It is recommended that all NFs must set Jetty Idle timeout to a non-zero value to be resilient to bad peers that do not respond to a GOAWAY.	-1	Integer
nettyIdleTimeout	This is a mandatory parameter. Netty server Idle Timeout value.	120000000 ms	Integer

PLMN Ingress Gateway

Table 3-35 PLMN Ingress Gateway

Parameter Name	Description	Default Value	Data Type
ingressServer.keepAlive.idleTime	This is an optional parameter. Time after which keep alive will be tried after successful response from the peer.	180 Sec	Integer
ingressServer.keepAlive.interval	This is an optional parameter. The interval after which it should retry in case of failure.	60 Sec	Integer

Table 3-35 (Cont.) PLMN Ingress Gateway

Parameter Name	Description	Default Value	Data Type
routesConfig.metadata.requestTimeout	This is a mandatory parameter. requestTimeout is used to set timeout at route level. Value should be in milliseconds.	2600 ms	Integer
routesConfig.metadata.requiredTime	This is a mandatory parameter (Applicable only if isSbiTimerEnabled is true). requiredTime is minimum time below which request will be rejected if isSbiTimerEnabled is true. Value should be in milliseconds.	3000 ms	Integer
dnsRefreshDelay	This is an optional parameter. This value represents the Time taken to refresh the DNS entries for a destination	120000 (ms)	Integer
globalIngressRateLimiting.duration	This is a mandatory parameter (Applicable only if globalIngressRateLimiting.enabled is true). Iterations of time duration(In seconds) for which bucketCapacity and refillRate are reset.	1 (Sec)	Integer
gracefulShutdown.gracePeriod	This is an optional parameter. Grace period to wait for active requests to be executed. If there are no active requests then this period is neglected # 's' in case of seconds and 'm' in case of minutes	1 min	Integer

Table 3-35 (Cont.) PLMN Ingress Gateway

Parameter Name	Description	Default Value	Data Type
commonCfgServer.pollingInterval	This is a mandatory parameter (Applicable only if commonCfgClient.enabled is set to true). This is the interval between two subsequent polling requests from config client to server	5000	Integer
connectionTimeout	This is a mandatory parameter. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	60 ms	Integer
jettyIdleTimeout	This is a mandatory parameter. Used for clearing out idle connections on Jetty Client Note: Jetty Idle timeout provides a waiting period before cleaning up the TCP socket when the client has sent a GOAWAY but the server never responded with GOAWAY. It is recommended that all NFs must set Jetty Idle timeout to a non-zero value to be resilient to bad peers that do not respond to a GOAWAY.	-1	Integer
nettyIdleTimeout	This is a mandatory parameter. Netty server Idle Timeout value	120000000 ms	Integer

N32 Egress Gateway

Table 3-36 N32 Egress Gateway

Parameter Name	Description	Default Value	Data Type
dnsRefreshDelay	This is an optional parameter. This value represents the Time taken to refresh the DNS entries for a destination.	10000 (ms)	Integer
connectionTimeout	This is an optional parameter. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	60 (ms)	Integer
requestTimeout	This is an optional parameter. The configuration for request timeout for the call from Egress Gateway to the producer NF.	1500 (ms)	Integer
gracefulCloseDelay	This is a mandatory parameter. gracefulCloseDelay value should be positive value greater than requestTimeout and lesser than jettyIdleTimeout. If gracefulCloseDelay is set to 0 then default value of 30000 ms will be considered internally	2000 (ms)	Integer
gracefulShutdown.gracePeriod	This is an optional parameter. Grace period to wait for active requests to be executed. If there are no active requests then this period is neglected. 's' in case of seconds and 'm' in case of minutes	1 min	Integer
sepp.removeUnusedProxyAfter	This is an optional parameter (If not added, default value is picked). Time in minutes after which unused proxy beans are removed	30 (min)	Integer

Table 3-36 (Cont.) N32 Egress Gateway

Parameter Name	Description	Default Value	Data Type
jettyIdleTimeout	This is a mandatory parameter. Used for clearing out idle connections on Jetty Client Note: Jetty Idle timeout provides a waiting period before cleaning up the TCP socket when the client has sent a GOAWAY but the server never responded with GOAWAY. It is recommended that all NFs must set Jetty Idle timeout to a non-zero value to be resilient to bad peers that do not respond to a GOAWAY.	-1	Integer
nettyIdleTimeout	This is a mandatory parameter. Netty server Idle Timeout value	120000000 ms	Integer

N32 Ingress Gateway

Table 3-37 N32 Ingress Gateway

Parameter Name	Description	Default Value	Data Type
ingressServer.keepAlive.idleTime	This is an optional parameter. Time after which keep alive will be tried after successful response from the peer	180 (ms)	Integer
ingressServer.keepAlive.interval	This is an optional parameter. The interval after which it should retry in case of failure	60 sec	Integer
routesConfig.metadata.requestTimeout	This is a mandatory parameter. requestTimeout is used to set timeout at route level. Value should be in milliseconds.	1200 ms	Integer

Table 3-37 (Cont.) N32 Ingress Gateway

Parameter Name	Description	Default Value	Data Type
routesConfig.metadata.requiredTime	This is a mandatory parameter (Applicable only if isSbiTimerEnabled is set to true). requiredTime is minimum time below which request will be rejected if isSbiTimerEnabled is true. Value should be in milliseconds.	3000	Integer
commonCfgServer.pollingInterval	This is a mandatory parameter (Applicable only if commonCfgClient.enabled is set to true). This is the interval between two subsequent polling requests from config client to server	5000	Integer
dnsRefreshDelay	This is an optional parameter. Dns Refresh Delay in milli-seconds	120000 (ms)	Integer
globalIngressRateLimiting.duration	This is a mandatory parameter (Applicable only if globalIngressRateLimiting.enabled). Iterations of time duration(In seconds) for which bucketCapacity and refillRate are reset.	1 (Sec)	Integer
gracefulShutdown.gracePeriod	This is an optional parameter. Grace period to wait for active requests to be executed # If there are no active requests then this period is neglected	1 (min)	Integer
connectionTimeout	This is an optional parameter. This value represents connectTimeout the max time, in milliseconds, a connection can take to connect to destinations. Zero value means infinite timeout.	60 (ms)	Integer

Table 3-37 (Cont.) N32 Ingress Gateway

Parameter Name	Description	Default Value	Data Type
jettyIdleTimeout	This is a mandatory parameter. Used for clearing out idle connections on Jetty Client Note: Jetty Idle timeout provides a waiting period before cleaning up the TCP socket when the client has sent a GOAWAY but the server never responded with GOAWAY. It is recommended that all NFs must set Jetty Idle timeout to a non-zero value to be resilient to bad peers that do not respond to a GOAWAY.	-1	Integer
nettyIdleTimeout	This is a mandatory parameter. Netty server Idle Timeout value	120000000 ms	Integer

Global Parameters

Table 3-38 Global Parameters

Parameter Name	Description	Default Value	Data Type
retryInterval	This is a mandatory parameter. Retry interval	300000 (ms)	Integer
altServiceReqTimeout	This is a mandatory parameter. alternate route service http request timeout value.	3000 (ms)	Integer
altServiceLookupInterval	This is a mandatory parameter. alternate route service lookup interval.	3000 (ms)	Integer
test.config.timeout	This is a mandatory parameter. Estimated total time required for SEPP deployment and helm test command completion.	180 (Sec)	Integer

Table 3-38 (Cont.) Global Parameters

Parameter Name	Description	Default Value	Data Type
`atsSpecificTimeouts.n32fCacheRefreshTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets the following timeout values for cn32f and pn32f microservice of SEPP: • cacheRefreshTimeout • securityCacheRefreshTimeout • topologyhidingCacheRefreshTimeout • nrfDiscoveryCacheRefreshTimeout	1000	Integer
`atsSpecificTimeouts.n32fRequestTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets requestTimeout for cn32f and pn32f microservices of SEPP.	2000	Integer
`atsSpecificTimeouts.egwRequestTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets requestTimeout for n32-egress-gateway and plmn-egress-gateway microservices of SEPP.	2000	Integer
`atsSpecificTimeouts.igwRequestTimeout`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets requestTimeout for n32-ingress-gateway microservice of SEPP.	5000	Integer
`atsSpecificTimeouts.pn32fEvictSanHeaderCacheDelay`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets evictSanHeaderCacheDelay for pn32f microservice of SEPP.	100	Integer

Table 3-38 (Cont.) Global Parameters

Parameter Name	Description	Default Value	Data Type
`atsSpecificTimeouts.configMgrEgwRerouteAttempts`	This is a mandatory parameter (if `atsSpecificDeployment` is set to true). This parameter sets sbiRoutingErrorActionSets attempts of config-mgr service in case of alternate routing.	3	Integer

3.1.21 SEPP Configurable Parameters for OCI Deployment

This section includes information about the SEPP configurable parameters for OCI deployment.

Table 3-39 SEPP Configurable Parameters for OCI Deployment

Parameter	Description	Details
`openTelemetry.jaeger.collector.httpHost`	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: occne-tracer-jaeger-collector.occne-infra
`n32-ingress-gateway.openTelemetry.jaeger.httpExporter.host`	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
`n32-egress-gateway.openTelemetry.jaeger.httpExporter.host`	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
`plmn-ingress-gateway.openTelemetry.jaeger.httpExporter.host`	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
`plmn-egress-gateway.openTelemetry.jaeger.httpExporter.host`	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
`alternate-route.openTelemetry.jaeger.httpExporter.host`	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
`pn32f-svc.openTelemetry.jaeger.httpExporter.host`	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra

Table 3-39 (Cont.) SEPP Configurable Parameters for OCI Deployment

Parameter	Description	Details
cn32f-svc.openTelemetry.jaeger.httpExporter.host	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
cn32c-svc.openTelemetry.jaeger.httpExporter.host	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
pn32c-svc.openTelemetry.jaeger.httpExporter.host	This is an optional parameter. openTelemetry host.	Data Type: String Range: NA Default Value: jaeger-collector.cne-infra
cn32c-svc.openTelemetry.jaeger.httpExporter.port	This is an optional parameter. openTelemetry port.	Data Type: Integer Range: NA Default Value: 4318
cn32c-svc.openTelemetry.jaeger.logSpans	This is an optional parameter. openTelemetry logspans.	Data Type: boolean Range: true or false Default Value: false
cn32c-svc.openTelemetry.jaeger.probabilisticSamplingRate	This is an optional parameter. Trace capture in percentage.	Data Type: Float Range: NA Default Value: 0.5 (Note: it means 50%)
cn32c-svc.enableOpenTelemetry	This is an optional parameter. This parameter enables the openTelemetry.	Data Type: boolean Range: true or false Default Value: false

This section includes information about perf-info configurable parameters for OCI deployment of the SEPP.

