Oracle® Communications

Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide

Release 25.2.201
G48359-01
April 2026

ORACLE

Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide, Release 25.2.201

G48359-01

Contents

3 Customizing SCP

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 1 Acronyms

Acronym	Meaning
ASM	Aspen Service Mesh
CLI	Command Line Interface
CNC Console	Oracle Communications Cloud Native Configuration Console
cnDBTier	Oracle Communications Cloud Native Core, cnDBTier
CNE	Oracle Communications Cloud Native Core, Cloud Native Environment
CNI	Container Network Interface
CNLB	Cloud Native Load Balancer
CP	Control Plane
CSAR	Cloud Service ARchive
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
NAD	Network Attachment Definition
NRF	Oracle Communications Cloud Native Core, Network Repository Function
OCCM	Oracle Communications Cloud Native Core, Certificate Management
OCNADD	Oracle Communications Network Analytics Data Director
OHC	Oracle Help Center
OCI	Oracle Cloud Infrastructure
OKE	Oracle Kubernetes Engine
OSDC	Oracle Software Delivery Cloud
PDB	Pod Disruption Budget
SCP	Oracle Communications Cloud Native Core, Service Communication Proxy
SCPC	Service Communication Proxy Control Plane
SEPP	Oracle Communications Cloud Native Core, Security Edge Protection Proxy
SPN	Service Proto Name, a combination of service, protocol, and name will be used in DNS SRV configuration.
SRV	Service Records
SSL	Secure Sockets Layer
SVC	Services
TLS	Transport Layer Security
TPS	Transaction Per Second

What's New in This Guide

This section introduces the documentation updates for release 25.2.2xx.

Release 25.2.201 - G48359-01, April 2026

General Updates:

- Updated the release number to 25.2.201 throughout this document.
- Removed the `scpProfileInfo.mediation_status` parameter from the Global Parameters section.
- Added the `userNamespacesEnabled` parameter in the Global Parameters section. This parameter manages the Kubernetes User Namespaces feature.
- Updated the description of the `scpProfileInfo.scpInfo.scpPrefix` parameter in the Global Parameters section. This parameter is matched with `apiPrefix` present in the received request URI (for both notification and service requests).
- Updated the error correction policy in the Oracle Error Correction Policy section.
- Updated the preinstalled software versions in the Software Requirements section.
- Updated cnDBTier resource requirements in the cnDBTier Resources section.
- Updated the resource requirements of the following services in the SCP Services section:
  - Helm test
  - Helm Hook
  - <helm-release-name>-scpc-audit
- Updated the resource requirements of the following services in the ASM Sidecar section:
  - Helm test
  - Helm Hook
  - <helm-release-name>-scpc-subscription
  - <helm-release-name>-scpc-notification
  - <helm-release-name>-scpc-audit
  - <helm-release-name>-scpc-configuration
  - scpc-alternate-resolution
  - <helm-release-name>-scp-nrfproxy
  - <helm-release-name>-scp-oauth-nrfproxy
  - scp-worker (profile 1)
- Added the following Helm parameters in the Global Parameters section:
  - `customExtension.hooks.labels`
  - `customExtension.hooks.annotations`
  - `customExtension.serviceaccount.labels`
  - `customExtension.serviceaccount.annotations`
  - `podResources.limits`

  - `podResources.requests`
  - `scpProfileInfo`
  - `scpPreferInternalTrafficOnIPv6`

Installation Updates:

- Updated the concurrency of SCP-Worker pods to 20 for a 12vCPU profile in the Deploying SCP with ASM section.
- Added a note about updating the cnDBTier resources before installing or upgrading the CNC Console in the CNC Console Requirements section.

Upgrade, Rollback, and Uninstall Updates:

- Updated the supported upgrade paths in the Supported Upgrade Paths section.
- Updated the supported rollback paths in Supported Rollback Paths section.
- Added a procedure to migrate SCP to an ASM-disabled cnDBTier in the Migrating SCP to Support an ASM Disabled cnDBTier section.
- Added a step about updating `MaxNoOfAttributes`, `MaxNoOfOrderedIndexes`, `MaxNoOfTables`, and `MaxNoOfUniqueHashIndexes` parameters in the Preupgrade Tasks section.