Table 3-40 perf-info Configurable parameters for OCI Deployment

Parameter	Description	Details
ociMetrics.apiBodyParamNamespace	This is a conditional parameter. This is the metrics namespace to use when searching for metric data points to aggregate. Mandatory for integration with OCI metrics.	Data Type: String Range: NA Default Value: NA
ociMetrics.apiBodyParamTimeRangeSecs	This is an optional parameter. This is the time range that should contain at least one metric data point. The guidance is to set it to 2x scraping interval (interval in which metrics is read from pods and reported to OCI). .	Data Type: Integer Range: 30 to 600 Default Value: 360

Table 3-40 (Cont.) perf-info Configurable parameters for OCI Deployment

Parameter	Description	Details
`ociMetrics.apiQueryParamCompartmentId`	This is an optional parameter. This is the OCID (Oracle Cloud ID) of the compartment containing the NF. Mandatory for integration with OCI metrics.	Data Type: Integer Range: NA Default Value: NA
`ociMetrics.clientTimeoutConnectionTimeoutSecs`	This is an optional parameter. This is the number of seconds to wait for client to establish a connection to the service.	Data Type: Integer Range: 1- 60 Default Value: 1
`ociMetrics.clientTimeoutReadTimeoutSecs`	This is an optional parameter. This is the number of seconds the client will wait for the service to send a response.	Data Type: Integer Range: 1- 60 Default Value: 1
`ociMetrics.enabled`	This is an optional parameter. This parameter indicates whether the integration with OCI metrics is enabled or not.	Data Type: Boolean Range: True or False Default Value: False
`ociMetrics.servicePrettyName`	This is an optional parameter. This is the OCI Monitoring service pretty name used in metrics generated for debugging or observability.	Data Type: String Range: NA Default Value: OCIMONITORING
`summarizeMetricsDataSleepMs`	This is an optional parameter. The sleep time to handle too many requests.	Data Type: Integer Range: NA Default Value: 300
`nrfclient.perf-info.tagNamespace`	This is a mandatory parameter. Specifies the Kubernetes namespace.	Data Type: String Range: NA Default Value: namespace **Note**: In OCI deployment, the value must be k8Namespace.

3.2 Configuring SEPP for NRF Interaction

SEPP starts with registering its profile with the home network NRF. All the heartbeat, discovery, and subscription messages will be redirected to the configured NRF.

For registering, the following configuration needs to be done via Helm or REST mode (depending on the environment).

> **Note**
>
> The user can customize the values as per their requirement.

NRF Static FQDN Support

The user needs to provide the NRF FQDN, nrf scheme, and the port used in the `ocsepp_custom_values_<version>.yaml` file under the nrf-client section.

The following section and parameter needs to be updated in the CV file:

```
primaryNrfApiRoot= ocnrf-ingressgateway.ocnrf:80  # NRF FQDN
nrfScheme=http
```

NRF Virtual FQDN Support

When NRF virtual FQDN needs to be used, the user needs to configure virtualHost configuration at plmn-egress-gateway micro-service through REST mode.

The following configuration needs to be done through REST APIs at plmn-egress-gateway microservice.

The sample configuration which can be used:

Peerconfiguration

This configuration defines the virtual FQDN for NRF.

```
curl  -X PUT http://<config-mgr-svc>:<port>/sepp/nf-common-component/v1/egw/
plmn/peerconfiguration -d
'[{"id":"peer1","apiPrefix":"/","virtualHost":"sepp.ats.test.routing.com"}]' -
H 'Content-Type:application/json'
```

Peersetconfiguration

This configuration denotes the set created for the virtual peer for NRF.

```
curl  -X PUT http://<config-mgr-svc>:<port>/sepp/nf-common-component/v1/egw/
plmn/peersetconfiguration -d '[{"id":"set0","httpConfiguration":
[{"priority":1,
"peerIdentifier":"peer1"}],"httpsConfiguration":
[{"priority":1,"peerIdentifier":"peer1"}]}]' -H 'Content-Type:application/
json'
```

SbiRoutingErrorCriteriaSets

This configuration will be used by the plmn-egress-gateway microservice to alternate between different NRF peers based on exceptions and errors responses received.

```
curl  -X PUT http://<config-mgr-svc>:<port>/sepp/nf-common-component/v1/egw/
plmn/sbiroutingerrorcriteriasets -d '[{"id":"scp_direct2_criteria_2","method":
["GET","POST","PUT","DELETE","PATCH"],"exceptions":
["java.util.concurrent.TimeoutException","java.net.UnknownHostException","java
.net.ConnectException"]}]' -H 'Content-Type:application/json'
```

SbiRoutingErrorActionSets

This configuration will be used by the plmn-egress-gateway microservice to retry or reroute among different NRF peers.

```
curl  -X PUT http://<config-mgr-svc>:<port>/sepp/nf-common-component/v1/egw/
plmn/sbiroutingerroractionsets -d
'[{"id":"scp_direct2_action_0","action":"rero
ute","attempts":2,"blacklist":{"enabled":false,"duration":60000}},
{"id":"scp_direct2_action_1","action":"reroute","attempts":2,"blacklist":
```

```
{"enabled":false,
"duration":60000}},
{"id":"scp_direct2_action_2","action":"reroute","attempts":1,"blacklist":
{"enabled":true,"duration":60000}}]' -H 'Content-Type:applicatio
n/json'
```

RoutesConfiguration

This configuration will be used by the plmn-egress-gateway microservice to identify the NRF only requests.

```
curl  -X PUT http://<config-mgr-svc>:<port>/sepp/nf-common-component/v1/egw/
plmn/routesconfiguration -d '[{"id":"egress_route_proxy","uri":"egress://
request.uri","order":100,"filters":
[{"name":"DefaultRouteRetry"}],"predicates":[{"args":{"pattern":"/
**"},"name":"Path"}]},{"id":"nrf_via_proxy","uri":"http://
request.uri","order":10,"filters":[{"args":{"errorHandling":
[{"priority":1,"actionSet":"scp_direct2_action_0","errorCriteriaSet":"scp_dire
ct2_criteria_2"}],"peerSetIdentifier":"set0","customPeerSelectorEnabled":false
},"name":"SbiRouting"},{"args":[{"name":"myheader1"},
{"name":"myheader3"}],"name":"RemoveRequestHeader"},{"args":
[{"name":"myresponseheader1"},
{"name":"myresponseheader3"}],"name":"RemoveResponseHeader"}],"metadata":
{"httpRuriOnly":false,"httpsTargetOnly":false,"sbiRoutingEnabled":true,"sbiRou
tingWeightBasedEnabled":true},"predicates":[{"args":{"pattern":"/nnrf-*/
**"},"name":"Path"}]}]' -H 'Content-Type:application/json'
```

For more information on REST APIs, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy REST Specification Guide*.

3.3 Configuring DNS for FQDN Resolution

Refer the following document to configure the DNS Server for Inter PLMN FQDN resolution in CNE Environment:

Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.

> **Note**
>
> For any other environment other than CNE, refer the corresponding document for configuring the DNS Server for FQDN resolution.

3.4 Routing Across Multiple Endpoints

SEPP provides flexible and configurable mechanisms for routing SBI and non-SBI traffic across multiple endpoints, supporting both inter-PLMN and intra-PLMN communication scenarios.

Traffic handling, such as routing, load balancing and load sharing is fully configurable based on the deployment architecture and configurations. Depending on the operational and performance requirements, users can define specific routing behaviours through configuration profiles.

The SEPP allows the operator to select from a range of supported routing configurations to ensure an efficient traffic distribution. These configurations enable:

- **Load Sharing and Balancing**: Parallel utilization of multiple endpoints and SBI message flows based on priority and weight using SRV records.
- **Endpoint Routing**: Directed forwarding of messages to specific SEPP peer endpoints.

The following sections provide detailed descriptions of each supported traffic routing mechanism.

3.4.1 Traffic Routing for Inter-PLMN Communication

Following are the different traffic management and routing methods for Inter-PLMN traffic.

3.4.1.1 Failover Routing Across Remote SEPPs

This routing mechanism enables SEPP to route inter-PLMN traffic through a statically configured list of Remote SEPP FQDNs. Messages are sent to the primary FQDN. If the primary SEPP is unreachable, the SEPP retries with the secondary FQDN, followed by the tertiary if needed. This ensures a predictable and reliable switch to the next available SEPP if one fails. This is a default routing mechanism for inter-plmn communication. This can be achieved by providing static FQDN (seppFqdn) in Remote SEPP configuration using CNC Console.

For more details, refer to "Alternate Routing Across Remote SEPPs" section in *Cloud Native Core, Security Edge Protection Proxy User Guide*.

3.4.1.2 Virtual FQDN or Virtual Host Based Load sharing Across Remote SEPPs

This routing mechanism enables SEPP to load share traffic using Virtual FQDNs or Virtual Hosts through DNS SRV queries. It supports load sharing across multiple Remote SEPPs by utilising DNS SRV records using alternate route service and share load on the basis of priority or weight. This can be achieved by providing virtual FQDN OR virtual Host in Remote SEPP's using CNC Console.

For more details, refer to "Load Sharing among Multiple Remote SEPP Nodes" in *Cloud Native Core, Security Edge Protection Proxy User Guide*.

3.4.2 Traffic Routing for Intra-PLMN Communication

Following are the different traffic management and routing methods for Intra-PLMN traffic.