1 Introduction

This guide describes how to install or upgrade Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) in a cloud native environment and Oracle Cloud Infrastructure (OCI). It also includes information on performing fault recovery for SCP.

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

SCP is a decentralized solution composed of Service Proxy Controllers and Service Proxy Workers. It is deployed alongside 5G network functions and provides routing control, resiliency, and observability to the core network. For more information about SCP architecture and features, see *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

SCP can leverage the service mesh for internal and external communications. The service mesh integration provides inter-NF communication and allows coworking with service mesh. The service mesh integration supports the services by deploying a special sidecar proxy in the environment to intercept network communications between microservices. For information about installing SCP with Aspen Service Mesh (ASM), see Configuring SCP to Support Aspen Service Mesh.

Note

The performance and capacity of the SCP system may vary based on the call model, feature or interface configuration, network conditions, and underlying CNE and hardware environment.

1.2 References

Refer to the following documents while deploying SCP:

- *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*
- *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*
- *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Operations Services Overlay Installation Guide*
- *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*
- *Oracle Communications Cloud Native Core, Network Function Data Collector User Guide*
- *Oracle Communications Network Analytics Data Director Installation, Upgrade, and Fault Recovery 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 Configuration Console Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core Automated Testing Suite Guide*
- *Oracle Communications Cloud Native Core Release Notes*

1.3 Oracle Error Correction Policy

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

Table 1-1 Oracle Error Correction Policy

Release Number	General Availability (GA) Date	Error Correction Grace Period End Date
3.25.2.200	April 2026	April 2027
3.25.2.100	November 2025	November 2026
3.25.1.200	July 2025	July 2026
3.25.1.100	April 2025	April 2026

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.

1.4 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 SCP

This chapter provides information about installing SCP in a cloud native environment, including the prerequisites and downloading the deployment package.

> **Note**
>
> SCP supports fresh installation, and it can also be upgraded from 25.1.2xx and 25.2.1xx. For more information about how to upgrade SCP, see Upgrading SCP.

SCP 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 Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
- Oracle Cloud Infrastructure (OCI) using OCI Adaptor: For more information about OCI, see *Oracle Communications Cloud Native Core, OCI Deployment Guide*.

SCP installation comprises of prerequisites, preinstallation, installation, and postinstallation tasks. You must perform SCP installation tasks in the same sequence as outlined in the following table:

Table 2-1 SCP Installation Tasks

Installation Sequence	Applicable for CNE Deployment	Applicable for OCI Deployment
Prerequisites	Yes	Yes
Software Requirements	Yes	Yes
Environment Setup Requirements	Yes	Yes
Resource Requirements	Yes	Yes
Preinstallation Tasks	Yes	Yes
Downloading the SCP Package	Yes	Yes
Pushing the Images to Customer Docker Registry	Yes	No
Pushing the SCP Images to OCI Docker Registry	No	Yes
Verifying and Creating Namespace	Yes	Yes
Manually Creating Service Account, Role, and Rolebinding	Yes	Yes
Automatically Creating Service Account, Role, and Rolebinding	Yes	Yes
Configuring Database for SCP	Yes	Yes
Configuring Kubernetes Secret for Accessing Database	Yes	Yes
Configuring SSL or TLS Certificates to Enable HTTPS	Yes	Yes
Configuring SSL or TLS Certificates for OCNADD	Yes	Yes
Configuring SCP to Support Aspen Service Mesh	Yes	Yes
Configuring Network Policies for SCP	Yes	Yes
Installation Tasks	Yes	Yes

Table 2-1 (Cont.) SCP Installation Tasks

Installation Sequence	Applicable for CNE Deployment	Applicable for OCI Deployment
Installing SCP Package	Yes	Yes
Postinstallation Tasks	Yes	Yes

2.1 Prerequisites

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

2.1.1 Software Requirements

This section lists the software that must be installed before installing SCP.

> **Note**
>
> Table 2-2 and Table 2-3 offer a comprehensive list of software necessary for the proper functioning of SCP 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.

The following software must be installed before installing SCP:

Table 2-2 Preinstalled Software Versions

Software	25.2.2xx	25.2.1xx	25.1.2xx	Software Requirement	Usage Description
Helm	3.19.1	3.18.2	3.17.1	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.

Table 2-2 (Cont.) Preinstalled Software Versions

Software	25.2.2xx	25.2.1xx	25.1.2xx	Software Requirement	Usage Description
Kubernetes	1.34.1	1.33.1	1.32.0	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.
Podman	5.6.0	5.2.2	4.9.4	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 versions of the preinstalled software in the cloud native environment, run the following commands:

```
kubectl version
```

```
helm version
```

```
podman version
```

> **Note**
>
> This guide covers the installation instructions for SCP 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*.

The following software are available if SCP is deployed in CNE. If you are deploying SCP in any other cloud native environment, these additional software must be installed before installing SCP.

To check the installed software, run the following command:

```
helm ls -A
```

The list of additional software items, along with the supported versions and usage, is provided in the following table:

Table 2-3 Additional Software Versions

Software	25.2.2xx	25.1.2xx Software Requirement	Usage Description
AlertManager	0.28.0	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	3.30.3	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	1.33.0	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.
containerd	2.0.5	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	1.12.0	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	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.

Table 2-3 (Cont.) Additional Software Versions

Software	25.2.2xx	25.1.2xx Software Requirement	Usage Description
Grafana	7.5.17	9.5.13 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	1.72.0	1.69.0 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	1.15.0	1.11.4 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.
MetalLB	0.15.2	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 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	4.2.1	4.1.3 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	2.18.0	2.11.85.00 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.

Table 2-3 (Cont.) Additional Software Versions

Software	25.2.2xx	25.1.2xx Software Requirement	Usage Description
OpenSearch Dashboard	2.18.0	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.
Prometheus	3.6.0	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	2.16.0	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	1.9.1	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	0.83.0	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	1.16.7	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	2.0.0	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	25.2.2xx	25.1.2xx	Software Requirement	Usage Description
Velero	1.13.2	1.13.2	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.

> **Note**
>
> On OCI, the above mentioned software are not required because OCI observability and management service is used for logging, metrics, alerts, and KPIs. For more information, see *Oracle Communications Cloud Native Core, OCI Deployment Guide*.

2.1.2 Environment Setup Requirements

This section describes the environment setup requirements for installing SCP.

2.1.2.1 Client Machine Requirement

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.
- network access to the Helm repository and Docker image repository.
- network access to the Kubernetes cluster.
- required environment settings to run `kubectl`, `docker`, and `podman` commands. The environment should have privileges to create a 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 Requirements

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

- Local Helm repository: It contains SCP Helm charts.

To check if the Kubernetes cluster hosts can access the local Helm repository, run the following command:

```
helm repo update
```

- Local Docker image repository: It contains SCP Docker images.
  To check if the Kubernetes cluster hosts can access the local Docker image repository, 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 repository.
- `<podman-repo>` is the IP address or host name of the Podman repository.
- `<image-name>` is the Docker image name.
- `<image-tag>` is the tag assigned to the Docker image used for the SCP pod.

For example:

```
docker pull CUSTOMER_REPO/oc-app-info:25.2.201
```

```
podman pull occne-repo-host:5000/ocscp/oc-app-info:25.2.201
```

> **Note**
>
> Run `kubectl` and `helm` commands on a system based on the deployment infrastructure. For example, they can be run on a client machine such as VM, server, local desktop, and so on.

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 SCP on Cloud Native Environment (CNE).

SCP supports CNE 25.2.2xx, 25.2.1xx, and 25.1.2xx.

To check the CNE version, run the following command:

```
echo $OCCNE_VERSION
```

> **Note**
>
> 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 namespace of SCP, cnDBTier, or Oracle Communications Cloud Native Configuration Console (CNC Console).