3.4.2.1 3gpp-sbi-target-apiRoot Header Based Routing Across Producer NFs

This is the default routing mechanism where messages are forwarded to backend NFs in core network based on the 3gpp-sbi-target-apiRoot header value. The corresponding default route is automatically provisioned during the SEPP installation.

3.4.2.2 Failover Routing Across Producer NFs

This routing mechanism allows SEPP to route intra-PLMN traffic towards backend NFs (Example: NRF, SCP, and UDR) using statically configured FQDNs. Traffic is directed to a primary FQDN, with automatic failover to secondary and tertiary FQDNs upon failure. This can be achieved by providing static FQDN in peer configuration on plmn-egress-gateway using

CNC Console. This behaviour is configured through CNC Console using defined Peers, Peersets, and routes based on network requirements.

For more details, refer to "Support for Core Networks with or without SCP/Routing Proxy" section in *Cloud Native Core, Security Edge Protection Proxy User Guide*.

3.4.2.3 Virtual FQDN or Virtual Host Based Load sharing Across Producer NFs

This feature enables SEPP to load share traffic using Virtual FQDNs or Virtual Hosts through DNS SRV queries. It supports load sharing across multiple backend NFs by utilising DNS SRV records using alternate route service and share load on the basis of priority or weight. This can be achieved by providing Virtual FQDN or Virtual Host in Peer configuration on plmn-egress-gateway using CNC Console.

For more details, refer to "Alternate Routing and Load sharing based on the DNS SRV Record for Home Network Functions" in *Cloud Native Core, Security Edge Protection Proxy User Guide*.

> **Note**
>
> Load sharing is supported only through DNS SRV records.

4 Upgrading SEPP

This chapter provides information about upgrading Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) deployment to the latest release. It is recommended to perform SEPP upgrade in a specific order. For more information about the upgrade order, see *Oracle Communications Cloud Native Core, Solution Upgrade Guide.*

The SEPP upgrade procedures for single cluster and multicluster deployments. SEPP instance can be upgraded from current version to the latest version using Helm upgrade command.

Following steps must be performed while upgrading the SEPP:

1. SEPP DB Backup
2. SEPP Upgrade

4.1 Supported Upgrade Paths

The following table lists the supported upgrade paths for SEPP:

> **Note**
>
> - SEPP delpoyed in SEPP mode can be upgraded only to SEPP mode.
> - SEPP deployed in Roaming Hub mode can be upgraded only to Roaming Hub mode.
> - Before proceeding with SEPP helm upgrade in this deployment model, SEPP instance database backup must be taken and stored in a location which can be easily restored. Refer SEPP Instance DB Backup section for more information.

Table 4-1 Supported Upgrade Paths

Source Release	Target Release
25.1.20x	25.1.202
25.1.10x	25.1.202
24.3.x	25.1.202

Table 4-2 Supported Upgrade Paths

Source Roaming Hub Release	Target Roaming Hub Release
25.1.20x	25.1.202
25.1.10x	25.1.202
24.3.x	25.1.202

> **Note**
>
> - SEPP must be upgraded before upgrading cnDBTier.
> - When performing an upgrade from 24.2.x or before source release to 25.1.2xx release, ensure `ndb_allow_copying_alter_table` in cnDBTier is set to ON. It can be set to OFF after upgrade.

4.2 Upgrade Strategy

SEPP supports in-service upgrade. The supported upgrade strategy is `RollingUpdate`. The rolling update strategy is a gradual process that allows you to update your Kubernetes system with only a minor effect on performance and no downtime. The advantage of the rolling update strategy is that the update is applied Pod-by-Pod so the greater system can remain active.

> **Note**
>
> It is recommended to perform SEPP upgrade in a specific order. For more information about the upgrade order, see *Oracle Communications Cloud Native Core, Solution Upgrade Guide*.

The following engineering configuration parameters are used to define upgrade strategy:

- `upgradeStrategy` parameter indicates the update strategy used in SEPP.
- `maxUnavailable` parameter determines the maximum number of pods that can be unavailable during upgrade.

Predefined Upgrade Strategy Value

Table 4-3 Predefined Upgrade Strategy Value

Microservice	Upgrade Value (maxUnavailable)
nf-mediation	1
n32-ingress-Gateway	25%
n32-egress-Gateway	25%
plmn-ingress-Gateway	25%
plmn-egress-Gateway	25%
pn32f-svc	Not Applicable **Note**: maxSurge=25% attribute is used for this microservice.
cn32f-svc	Not Applicable **Note**: maxSurge=25% attribute is used for this microservice.
pn32c-svc	Not Applicable **Note**: maxSurge=25% attribute is used for this microservice.

Table 4-3 (Cont.) Predefined Upgrade Strategy Value

Microservice	Upgrade Value (maxUnavailable)
cn32c-svc	Not Applicable **Note**: maxSurge=25% attribute is used for this microservice.
config-mgr-svc	Not Applicable **Note**: maxSurge=25% attribute is used for this microservice.
Appinfo	25%
ocpm-config	50%
performance	50%
sepp-nrf-client-nfmanagement	Single Replica
sepp-nrf-client-nfdiscovery	25%
coherence-svc	1
alternate-route	25%

> **Note**
>
> When SEPP is deployed with OCCM, follow the specific upgrade sequence as mentioned in *Oracle Communications, Cloud Native Core Solution Upgrade Guide*.

4.3 Preupgrade Tasks

This section provides information about preupgrade tasks to be performed before upgrading SEPP.

While upgrading an existing SEPP deployment, the running set of containers and pods are replaced with the new set of containers and pods. However, if there is no change in the pod configuration, the running set of containers and pods are not replaced.

> **Note**
>
> - No configuration should be performed during the upgrade.
> - Do not exit from Helm upgrade command manually. After running the Helm upgrade command, it takes some time (depending upon the number of PODs to upgrade) to upgrade all of the services. In the meantime, you must not press "ctrl+c" to come out from Helm upgrade command. It may lead to anomalous behavior.

Note

- The `releaseVersion` value in the `ocsepp_values.yaml` file can not be changed.
- While performing an upgrade from an older release to a newer release, you must align the `ocsepp_values.yaml` file of the new release as per the `ocsepp_values.yaml` file of the older release. Ensure that you do not change any Helm parameter values. Do not enable any new feature during the upgrade. Any `ocsepp_values.yaml` parameter must not be changed while upgrading unless explicitly specified in this guide. For information about enabling any new feature through Helm parameters, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.
- Install or upgrade the network policies, if applicable. For more information, see Configuring Network Policies.
- While performing an upgrade, the Global Rate Limiting feature must be disabled on both the ingress gateways (n32-ingress-gateway, plmn-ingress-gateway) in the source `custom_values.yaml` file.

```
rateLimiting:
    enabled: false
  rssRateLimiter:
    enabled: false
  globalIngressRateLimiting:
    enabled: false
```

- After the upgrade, the Cat-3 Previous Location Check feature must be restored to its previous state, if the feature was enabled previously.

Preupgrade Steps

1. Keep current custom_values.yaml file as backup, that is, `ocsepp_custom_values_<version>.yaml` for upgrading.
2. Update the new *custom_values.yaml* defined for target SEPP release. See Customizing SEPP section for more details about Helm configurable parameters.
3. Perform sanity check using Helm test. See the Performing Helm Test section for the Helm test procedure.
4. Before starting upgrade, take a manual backup of SEPP REST based configuration. It will help if manual backup is taken in case the data need to be restored before the upgrade. For REST API configuration details, see SEPP Instance DB Backup section to take the backup.
5. If you are upgrading from version 24.3.x to target SEPP release, follow the steps below:
   - Before starting the procedure to upgrade, perform the following tasks:
     - Perform the following scenarios for enabling or disabling the Open Telemetry tracing as per the requirement, when upgrading from 24.3.x to target SEPP release:
       * To enable tracing in the target SEPP release, perform the following:
         a. Ensure that Jaeger collector service is up and running inside occne-infra, with port specified in `ocsepp_custom_values_<version>.yaml` file.

b. The following flag must be set to true to enable the Open Telemetry for n32c and n32f SEPP services:

```
enableOpenTelemetry: true
```

c. Ensure that following configuration is added or updated in 24.3.x in `ocsepp_custom_values_<version>.yaml` in n32c and n32f microservices.

```
#Jaeger Tracing
jaegerTracingEnabled: false
bodyInTraceEnabled: false
otel:
  jaeger:
    udpSender:
      host: "jaeger-collector.cne-infra"
      port: 4318
    logSpans: false
    probabilisticSamplingRate: 0.1
```

d. Ensure that following configuration is added or updated in 24.3.x in e `ocsepp_custom_values_<version>.yaml` in n32-ingress-gateway, plmn-ingress-gateway, n32-egress-gateway, and plmn-egress-gateway.

```
# enable jaeger telemetry tracing
jaegerTelemetryTracingEnabled: false

openTelemetry:
  jaeger:
    httpExporter:
      host: "jaeger-collector.cne-infra"
      port: 4318
    probabilisticSampler: 0.5
```

* To disable tracing for n32c and n32f microservices, the following flag must be set to false in e `ocsepp_custom_values_<version>.yaml` file:

```
enableOpenTelemetry: 'false'
```

SEPP Instance DB Backup

This section describes the procedure to perform the DB backup of SEPP Instance.

Prerequisites:

- MySQL NDB cluster should be in a healthy state.
- Every database node of the MySQL NDB cluster should be in running state.
- For cnDBTier to verify the prerequisites, check mysql pod is up and running.
- Log in to the deployment and run the following command to take the dump (backup) of the database. The user is required to enter the password.

```
kubectl exec -i -n <namespace> <sql-node> -- mysqldump --single-
transaction --no-tablespaces --no-create-info -h 127.0.0.1 -u <username> -
p <sepp database-name> | gzip > <backup_filename>.sql.gz
```

For example:

```
kubectl exec -i -n occne-ndb ndbappmysqld-0 -- mysqldump --single-
transaction --no-tablespaces --no-create-info
      -h 127.0.0.1 -u seppusr -p seppdb_sepp1 | gzip >
sepp_sepp1_dbBackup.sql.gz
```

> **Note**
>
> The operator must ensure there is enough space on the current directory in order to save the backup file.