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

2.1.2.5 OCI Requirements

SCP can be deployed in OCI. While deploying SCP in OCI, the user must use the Operator instance/VM instead of Bastion Host.

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

2.1.2.6 cnDBTier Requirements

> **Note**
>
> Obtain the values of the cnDBTier parameters listed in cnDBTier Customization Parameters from the delivered `ocscp_dbtier_custom_values.yaml` file and use these values in the new `ocscp_dbtier_custom_values.yaml` file if the parameter values in the new `ocscp_dbtier_custom_values.yaml` file are different from the delivered `ocscp_dbtier_custom_values.yaml` file.

SCP supports cnDBTier 25.2.2xx, 25.2.1xx, and 25.1.2xx. cnDBTier must be configured and running before installing SCP.

> **Note**
>
> In georedundant deployment, each site should have a dedicated cnDBTier.

To install cnDBTier 25.2.2xx with resources recommended for SCP, customize the `ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml` file in the `ocscp_csar_25_2_2_0_1_0.zip` folder with the required deployment parameters. cnDBTier parameters will vary depending on whether the deployment is on a single site, two site, or three site. For more information, see cnDBTier Customization Parameters.

> **Note**
>
> If you already have an older version of cnDBTier, upgrade cnDBTier with resources recommended for SCP by customizing the `ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml` file in the `ocscp_csar_25_2_2_0_1_0.zip` folder with the required deployment parameters. Use the same PVC size as it was in the previous release. For more information, see cnDBTier Customization Parameters.

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

2.1.2.7 OCCM Requirements

SCP supports OCCM 25.2.2xx.
To support automated certificate lifecycle management, SCP integrates with Oracle Communications Cloud Native Core, Certificate Management (OCCM) in compliance with 3GPP security recommendations. For more information about OCCM, see the following guides:

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

2.1.2.8 OSO Requirement

SCP supports Operations Services Overlay (OSO) 25.2.2xx, 25.2.1xx, and 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 Guide*.

2.1.2.9 CNC Console Requirements

SCP supports CNC Console 25.2.2xx to configure and manage Network Functions. For more information, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide .*

> **Note**
>
> Before starting the CNC Console installation or upgrade, ensure that the cnDBTier across all sites is updated with the latest maximum limit values. For cnDBTier limit references, see the values of the following parameters in Table 3-14:
>
> - `MaxNoOfAttributes`
> - `MaxNoOfOrderedIndexes`
> - `MaxNoOfTables`
> - `MaxNoOfUniqueHashIndexes`
>
> If your deployment shares a cnDBTier between SCP and the CNC Console, the SCP DB profile sizing should incorporate the CNC Console DB profile requirements, along with the new cnDBTier max limit values.

2.1.3 Resource Requirements

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

> **Note**
>
> The performance and capacity of the SCP system may vary based on the call model, feature or interface configuration, network conditions, and underlying CNE and hardware environment.

2.1.3.1 SCP Services

The following table lists resource requirement for SCP Services:

Table 2-4 SCP Services

Service Name	SCP Service PODs						Ephemeral Storage Per Pod	
	Pod Replica		vCPU/Pod		Memory in Gi/Pod		Minimum Value in Mi (If Enabled)	Maximum Value in Gi (If Enabled)
	Min	Max	Min	Max	Min	Max		
Helm test	1	1	**1.1**	**1.1**	**1**	**1**	70	1
Helm Hook	1	1	**1.1**	**1.1**	**1**	**1**	70	1
<helm-release-name>-scpc-subscription	1	1	2	2	2	2	70	1
<helm-release-name>-scpc-notification	1	1	8	8	8	8	70	1

Table 2-4 (Cont.) SCP Services

Service Name	SCP Service PODs						Ephemeral Storage Per Pod	
<helm-release-name>-scpc-audit	1	1	**4**	**4**	4	4	70	1
<helm-release-name>-scpc-configuration	1	1	2	2	2	2	70	1
<helm-release-name>-scpc-alternate-resolution	1	1	2	2	2	2	70	1
<helm-release-name>-scp-cache	3	3	8	8	8	8	70	1
<helm-release-name>-scp-nrfproxy	2	16	8	8	8	8	70	1
<helm-release-name>-scp-load-manager	2	3	8	8	8	8	70	1
<helm-release-name>-scp-oauth-nrfproxy	2	16	8	8	8	8	70	1
<helm-release-name>-scp-worker(profile 1)	2	32	4	4	12	12	70	1
<helm-release-name>-scp-worker(profile 2)	2	64	8	8	18	18	70	1
<helm-release-name>-scp-mediation	2	16	8	8	8	8	70	1
<helm-release-name>-scp-mediation test	1	1	8	8	8	8	70	1

Table 2-4 (Cont.) SCP Services

Service Name	SCP Service PODs						Ephemeral Storage Per Pod	
<helm-release-name>-scp-worker(profile 3)	2	64	12	12	24	24	70	1

> **Note**
>
> - To go beyond 60000 Transactions Per Second (TPS), you must deploy SCP with scp-worker configured with Profile 2.
> - <helm-release-name> will be prefixed in each microservice name. For example, if the Helm release name is OCSCP, then the SCPC-Subscription microservice name will be "OCSCP-SCPC-Subscription".
> - **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.

2.1.3.2 Upgrade

Following is the resource requirement for upgrading SCP.

Table 2-5 Upgrade

Service Name	Upgrade Resources						Ephemeral Storage Per Pod	
	Pod Replica		vCPU/Pod		Memory in Gi/Pod		Minimum Value in Mi (If Enabled)	Maximum Value in Gi (If Enabled)
	Min	Max	Min	Max	Min	Max		
Helm test	0	0	0	0	0	0	70	1
Helm Hook	0	0	0	0	0	0	70	1
<helm-release-name>-scpc-subscription	1	1	2	2	2	2	70	1
<helm-release-name>-scpc-notification	1	1	8	8	8	8	70	1

Table 2-5 (Cont.) Upgrade

Service Name	Upgrade Resources						Ephemeral Storage Per Pod	
<helm-release-name>-scpc-audit	1	1	3	3	4	4	70	1
<helm-release-name>-scpc-configuration	1	1	2	2	2	2	70	1
<helm-release-name>-scpc-alternate-resolution	1	1	2	2	2	2	70	1
<helm-release-name>-scp-cache	1	1	8	8	8	8	70	1
<helm-release-name>-scp-nrfproxy	1	4	8	8	8	8	70	1
<helm-release-name>-scp-load-manager	1	1	8	8	8	8	70	1
<helm-release-name>-scp-oauth-nrfproxy	1	4	8	8	8	8	70	1
<helm-release-name>-scp-worker(profile 1)	2	8	4	4	12	12	70	1
<helm-release-name>-scp-worker(profile 2)	2	16	8	8	18	18	70	1
<helm-release-name>-scp-mediation	2	4	8	8	8	8	70	1
<helm-release-name>-scp-mediation test	0	0	0	0	0	0	70	1

Table 2-5 (Cont.) Upgrade

Service Name	Upgrade Resources						Ephemeral Storage Per Pod	
<helm-release-name>-scp-worker(profile 3)	2	16	12	12	24	24	70	1

> **Note**
>
> <helm-release-name> will be prefixed in each microservice name. For example, if the Helm release name is OCSCP, then the SCPC-Subscription microservice name will be "OCSCP-SCPC-Subscription".

2.1.3.3 ASM Sidecar

SCP leverages the Platform Service Mesh (for example, Aspen Service Mesh) for all internal and external TLS communication. If ASM Sidecar injection is enabled during SCP deployment or upgrade, this container is injected to each SCP 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 installing ASM, see Configuring SCP to Support Aspen Service Mesh.