Verifying cnDBTier

Perform the following steps while upgrading from SEPP 24.2.x or earlier versions to SEPP 24.3.x:

1. Run the following command to check the current plugin:

   ```
   SELECT user, host, plugin FROM mysql.user;
   ```

   Example:

   ```
   SELECT user, host, plugin FROM mysql.user;
   ```

   Output:

   ```
   user             | host      | plugin                |
   +------------------+-----------+-----------------------+
   | cnccusr          | %         | caching_sha2_password |
   | occnerepluser    | %         | caching_sha2_password |
   | occneuser        | %         | mysql_native_password |
   | seppuser1        | %         | caching_sha2_password |
   | seppuser3        | %         | mysql_native_password |
   | healthchecker    | localhost | caching_sha2_password |
   | mysql.infoschema | localhost | caching_sha2_password |
   | mysql.session    | localhost | caching_sha2_password |
   | mysql.sys        | localhost | caching_sha2_password |
   | root             | localhost | caching_sha2_password |
   +------------------+-----------+-----------------------+
   10 rows in set (0.00 sec)
   ```

2. Run the following command to check the plugin that is associated with the seppuser, and used for the SEPP that is planned to be upgraded:
   Example: `| seppuser3 | % | mysql_native_password |`
3. If the plugin is ‘mysql_native_password’, run the following command to change the plugin from ‘mysql_native_password’’ to ‘caching_sha2_password’:

   ```
   ALTER USER '<username>'@'%' IDENTIFIED WITH caching_sha2_password BY
   '<password>';
   ```

Example:

```
ALTER USER 'seppuser3'@'%' IDENTIFIED WITH caching_sha2_password BY
'NextGenCne1';
```

4. Run the following command to verify that the plugin is updated:

   ```
   SELECT user, host, plugin FROM mysql.user;
   ```

   The plugin should get updated to 'caching_sha2_password'.
   Output: `| seppuser3 | % | caching_sha2_password |`

5. Wait for some time and verify the health of the SEPP pods. Run the following command to check if the pods are up and running:

   ```
   Kubectl get po -n <namespace>
   ```

> **Note**
>
> If the plugin selected is '`caching_sha2_password`', then the above changes are not required.

Database Configuration

Before performing an upgrade to 24.3.x release, run the following command to provide the required permission to MySQL Database:

```
$ GRANT SELECT,INSERT,CREATE,ALTER,DROP,LOCK TABLES,CREATE TEMPORARY
TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON mysql.* TO '<OCSEPP User
Name>'@'%';
```

Example:

```
GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE TEMPORARY
TABLES,DELETE,UPDATE,REFERENCES,EXECUTE ON mysql.* TO 'seppusr'@'%';
```

4.4 Upgrade Tasks

This section includes information about upgrading an existing SEPP deployment.

4.4.1 Helm Upgrade

Upgrading an existing deployment replaces the running containers and pods with new containers and pods. If there is no change in the pod configuration, it is not replaced.

Unless there is a change in the service configuration of a microservice, the service endpoints remain unchanged.

4.4.2 Upgrading SEPP

Perform the following procedure to upgrade SEPP.

⚠ Caution

- Stop the provisioning traffic before you start the upgrade procedure.
- No configuration should be performed during upgrade.
- Do not exit from `helm upgrade` command manually. After running the `helm upgrade` command, it takes some time (depending upon the number of pods to upgrade) to upgrade all the services. In the meantime, you must not press "`ctrl+c`" to come out from `helm upgrade` command. It may lead to anomalous behavior.

ⓘ Note

- If the Helm upgrade results in failure and displays *ConfigMap <Egress Rate Limiting ConfigMap Name> in namespace <Namespace> exists and cannot be imported into the current release: invalid ownership metadata* error, do the following:

  Delete the Egress Rate Limit ConfigMap using the following command: `kubectl delete cm <Egress Rate Limiting ConfigMap Name> -n <namespace>` and run the Helm upgrade again.

1. Untar the latest SEPP package and if required, re-tag and push the images to registry. For more information, see Downloading SEPP package and Pushing the Images to Customer Docker Registry.
2. Modify the `ocsepp_custom_values_25.1.202.yaml` file parameters as per site requirement.
3. Run the following command to upgrade an existing SEPP deployment:
   a. Using local Helm chart:

   ```
   helm upgrade <release_name> <helm_chart> -f
   <ocsepp_customized_values.yaml> --namespace <namespace-name>
   ```

   Example:

   ```
   helm upgrade ocsepp-release ocsepp-25.1.202.tgz -f ocsepp-custom
   values-25.1.202.yaml --namespace seppsvc
   ```

   Where,

   `<release_name>` is the SEPP release name.

   `<helm_chart>` is the Helm chart.

   `<sepp_customized_values.yaml>` is the latest custom-values.yaml file.

For example, ocsepp-25.1.202.0.0.custom-values.yaml

<namespace> is namespace of SEPP deployment.

b. Using chart from Helm repo:

```
helm upgrade <release_name> <helm_repo/helm_chart> --version
<chart_version> -f <ocsepp_customized_values.yaml> --namespace
<namespace>
```

Example:

```
helm upgrade ocsepp-release ocsepp-25.1.202.tgz --version
<chart_version> -f ocsepp-custom values-25.1.202.yaml --namespace
seppsvc
```

Where,

<release_name> is the SEPP release name.

<helm_chart> is the Helm chart.

<sepp_customized_values.yaml> is the latest custom-values.yaml file.

For example, ocsepp-25.1.202.0.0.custom-values.yaml

<namespace> is namespace of SEPP deployment.

4. Run the following command to check the status of the upgrade:

```
helm status <release_name> --namespace <namespace-name>
```

Where,

<release_name> is the SEPP release name.

<namespace> is namespace of SEPP deployment.

For example:

```
$ helm status ocsepp-release --namespace seppsvc
```

Sample output of a successful upgrade:

```
[cloud-user@occne-22-2-0-cluster-bastion-1 ocsepp-25.1.200]$  helm history
ocsepp-release -n seppsvc
REVISION        UPDATED                         STATUS
CHART           APP VERSION     DESCRIPTION
1               Wed May  13 07:19:50 2023        superseded
ocsepp-25.1.200   25.1.202.0.0      Install complete
2               Wed May  13 07:31:21 2023        superseded
ocsepp-25.1.200   25.1.202.0.0      Upgrade complete
3               Wed May  13 07:50:08 2023        superseded
ocsepp-25.1.200   25.1.202.0.0      Rollback to 1
```

5. Perform sanity check using Helm test. See the Performing Helm Test section for the Helm test procedure.

6. If the upgrade fails, see Upgrade or Rollback failure in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide*.

5
Rolling Back SEPP

This chapter provides information about rolling back Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) deployment to the previous release. It is recommended to perform SEPP rollback in a specific order. For more information about the rollback order, see *Oracle Communications Cloud Native Core, Solution Upgrade Guide.*

Following steps must be followed while performing rollback:

1. SEPP DB Rollback or Restore
2. SEPP Rollback

> **Note**
>
> It is recommended to verify the copy pasted content especially when the hyphens or any special characters are part of copied content.

5.1 Supported Rollback Paths

The following table lists the supported rollback paths for SEPP:

> **Note**
>
> - SEPP deployed in SEPP mode can be rolled back only to SEPP mode.
> - SEPP deployed in Roaming Hub mode can be rolled back only to Roaming Hub mode.

Table 5-1 Supported Rollback Paths

Source Release	Target Release
25.1.202	25.1.20x
25.1.202	25.1.10x
25.1.202	24.3.x

Table 5-2 Supported Rollback Paths

Source Roaming Hub Release	Target Roaming Hub Release
25.1.202	25.1.20x
25.1.202	25.1.10x
25.1.202	24.3.x

> **Note**
>
> When performing a rollback from 25.1.1x to 24.2.x release, ensure `ndb_allow_copying_alter_table` in cnDBTier is set to ON.

5.2 Pre-rollback Tasks

This section describes the tasks to be performed before a rollback.

5.2.1 SEPP Instance DB Rollback or Restore

This section provides details of SEPP instance DB Rollback. In case of SEPP Upgrade failure, rollback SEPP DB to previous version by following the below steps.

> **Note**
>
> The latest backup must be used for rollback.

To perform a SEPP DB rollback or Restore:

> **Note**
>
> The following are the summary of steps to be performed:
>
> 1. Log in to the deployment cluster, drop the existing database, and create a new database.
> 2. Run the DB Schema file provided as part of package *<ocsepp_rollback_schema_<version>.sql>* to create the SEPP database schema in the newly created database.
>   - Use the schema file from the SEPP version to which you are performing the rollback.
> 3. Rearrange the DB Dump file (taken during SEPP instance DB backup) sequentially so that there wont be any foreign key constraints issue.
> 4. Run the following command to restore Database with rearranged sql file:
>
>    ```
>    mysql -h 127.0.0.1 -u occneuser -p seppdb_sepp1 < restore.sql
>    ```

Perform the following steps to do a SEPP DB rollback or Restore:

1. Run the following command to drop the Database and create a new database:

   ```
   DROP DATABASE <SEPP Database>
   CREATE DATABASE IF NOT EXISTS <SEPP Database>;
   ```

For example:

```
#To be run in the mysql pod:
DROP DATABASE seppdb_sepp1;
CREATE DATABASE IF NOT EXISTS seppdb_sepp1;
```

> **Note**
>
> - The Database should be dropped from all the sites in case of multi site replication.
> - You must take the <ocsepp_rollback_schema_<version>.sql> file from the SEPP version to which you are performing the rollback.