Table 2-6 ASM Sidecar

Service Name	ASM Sidecar				Ephemeral Storage Per Pod	
	vCPU/Pod		Memory in Gi/Pod		Minimum Value in Mi (If Enabled)	Maximum Value in Gi (If Enabled)
	Min	Max	Min	Max		
Helm test	**1.1**	**1.1**	1	1	70	1
Helm Hook	**1.1**	**1.1**	**1**	**1**	70	1
<helm-release-name>-scpc-subscription	**2**	**2**	1	1	70	1
<helm-release-name>-scpc-notification	**4**	**4**	3	3	70	1
<helm-release-name>-scpc-audit	**2**	**2**	1	1	70	1
<helm-release-name>-scpc-configuration	**1.1**	**1.1**	1	1	70	1
scpc-alternate-resolution	**1.1**	**1.1**	1	1	70	1
<helm-release-name>-scp-cache	4	4	4	4	70	1
<helm-release-name>-scp-nrfproxy	**6**	**6**	5	5	70	1

Table 2-6 (Cont.) ASM Sidecar

Service Name	ASM Sidecar				Ephemeral Storage Per Pod	
<helm-release-name>-scp-load-manager	4	4	4	4	70	1
<helm-release-name>-scp-oauth-nrfproxy	**6**	**6**	5	5	70	1
scp-worker (profile 1)	**4**	**4**	4	4	70	1
<helm-release-name>-scp-worker (profile 2)	6	6	6	6	70	1
<helm-release-name>-scp-mediation	0	0	0	0	70	1
<helm-release-name>-scp-mediation test	0	0	0	0	70	1
<helm-release-name>-scp-worker (profile 3)	10	10	10	10	70	1

> **Note**
>
> <helm-release-name> will be prefixed in each microservice name. For example, if the Helm release name is OCSCP, then the SCPC-Subscription microservice name will be "OCSCP-SCPC-Subscription".

2.1.3.4 Debug Tool Container

The Debug Tool Container provides third-party troubleshooting tools for debugging the runtime issues in a lab environment. If Debug Tool Container injection is enabled during SCP deployment or upgrade, this container is injected to each SCP 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 Container, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.

Table 2-7 Debug Tool Container

Service Name	Debug Tool Container				Ephemeral Storage Per Pod	
	vCPU/Pod		Memory in Gi/Pod		Minimum Value in Mi (If Enabled)	Maximum Value in Gi (If Enabled)
	Min	Max	Min	Max		
Helm test	0	0	0	0	70	1
Helm Hook	0	0	0	0	70	1
<helm-release-name>-scpc-subscription	1	1	2	2	70	1

Table 2-7 (Cont.) Debug Tool Container

Service Name	Debug Tool Container				Ephemeral Storage Per Pod	
<helm-release-name>-scpc-notification	1	1	2	2	70	1
<helm-release-name>-scpc-audit	1	1	2	2	70	1
<helm-release-name>-scpc-configuration	1	1	2	2	70	1
<helm-release-name>-scpc-alternate-resolution	1	1	2	2	70	1
<helm-release-name>-scp-cache	1	1	2	2	70	1
<helm-release-name>-scp-nrfproxy	1	1	2	2	70	1
<helm-release-name>-scp-load-manager	1	1	2	2	70	1
<helm-release-name>-scp-oauth-nrfproxy	1	1	2	2	70	1
<helm-release-name>-scp-worker(profile 1)	1	1	2	2	70	1
<helm-release-name>-scp-worker(profile 2)	1	1	2	2	70	1
<helm-release-name>-scp-mediation	1	1	2	2	70	1
<helm-release-name>-scp-mediation test	1	1	2	2	70	1
<helm-release-name>-scp-worker (profile 3)	1	1	2	2	70	1

> **Note**
>
> <helm-release-name> will be prefixed in each microservice name. For example, if the Helm release name is OCSCP, then the SCPC-Subscription microservice name will be "OCSCP-SCPC-Subscription".

2.1.3.5 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 SCP, see *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* .

2.1.3.6 cnDBTier Resources

This section describes the cnDBTier resources required to deploy SCP.