2. Copy the DB Schema file provided as part of package into the MySQL pod (<ocsepp_rollback_schema_<version>.sql>).
   Run the following command to copy the DB Schema file to pod:

   ```
   kubectl cp<ocsepp_rollback_schema_<version>.sql> <namespace>/<pod-
   name>:<directory where you want your fileplaced>
   ```

   For example:

   ```
   kubectl cp ocsepp_rollback_schema_<version>.sql gr-cndb-site1/
   ndbappmysqld-0:/home/mysql
   ```

3. Run the following command to connect to the SQL node of the NDB cluster or connect to the cnDBTier:

   ```
   $ kubectl -n <cndbtier_namespace> exec -it <cndbtier_sql_pod_name> -c
   <cndbtier_sql_container_name> -- bash
   ```

   For example:

   ```
   $ kubectl -n cndbtier  exec -it ndbappmysqld-0 -c mysqlndbcluster -- bash
   ```

4. Restore this new database with the DB Schema file provided as part of package (ocsepp_rollback_schema_<version>.sql).
   Run the following command to Restore DB Schema:

   ```
   mysql -h 127.0.0.1 -u root -p <DB name> < <DB Schema file name>
   ```

   For example:

   ```
   mysql -h 127.0.0.1 -u root -p seppdb_sepp1 <
   ocsepp_rollback_schema_<version>.sql
   ```

5. The DB dump has to be rearranged sequentially not to get any foreign key constraints issue. For that, create the ENV variables and run it in a loop.

a. Run the following command to convert the mysqldump file which was taken as a backup (sql.gz file) to a sql file to rearrange it:
Unzipping the gz file:

```
gunzip -d <backup_filename>.sql.gz
```

For example:

```
gunzip -d sepp_sepp1_dbBackup.sql.gz
```

b. Rearrange the backup sql file in correct order by using following procedure:

i. Run the following command to rearrange the Table Data :

```
export KC_TABLES="APP_STATE MEDIATION_CONFIG_RELEASE MEDIATION_RULE
OCMEDIATION_ROLLBACK_ACTION OCMEDIATION_SYSTEM_OPTIONS
ROLLBACK_ACTION ReleaseConfig SiteJsonSchemaVersionInfo
UPGRADE_ROLLBACK_EVENTS common_configuration
common_configuration_backup snapshot_mapping topic_info
topic_info_backup configuration_item configuration_item_backup
NrfLeaderPod leader_election discovery_requests_nologging
producer_profiles_nologging header topology_body
roaming_partner_profile n32f_db_context roaming_partner_set plmn
actual_values pseudo_values topology_option
default_service_api_list_configuration security_allowed_list_action
security_allowed_list_content security_allowed_list_rule
security_allowed_list_content_rule sepp_feature_config
mediation_trigger_rule_list mediation_trigger_rule
mediation_trigger_rule_error_config
plmn_validation_header_path_config plmn_validation_body_config
security_plmn_list_action security_allowed_plmn_content
security_plmn_list_rule security_plmn_list_content_rule
sepp_sor_config sepp_sor_allowed_rss_list sepp_sor_url_list
sepp_sor_allowed_url_join sepp_feature_error_config
ingress_rate_limiting message_validation_list_config
message_validation_rule_config message_validation_list_rule_mapping
message_validation_api_config message_validation_feature_config
previous_location_list_config previous_location_rule_config
previous_location_list_rule_config
previous_location_serving_header_config
previous_location_serving_body_config
previous_location_ue_header_config previous_location_ue_body_config
cache_refresh_config egress_rate_limit_config
egress_rate_limit_list_config sepp_service_log_configuration
orig_nw_id_hdr_support verbose_err_rsp_config";
```

ii. Run the following command to create an ENV pointing to the sql file to be filtered:

```
export KC_BACKUP="./<Backup SQL Dump File>";
```

For example:

```
export KC_BACKUP="./sepp_sepp1_dbBackup.sql";
```

iii. Run the following command to verify that the ENV variables are set:

```
echo$KC_TABLES
echo$KC_BACKUP
```

iv. Run the following command to rearrange the dump file to make it in sequential insertion order:

```
for i in $KC_TABLES; do if [ "$i" = "topic_info" ]; then echo
"DELETE FROM \`$i\` WHERE NAME='nrfclient.cfg';"; fi;  grep "INSERT
INTO \`$i\`" "$KC_BACKUP"; done > <file name along with its
location>
```

Example:

```
for i in $KC_TABLES; do if [ "$i" = "topic_info" ]; then echo
"DELETE FROM \`$i\` WHERE NAME='nrfclient.cfg';"; fi;  grep "INSERT
INTO \`$i\`" "$KC_BACKUP"; done > /tmp/restore.sql
```

v. Run the following command to provide execution permission to the file:

```
chmod +x /tmp/restore.sql
```

6. Run the following command to copy file into the pod:

```
kubectl cp <backup_file name>.sql <namespace>/<pod-name>:<directory where
you want your file placed>
```

For example:

```
kubectl cp restore.sql cndbtier1/ndbappmysqld-0:/home/mysql
```

7. Run the following command to connect to the SQL node of the NDB cluster or connect to the cnDBTier:

```
$ kubectl -n <cndbtier_namespace> exec -it <cndbtier_sql_pod_name> -c
<cndbtier_sql_container_name>-- bash
```

For example:

```
$ kubectl -n cndbtier  exec -it ndbappmysqld-0 -c mysqlndbcluster -- bash
```

8. Populate the Database with data using the file that you have, after filtering the sqldump file.
9. Run the following command to restore Database Data:

```
mysql -h 127.0.0.1 -u root -p <DB name> < <backup_filename>
```

For example:

```
mysql -h 127.0.0.1 -u root -p seppdb_sepp1 < restore.sql
```

> **Note**
>
> Verify that the created restore.sql begins with the "INSERT INTO" statement. Anything appended before it must be removed.

10. Log in to the MySQL prompt and confirm that the databases are restored.
11. Run the following command to delete the sql files copied into the pod after the restore process is complete and successful (by logging into the SQL node):

```
rm -rf <DB Schema file name>
rm -rf <backup_filename>
```

Example:

```
rm -rf ocsepp_rollback_schema_<version>.sql
rm -rf restore.sql
```

5.3 Rollback Steps

Perform this procedure to roll back SEPP deployment from 25.2.100 to the previously supported versions:

> **Caution**
>
> - No configuration should be performed during rollback.
> - Do not exit from `helm rollback` command manually. After running the `helm rollback` command, it takes some time (depending upon number of pods to rollback) to rollback all of the services. In the meantime, you must not press "`ctrl+c`" to come out from `helm rollback` command. It may lead to anomalous behavior.
> - Ensure that no SEPP pod is in the failed state.
> - If the Helm rollback results in failure and displays *Rollback "ocsepp" failed: no ConfigMap with the name "rss-ratelimit-map" found* error, it indicates that Helm is not able to merge current and rollback charts. Then run the Helm rollback again with **--force**.
> - If the Helm rollback results in failure and displays *ConfigMap <Egress Rate Limiting ConfigMap Name> in namespace <Namespace> exists and cannot be imported into the current release: invalid ownership metadata* error, do the following:
>
>   Delete the Egress Rate Limit ConfigMap using the following command: `kubectl delete cm <Egress Rate Limiting ConfigMap Name> -n <namespace>` and run the Helm rollback again.

> **Note**
>
> SEPP might raise alerts while performing rollback. To clear any alert, see "Alerts" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*.

1. Run the following command to check the revision you must roll back to:

   ```
   helm history <release_name> -n <release_namespace>
   ```

   Where,

   - `<release_name>` is the release name used by the Helm command.
   - `<release_namespace>` is the namespace where SEPP is deployed.

   For example:

   ```
   helm history ocsepp --namespace seppsvc
   ```

2. Run the command to rollback to the required revision:

   ```
   helm rollback <release_name> <revision_number> --namespace
   <release_namespace>
   ```

   Where, `<revision_number>` is the release number to which SEPP needs to be rolled back.

   For example:

   ```
   helm rollback ocsepp 1 --namespace seppsvc
   ```

3. If the rollback fails, see "Upgrade or Rollback Failure" section in *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Troubleshooting Guide.*

5.4 Post Rollback Tasks

After performing rollback, restore preupgrade data obtained earlier through manual backup.

GET API for different resources can be used to see current values in SEPP, then accordingly if any update required, individual service APIs defined for different resources can be used to reconfigure the data backup taken before upgrade.

> **Caution**
>
> Run the following command to delete the `rateLimitingConfigMap` ConfigMap manually, post rollback (applicable only for the roll back to 22.4.x or previous versions):
>
> ```
> kubectl delete cm <rateLimitingConfigMap> -n <release-namespace>
> ```

See *Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) Rest Specification* for API details.

6
Uninstalling SEPP

This chapter provides information about uninstalling Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP).

> **Note**
>
> kubectl commands might vary based on the platform deployment. Replace kubectl with Kubernetes environment-specific command line tool to configure Kubernetes resources through kube-api server. The instructions provided in this document are as per the Oracle Communications Cloud Native Environment (CNE) version of kube-api server.

> **Caution**
>
> User, computer and applications, and character encoding settings may cause an issue when copy-pasting commands or any content from PDF. PDF reader version also affects the copy-pasting functionality. It is recommended to verify the pasted content especially when the hyphens or any special characters are part of the copied content.

6.1 Uninstalling SEPP Using Helm

To uninstall SEPP, run the following command:

1. Run the following command to uninstall SEPP deployment:

   ```
   helm uninstall <helm-release> -n <ocsepp namespace>
   ```

   Where,

   `helm-release` is a name provided by the user to identify the helm deployment.

   `release-namespace` is a name provided by the user to identify the namespace of SEPP deployment.

   Example:

   ```
   helm uninstall ocsepp-release -n seppsvc
   ```

2. Run the following command to reverify whether the SEPP uninstallation is successful and the config maps are deleted:

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

Output:

```
[seppuser@thrust6-bastion-1 ~]$ kubectl get cm -n <namespace>
NAME                 DATA   AGE
istio-ca-root-cert   1      87m
kube-root-ca.crt     1      87m
[seppuser@thrust6-bastion-1 ~]$
```

3. Helm keeps a record of its releases, so you can still reactivate the release after uninstalling it.
   To completely remove a release from the cluster, add the `--purge` parameter to `helm delete` command:

   ```
   helm delete --purge <helm-release>
   ```

   For example:

   ```
   helm delete --purge ocsepp-release
   ```

6.2 Verifying Uninstallation and Deleting Kubernetes Namespace

This section describes how to verify SEPP uninstallation.

1. Run the following command to verify the SEPP uninstallation:

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

2. Run the following command to delete specific resources:

   ```
   kubectl delete <resource-type> <resource-name> -n <namespace>
   ```

3. Run the following command to delete all the objects:

   ```
   $ kubectl delete all -n <namespace>
   ```

   > ⚠ **Caution**
   >
   > The command deletes all the Kubernetes objects of the specified namespace. In case you have created the RBAC resources and service accounts before the helm installation in the same namespace and these resources are required, then do not delete them.

4. For example, to remove the config map, run the following command:

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

5. Run the following command to delete the Kubernetes namespace:

   ```
   kubectl delete namespace  <namespace>
   ```

Example:

```
kubectl delete namespace seppsvc
```

6. Run the following command to verify the uninstallation:

   ```
   kubectl get namespace
   ```

   No SEPP namespace must be displayed in the command output. In case of any failure, contact My Oracle Support .

In case of successful uninstallation, no SEPP resource is displayed in the command output.

6.3 Cleaning up Database

This section describes the steps to completely remove MySQL database and username in the following scenarios.

> **Note**
>
> - SEPP is not going to be installed on that cluster.
> - User is configuring the MySQL database name or MySQL user name.

1. Log in to the machine which has permission to access the SQL nodes of NDB cluster.
2. Connect to the SQL node of NDB cluster successively.
3. Log in to the MySQL prompt using root permission or user, which has permission to drop the tables. For example:

   ```
   mysql -h 127.0.0.1 -u<username> -p<password>
   ```

   > **Note**
   >
   > This command may vary from system to system, path for MySQL binary, root user and root password. After running this command, the user must enter the password specific to the user mentioned in the command.

4. Run the following commands to remove SEPP database and backup database:
   a. Run the following command to remove SEPP database:

      ```
      $ DROP DATABASE if exists <SEPP database>;
      ```

      Example:

      ```
      $ DROP DATABASE if exists seppdb;
      ```

   b. Run the following command to remove SEPP backup database:

```
$ DROP DATABASE if exists <SEPP backup database>;
```

Example:

```
$ DROP DATABASE if exists seppbackupdb;
```

> **⚠ Caution**
>
> Removal of MySQL Users must be done on all the SQL nodes from the SEPP site.

5. Exit from MySQL prompt and SQL node.

6.4 Removing Database Users

This section describes how to remove MySQL users.

Run the following command to remove MySQL users while uninstalling SEPP:

```
DROP USER IF EXISTS <OCSEPP User Name>;
```

Example:

```
DROP USER IF EXISTS seppusr;
```

> **ⓘ Note**
>
> Removal of users must be done on all the SQL nodes for all SEPP sites.

7 Fault Recovery

This chapter describes the procedures to perform fault recovery for Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP) deployment.

7.1 Overview

You must take backup of the databases and restore them either on the same or a different cluster. The SEPP database (MySQL NDB Cluster) is used for running any command or to follow any instruction.

> **Note**
>
> This section describes recovery procedures to restore SEPP completely or partially.

7.2 Impacted Areas

The following table provides information about the impacted areas during SEPP fault recovery:

Table 7-1 Impacted Areas

Scenario	Requires Fault Recovery or re-install of CNE?	Requires Fault Recovery or re-install of cnDBTier?	Requires Fault Recovery or re-install of SEPP?	Other
Scenario 1: Deployment Failure	No	No	Yes	SEPP DB is not restored. Only helm uninstall/ install is done.
Scenario 2: cnDBTier Corruption	No	Yes	No (use helm upgrade if DB configuration is changed)	cnDBTier must be restored from backup and not re-install. If re-install of cnDBTier is needed, then CNE also need to re-installed.
Scenario 2A: When DBTier failed in Single or Multiple (but not all) Sites	No	Yes	No	NA
Scenario 2B: When DBTier failed in all Sites	No	Yes	No	NA

Table 7-1 (Cont.) Impacted Areas

Scenario	Requires Fault Recovery or re-install of CNE?	Requires Fault Recovery or re-install of cnDBTier?	Requires Fault Recovery or re-install of SEPP?	Other
Scenario 3: Database Corruption	No	No	No	SEPP backup and restore of configuration database is required on impacted site. This needs automatic periodic backup.
Scenario 4: Site Failure	Yes	Yes	Yes	NA
Scenario 4A: Single or Multiple Site Failure	Yes	Yes	Yes	NA
Scenario 4B:All Site Failure	Yes	Yes	Yes	NA

7.3 Prerequisites

Before performing any fault recovery procedure, ensure that the following prerequisites are met:

1. cnDBTier must be in a healthy state and available on multiple sites along with SEPP. To check the cnDBTier status, perform the following steps:
   a. Run the following command to ensure that all the nodes are connected:

      ```
      ndb_mgm> show
      ```

   b. Run the following command to check the pod status:

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

      If the pod status is `Running`, then cnDBTier is in healthy state.

   c. Run the following command to check if the replication is up:

      ```
      mysql> show slave status\G
      ```

      In case there is any error, see*Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*

   d. Run the following command to check which cnDBTier has ACTIVE replication to take backup:

      ```
      select * from replication_info.DBTIER_REPLICATION_CHANNEL_INFO;
      ```

2. Automatic backup must be enabled on cnDBTier. Enabling automatic backup helps in:
   - restoring stable version of the SEPP database.

- minimizing significant loss of data due to upgrades or roll back failures.
- minimizing loss of data due to system failure.
- minimizing loss of data due to data corruption or deletion due to external input.
- migrating database information from one site to another.

3. The following files must be available for fault recovery:
   - Custom values file used at the time of network function deployment
   - Helm charts used at the time of network function deployment
   - Secrets and Certificates
   - RBAC resources

7.4 Fault Recovery Scenarios

This section describes the fault recovery procedures for various scenarios.

7.4.1 Scenario 1: Deployment Failure

This scenario describes how to recover SEPP when the deployment corrupts.

To recover SEPP:

1. Run the following command to uninstall SEPP:

   ```
   helm uninstall <release_name> --namespace <namespace>

   Example:
   helm uninstall ocsepp --namespace seppsvc
   ```

   For more information about uninstalling SEPP, see the Uninstalling SEPP section.
2. Install SEPP as described in the Installing SEPP section. Use the backup of custom values file to reinstall SEPP.

Restore SEPP, cnDBTier, and SEPP database (DB) as described in Restoring SEPP and cnDBTier.

7.4.2 Scenario 2: cnDBTier Corruption

This section describes how to recover database when the data replication is broken due to database corruption and cnDBTier has failed in single, multiple sites or all sites.

When the database corrupts, the database on all the other sites may also corrupt due to data replication. It depends on the replication status after the corruption has occurred. If the data replication is broken due to database corruption, then cnDBTier fails in either single or multiple sites (not all sites). And if the data replication is successful, then database corruption replicates to all the cnDBTier sites and cnDBTier fails in all sites.

The following are cnDBTier failure scenarios:

If corrupted database is replicated to mated sites, follow:

- **When DBTier failed in Single or Multiple (but not all) Sites**

If corrupted database cause replication failure and hence local to a site, follow:

- **When DBTier failed in all Sites**

> **Note**
>
> This scenario impacts all the NFs using the corrupted cnDBTier. All the NFs sharing cnDBTier needs to do a fault recovery as cnDBTier is corrupted.

7.4.2.1 When cnDBTier failed in Single or Multiple (but not all) Sites

This section describes how to recover database when the data replication is broken due to database corruption and cnDBTier has failed in either single or multiple sites (not all sites).

To recover database:

1. Uninstall SEPP Helm chart. For information about uninstalling SEPP, see the Uninstalling SEPP section.
2. For cnDBTier fault recovery:
   a. Create on-demand backup from mated site that has health replication with failed site. For more information about cnDBTier backup, see the "Create On-demand Database Backup" chapter in the *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
   b. Use the backup data from mate site for restore. For more information about cnDBTier restore, see the "Restore Georeplication Failure" chapter in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*

   > **Note**
   >
   > The "Restore Georeplication Failure" chapter in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide* has a procedure for two sites where one of the cluster has fatal error. You can perform that procedure for all the sites in a multiple site setup.

3. Install SEPP Helm chart. For more information about installing SEPP, see the Installing SEPP section.

7.4.2.2 When cnDBTier failed in all Sites

This section describes how to recover database when successful data replication corrupts all the cnDBTier sites.

To recover database:

1. Uninstall SEPP helm charts. For more information about uninstalling SEPP, see the Uninstalling SEPP section.
2. For cnDBTier fault recovery:
   a. Use on-demand backup file to restore database from the previous data backup. For more information about cnDBTier restore, see the Restore Georeplication Failure chapter in the *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

> **Note**
>
> The Restore Georeplication Failure chapter has a procedure for two sites where one of the cluster has fatal error. You can perform that procedure for all the sites in a multiple site setup.

3. Install SEPP helm charts. For more information about installing SEPP, see the see the Installing SEPP section.

7.4.3 Scenario 3: Configuration Database Corruption

This scenario describes how to recover SEPP when its configuration database corrupts.

The configuration database is stored in a site exclusive database along with its tables. Thus, corruption of configuration database impacts only a particular site.

To recover SEPP configuration database, user has to restore the datebase (DB) backup.

1. Transfer the `<backup_ filename >.sql.gz` file to the SQL node where user wants to restore it.
2. Log in to MySQL NDB Cluster's SQL node on the new DB cluster and create a new database where the database needs to be restored.
3. For details on creating database and user and adding permissions, see Configuring Database, Creating Users, and Granting Permissions section.

> **Note**
>
> The database name created in the above step should be same as the database name created in the following step. The Kubernetes secret must be the same as in the custom_values.yaml used later for Installing SEPP.

4. Use the following command to restore the database to the new database:

   ```
   gunzip < <backup_filename>.sql.gz | mysql -h127.0.0.1 –u <username> -p
   <backup-database-name>
   ```

   Enter the password when prompted.

   Example:

   ```
   gunzip < SEPPdbBackup.sql.gz | mysql -h127.0.0.1 -u dbuser -p seppdb
   ```

7.4.4 Scenario 4: Site Failure

This section describes how to perform fault recovery when either one, multiple, or all sites have a software failure. The following are site failure scenarios:

- Single or Multiple Site Failure
- All Sites Failure

7.4.4.1 Single or Multiple Site Failure

This scenario applies when one or more sites, and not all sites, have failed and there is a requirement to perform fault recovery. It is assumed that the user has cnDBTier and SEPP installed on multiple sites with automatic data replication and backup enabled.

To recover the failed sites:

1. Run the Cloud Native Environment (CNE) installation procedure to install a new cluster. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation Guide*.
2. For cnDBTier fault recovery:
   a. Take on-demand backup from the mate site that has health replication with the failed site or sites. For more information about on-demand backup, see the "Create On-demand Database Backup" chapter in the *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
   b. Use the backup data from the mate site to restore the database. For more information about database restore, see "Restore Georeplication Failure" chapter in the *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
3. Install SEPP Helm chart. For more information about installing SEPP, see the Uninstalling SEPP section.

7.4.4.2 All Sites Failure

This scenario applies when all sites have failed, and there is a requirement to perform fault recovery. It is assumed that the user has cnDBTier and SEPP installed on multiple sites with automatic data replication and backup enabled.

To recover all the failed sites:

1. Run the Cloud Native Environment (CNE) installation procedure to install a new cluster. For more information, see *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide.*
2. Use on-demand backup file to restore database from previous data backup. For more information about database restore, see "Restore Georeplication Failure" chapter in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
   Note:
   - The auto-data backup file is one that is built from scheduled automatic backup.
   - The "Restore Georeplication Failure" chapter contains a procedure for two sites where one of the clusters has fatal error. You can perform the same procedure for all the sites in a multiple site setup.
3. Install SEPP helm chart.

A.1 SEPP Database Backup and Restore

Introduction

Perform this procedure to take a backup of the SEPP database (DB) and restore the database on a different cluster. This procedure is for on-demand backup and restoring of SEPP DB. The commands used for these procedures are provided by the MYSQL Network Database (NDB) cluster.

Prerequisite

Ensure that the MYSQL NDB cluster is in a healthy state, and each database node must be in the running state. Run the following command to check the status of cnDBTier service:

```
kubectl -n <namespace> exec <management node pod> -- ndb_mgm -e show
```

Where,

- `<namespace>` is the namespace where cnDBTier is deployed.
- `<management node pod>` is the management node pod of cnDBTier.

Example:

```
[cloud-user@vcne2-bastion-1 ~]$ kubectl -n seppsvc exec ndbmgmd-0 -- ndb_mgm -
e show
Connected to Management Server at: localhost:1186
Cluster Configuration
---------------------
[ndbd(NDB)]     2 node(s)
id=1    @10.233.86.202  (mysql-8.0.22 ndb-8.0.22, Nodegroup: 0, *)
id=2    @10.233.81.144  (mysql-8.0.22 ndb-8.0.22, Nodegroup: 0)

[ndb_mgmd(MGM)] 2 node(s)
id=49   @10.233.81.154  (mysql-8.0.22 ndb-8.0.22)
id=50   @10.233.86.2  (mysql-8.0.22 ndb-8.0.22)

[mysqld(API)]   2 node(s)
id=56   @10.233.81.164  (mysql-8.0.22 ndb-8.0.22)
id=57   @10.233.96.39  (mysql-8.0.22 ndb-8.0.22)

[cloud-user@vcne2-bastion-1 ~]$
```

SEPP DB Backup

If the SEPP database backup is required, do the following:

1. Log in to any of the SQL node or API node, and then run the following command to take dump of the database:

   ```
   kubectl exec -it <sql node> -n <namespace> bash
   mysqldump --quick -h127.0.0.1 –u <username> -p  <databasename>| gzip >
   <backup_filename>.sql.gz
   ```

   Where,

- <sql node> is the SQL node of cnDBTier.
- <namespace> is the namespace where cnDBTier is deployed.
- <username> is the database username.
- <databasename> is the name of the database that has to be backed up.
- <backup_filename> is the name of the backup dump file.

2. Enter the SEPP database name and password in the command when prompted. Example:

```
kubectl exec -it ndbmysqld-0 -n sepp bash
mysqldump --quick -h127.0.0.1 -u dbuser -p seppdb | gzip >
SEPPdbBackup.sql.gz
```

> **Note**
>
> Ensure that there is enough space on the directory to save the backup file.

SEPP Restore

If the SEPP database restore is required, do the following:

1. Transfer the <backup_ filename>.sql.gz file to the SQL node where you want to restore it.
2. Log in to the SQL node of the MYSQL NDB cluster on the new DB cluster and create a new database where the database needs to be restored.
3. Create database, database user, and grant permissions as described in Configuring Database, Creating Users, and Granting Permissions section.

> **Note**
>
> The database name created in this step should be the same as the database name created in the next sub step. Also, the Kubernetes secret should be the same as in the values.yaml file used for installing SEPP.

4. To restore the database to the new database created, run the following command:

```
gunzip < <backup_filename>.sql.gz | mysql -h127.0.0.1 –u <username> -p
<databaseName >
```

Example:

```
gunzip < seppdbBackup.sql.gz | mysql -h127.0.0.1 -u dbuser -p newseppdb
```

5. Enter the password when prompted.

A.2 Restoring SEPP and cnDBTier

Perform this procedure to restore SEPP, cnDBTier, and SEPP database (DB).

Prerequisites:

- Take a backup of the `custom_values.yaml` file that was used for installing SEPP.
- Take a backup of the SEPP database and restore the database as described in SEPP Database Backup and Restore. Perform this task once every evening.

If SEPP deployment is corrupted, do the following:

1. Run the following command to uninstall the corrupted SEPP deployment:

   ```
   helm uninstall <release_name> --namespace <namespace>
   ```

   Where,

   - `<release_name>` is a name used to track this installation instance.
   - `<namespace>` is the release number.

   Example:

   ```
   helm uninstall ocSEPP --namespace SEPPsvc
   ```

2. Install SEPP using the backed up copy of the `custom_values.yaml` file.
   For information about installing SEPP using Helm, see Installing SEPP section.

If cnDBTier and NF deployment is corrupted, do the following:

1. Install cnDBTier as described in *Oracle Communication Cloud Native Core DBTier Installation, Upgrade, and Fault Recovery Guide*.
2. Restore SEPP DB as described in SEPP Database Backup and Restore.
3. Install SEPP using the backed up copy of the `custom_values.yaml` file.
   For information about installing SEPP using Helm, see Installing SEPP section.

If DB Secret or cnDBTier mysql FQDN or IP or PORT is changed, do the following:

1. In the backed up copy of the `custom_values.yaml` file, update these values: `dbHost/dbPort/dbAppUserSecretName/dbPrivilegedUserSecretName`.

   ```
   # DB Connection Service IP Or Hostname with secret name.
     database:
       dbHost: "mysql-connectivity-service.seppsvc"
       dbPort: "3306"
       # K8s Secret containing Database/user/password for all services of
   SEPP interacting with DB.
       dbAppUserSecretName: "seppuser-secret"
       # K8s Secret containing Database/user/password for DB Hooks for
   creating tables
       dbPrivilegedUserSecretName: "seppprivilegeduser-secret"
   ```

2. Run the following Helm upgrade command to update the secrets for SEPP control plane microservices, such as configuration, subscription, audit, and notification, to connect to the DB with changed DB Secret or DB FQDN, IP, or Port:

   ```
   helm upgrade <release name> -f <custom_values.yaml> --namespace
   <namespace> <helm-repo>/chart_name --version <helm_version>
   ```

   Example:

   ```
   helm upgrade ocsepp -f /home/cloud-user/1.12/values.yaml /home/cloud-user/
   1.11.0/ocsepp --namespace seppsvc
   ```

A.3 Adding a Site to an Existing SEPP Georedundant Site

This section describes the procedure to add a site to an existing SEPP site.

Prerequisites

1. SEPP connected to a cnDBTier is up and running. This is referred as Site 1 or Site 2.
2. SEPP and cnDBTier versions used for Site 1 and Site 2 installation must be identified and same must be used for adding another site.

Adding a site

1. Install a new cnDBTier. This cnDBTier must act as a georedundant database to the cnDBTier in Site-1 or Site-2. For more information to install a cnDBTier, see *Oracle Communications Cloud Native Core cnDBTier User Guide*.
2. Verify the replication channel between the cnDBTier sites by sending the following request to the dbMonitor service of both the cnDBTier sites. The responses from both the cnDBTier sites must show the status of replication channel as up:

   ```
   curl http://<mysql-db-monitor-service>:8080/db-tier/status/replication/
   realtime
   ```

   Sample command:

   ```
   curl http://mysql-cluster-db-monitor-svc:8080/db-tier/status/replication/
   realtime
   ```

   Sample output:

   ```
   [{"localSiteName":"Site-1","remoteSiteName":"Site-2","remoteSiteName":"Site
   -3","replicationStatus":"UP","secondsBehindRemote":
         0}]
   ```

3. Create the required secrets to install the Site-2 or Site-3 SEPP in the same namespace as the new cnDBTier installed in step-1, by following the steps described in the "Configuring Kubernetes Secret for Accessing SEPP Database" subsection from "Installing SEPP" chapter in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
4. Run the following command to verify the secret created:

   ```
   $ kubectl describe secret <database secret name> -n <Namespace of SEPP
   deployment>
   ```

5. Install the Site-2 or Site-3 SEPP using the updated `ocsepp-custom values-<version>.yaml` file. For more information on installation procedure, see *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*
   Verify the installation as mentioned in *Oracle Communications Cloud Native Core Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide.*

6. After the installation is complete, make sure that the "DbReplicationStatusInactive" alert is not raised in the alert dashboard. If the alert exists, verify the above configuration steps. If the alert is not present, it means the DBReplication is up and the georedundant deployment of all sites is successful.

A.4 Removing a Site from an Existing Georedundant Deployment

This section describes the procedure to remove a site from an existing SEPP deployment.
Prerequisites

1. SEPP connected to a cnDBTier is up and running. This is referred as Site 1 (SEPP-1 and SEPP-2).

Procedure

This section describes the procedure to remove a site (Site1 or Site 2) from an existing georedundant SEPP deployment.

1. Uninstall the SEPP instance from the site to be removed.
   For more information on uninstallation procedure, see *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation, Upgrade, and Fault Recovery Guide*.
2. Remove the DB Replication and the NDBCluster on the site to be removed. For more information on this procedure, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

A.5 Creating Private Keys and Certificate

This section explains the procedure to create private keys and certificate for enabling HTTPs on N32 gateway and PLMN Gateway (both Ingress and Egress).

> **Note**
>
> Creating keys and certificates are outside SEPP scope and user or operator should perform this at their discretion.

Gateway supports both RSA and ECDSA signing for ingress and egress traffic. Initial algorithm selection is configured by using initialAlgorithm flag in the custom-values.yaml for each gateway.

Select as follow:

- For RSA use RS256
- For ECDSA use ES256

Certificates for selected initial algorithm must be included in the ocsepp-n32-secret and ocsepp-plmn-secret.

> **Note**
>
> **Prerequisites**:
>
> Use the following sample file of ssl.conf to configure default entries along with subject alternate name (SAN) details for your certificate.
>
> - ssl.conf has various requirements such as commonName, commonName_default, subjectAltName. Configure these values as per SEPP FQDN configuration.
> - The SEPP FQDN can be extracted from `ocsepp_custom_values_<version>.yaml` file localProfile:interPlmnFqdn:
> - Other commands require similar configuration. Keep these parameters consistent across commands.

1. Use the following sample file of ssl.conf to configure default entries along with subject alternate name (SAN) details for your certificate: Run the following command to create ssl.conf file:

   Update the following parameters with SEPP inter PLMN FQDN to be used in TLS certificate:

   - commonName_default
   - commonName
   - DNS.1

   ```
   cat > ssl.conf << EOF
   ```

```
#ssl.conf
[ req ]
default_bits = 4096
distinguished_name = req_distinguished_name
req_extensions = req_ext

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = IN
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Karnataka
localityName = Locality Name (eg, city)
localityName_default = Bangalore
organizationName = Organization Name (eg, company)
organizationName_default = Oracle
commonName = sepp2.inter.oracle.com
commonName_max = 64
commonName_default = sepp2.inter.oracle.com

[ req_ext ]
subjectAltName = @alt_names

[alt_names]
IP = 127.0.0.1
DNS.1 = sepp2.inter.oracle.com
EOF
```

RSA Certificate Generation (To be done for consumer SEPP and producer SEPP individually)

2. Run the following command to generate RSA private key:

```
//Generate rsa_certificate.crt and rsa_private_key

openssl req -x509 -nodes -sha256 -days 365 -newkey rsa:2048 -keyout
rsa_private_key -out rsa_certificate.crt -subj '/C=IN/ST=Karnataka/
L=Bangalore/O=Oracle/CN=sepp2.inter.oracle.com'
```

3. Run the following command to convert the private key to .pem format:

```
//Generate rsa_private_key_pkcs1.pem
openssl rsa -in rsa_private_key -outform PEM -out rsa_private_key_pkcs1.pem
```

4. Run the following command to generate a certificate using private key:

```
/Generate ocsepp.csr
openssl req -new -key rsa_private_key -out ocsepp.csr -config ssl.conf -
subj '/C=IN/ST=Karnataka/L=Bangalore/O=Oracle/CN=sepp2.inter.oracle.com'
```

5. Run the following command to generate serial.txt file:

```
///Generate serial.txt
echo 1234 > serial.txt
```

Root CA creation for self signed certificates (Only done once for any SEPP)

6. Run the following set of commands to create root certificate authority (CA):

```
//Generate cakey.pem and careq.pem
openssl req -new -keyout cakey.pem -out careq.pem -passout pass:$
{PEM_PHRASE} -subj "/C=IN/ST=Karnataka/L=Bangalore/O=Oracl/
CN=sepp2.inter.oracle.com"

//Genearte caroot.cer
openssl x509 -signkey cakey.pem -req -days 3650 -in careq.pem -out
caroot.cer -extensions v3_ca -passin pass:${PEM_PHRASE}
```

Self Signing RSA Certificates (To be done for consumer and producer SEPP individually)

7. Run the following command to sign the server certificate with root CA private key:

```
openssl x509 -CA caroot.cer -CAkey cakey.pem -CAserial serial.txt -req -in
ocsepp.csr -out ocsepp.cer -days 365 -extfile ssl.conf -extensions req_ext
-passin pass:${PEM_PHRASE}
```

ECDSA Certificate Generation and Self Signing (To be done for consumer SEPP and producer SEPP individually)

8. Run the following command to generate ECDSA private key and certificate using private key. After that sign the server certificate with root CA private key:

```
openssl ecparam -genkey -name prime256v1 -out host.key

openssl req -new -sha256 -key host.key -nodes -out ecdsa_certificate.csr -
config ssl.conf -subj "/C=IN/ST=Karnataka/L=Bangalore/O=Oracle/
CN=sepp2.inter.oracle.com"

openssl x509 -CA caroot.cer -req -sha256 -days 730 -in
ecdsa_certificate.csr -CAkey cakey.pem -CAcreateserial -extfile ssl.conf -
extensions req_ext -out ssl_ecdsa_certificate.crt -passin pass:$
{PEM_PHRASE}

openssl pkcs8 -topk8 -in host.key -out ssl_ecdsa_private_key.pem -nocrypt
```

9. Create key.txt by entering any password. This password is used to configure gateway key store.
   Example:

```
echo "password" > key.txt
```

10. Create trust.txt by entering any password. This password is used to configure gateway trust store.
    Example:

```
echo "password" > trust.txt
```

11. Run the following commands to create a secret on n32-egress-gateway and n32-ingress-gateway:

```
kubectl create secret generic ocsepp-n32-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=trust.txt --from-file=key.txt --from-file=caroot.cer --from-
file=rsa_certificate.crt --from-file=ssl_ecdsa_certificate.crt --from-
file=ocsepp.cer -n <namespace>
```

Where, <namespace> is the namespace where SEPP is deployed. example:

```
kubectl create secret generic ocsepp-n32-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=trust.txt --from-file=key.txt --from-file=caroot.cer --from-
file=rsa_certificate.crt --from-file=ssl_ecdsa_certificate.crt --from-
file=ocsepp.cer -n seppsvc
```

12. Run the following commands to create a secret on plmn-egress-gateway and plmn-ingress-gateway:

```
kubectl create secret generic ocsepp-plmn-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=trust.txt --from-file=key.txt --from-file=caroot.cer --from-
file=rsa_certificate.crt --from-file=ssl_ecdsa_certificate.crt --from-
file=ocsepp.cer -n <namespace>
```

Where, <namespace> is the namespace where SEPP is deployed. example:

```
kubectl create secret generic ocsepp-plmn-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=trust.txt --from-file=key.txt --from-file=caroot.cer --from-
file=rsa_certificate.crt --from-file=ssl_ecdsa_certificate.crt --from-
file=ocsepp.cer -n seppsvc
```

B.1 PodDisruptionBudget Kubernetes Resource

Background

Pods are the basic units of Kubernetes and are used to deploy Cloud Native Core (CNC) Network Functions (NFs).

Pod disruption occurs due to voluntary and involuntary disruptions.

Voluntary Disruptions

Voluntary pod disruption occurs when:

- pods are removed from a cluster.
- SEPP worker nodes are drained at the time of cluster upgrade and running pods are evicted from these nodes.
- load balancing of worker nodes is performed by evenly distributing pods among worker nodes.

Involuntary Disruptions

Involuntary pod disruption occurs when:

- the system hardware or software fails.
- SEPP worker nodes are removed accidentally.
- pods are evicted due to insufficient resources on SEPP worker nodes.

Kubernetes has introduced the PodDisruptionBudgets (PDB) concept to manage pod disruption outages in the clusters. PDB is applicable only for voluntary disruptions. It is used to avoid service impact due to voluntary disruption and ensures high availability of NF.

PodDisruptionBudget SEPP Implementation Overview
PodDisruptionBudget (PDB) is a Kubernetes resource that allows you to achieve high availability of scalable application services when the cluster administrators perform voluntary disruptions to manage the cluster nodes. PDB restricts the number of pods that are down simultaneously from voluntary disruptions. Defining PDB is helpful to keep the services running undisrupted when a pod is deleted accidentally or deliberately. PDB can be defined for highly available and scalable OC SEPP services such as cn32f-svc, pn32f-svc, cn32c-svc, pn32c-svc, n32-ingress-gateway, n32-egress-gateway, plmn-ingress-gateway, plmn-egress-gateway, nfmanagement-svc, nfdiscovery-svc and perf-info services.

It allows safe eviction of pods when a Kubernetes node is drained to perform maintenance on the node. It uses the maxUnavailable parameter specified in the Helm chart to determine the maximum number of pods that can be unavailable during a voluntary disruption. For example, when a `maxUnavailable` is 25%, pod evictions are allowed as long as no more than 25% of the desired pods are in unhealthy state.

For more information about this functionality, see https://kubernetes.io/docs/concepts/workloads/pods/disruptions/#pod-disruption-budgets.

Default PodDisruptionBudget for SEPP Deployment

Table 2 Default PodDisruptionBudget for SEPP Deployment

Microservice	PDB Value Specified (maxUnavailable)
cn32c-svc	25%
pn32c-svc	25%
cn32f-svc	25%
pn32f-svc	25%
config-mgr-svc	Not Applicable
plmn-ingress-gateway	25%
plmn-egress-gateway	25%
n32-ingress-gateway	25%
n32-egress-gateway	25%
app-info	25%
config-server	50%
perf-info	25%
nf-mediation	25%
coherence-svc	25%