Table 2-8 cnDBTier Resource Requirements (Non-ASM)

Service Name	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
postInstallJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
preUpgradeJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
preRollbackJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
postUpgradeJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
postRollbackJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
helm-test	0.1	0.1	256Mi		NA	NA	90Mi	1Gi
MGMT (ndbmgmd)	2	2	4	5	14	NA	90	1000
DB (ndbmtd)	2	2	8	8	14	6	90	1000
SQL - Replication (ndbmysqld)	4	4	10	10	25	NA	90	1000
SQL - Access (ndbappmysqld)	4	4	8	8	20	NA	90	1000
Monitor Service (db-monitor-svc)	4	4	4	4	0	NA	90	1000
db-connectivity-service	0	0	0	0	0	NA	0	0
Replication Service(db-replication-svc)	2	2	12	12	190	NA	90	1000
Replication Service - Other(db-replication-svc)	1.1	1.1	1	2	NA	NA	90	1000
Backup Manager Service (db-backup-manager-svc)	1.1	1.1	1	1	0	NA	90	1000

Table 2-9 cnDBTier Resource Requirements (Non-ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
postInstallJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
postInstallJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-9 (Cont.) cnDBTier Resource Requirements (Non-ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
postInstallJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
postInstallJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-9 (Cont.) cnDBTier Resource Requirements (Non-ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
helm-test init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
helm-test db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
helm-test init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
helm-test db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) db-infra-monitor-svc	0.2	0.2	0.256	0.256	14	NA	90	1000
DB (ndbmtd) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
DB (ndbmtd) db-executor-svc	2	2	2	2	14	6	90	1000
DB (ndbmtd) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
DB (ndbmtd) db-infra-monitor-svc	0.2	0.2	0.256	0.256	14	6	90	1000
SQL - Replication (ndbmysqld) init-sidecar	0.1	0.1	0.256	0.256	25	NA	90	1000
SQL - Replication (ndbmysqld) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
SQL - Replication (ndbmysqld) init-discover-sql-ips	0.2	0.2	0.256	0.256	25	NA	90	1000

Table 2-9 (Cont.) cnDBTier Resource Requirements (Non-ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
SQL - Replication (ndbmysqld) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
SQL - Access (ndbappmysqld) init-sidecar	0.1	0.1	0.256	0.256	20	NA	90	1000
SQL - Access (ndbappmysqld) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
SQL - Access (ndbappmysqld) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
SQL - Access (ndbappmysqld) db-infra-monitor-svc	0.2	0.2	0.256	0.256	20	NA	90	1000
Monitor Service (db-monitor-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
Monitor Service (db-monitor-svc) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Monitor Service (db-monitor-svc) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
Monitor Service (db-monitor-svc) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-9 (Cont.) cnDBTier Resource Requirements (Non-ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
Replication Service(db-replication-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service(db-replication-svc) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service(db-replication-svc) init-discover-sql-ips	0.2	0.2	0.5	0.5	190	NA	90	1000
Replication Service(db-replication-svc) db-infra-monitor-svc	0.2	0.2	0.256	0.256	190	NA	90	1000
Replication Service - Other(db-replication-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service - Other(db-replication-svc) db-executor-svc	0.2	0.2	0.5	0.5	NA	NA	90	1000
Replication Service - Other(db-replication-svc) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service - Other(db-replication-svc) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Backup Manager Service (db-backup-manager-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
Backup Manager Service (db-backup-manager-svc) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-9 (Cont.) cnDBTier Resource Requirements (Non-ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
Backup Manager Service (db-backup-manager-svc) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
Backup Manager Service (db-backup-manager-svc) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-10 cnDBTier Resource Requirements (ASM)

Service Name	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
postInstallJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
preUpgradeJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
preRollbackJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
postUpgradeJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
postRollbackJob	0.1	0.1	256Mi	256Mi	NA	NA	90Mi	1Gi
helm-test	0.1	0.1	256Mi		NA	NA	90Mi	1Gi
MGMT (ndbmgmd)	2	2	4	5	14	NA	90	1000
DB (ndbmtd)	2	2	8	8	14	6	90	1000
SQL - Replication (ndbmysqld)	4	4	10	10	25	NA	90	1000
SQL - Access (ndbappmysqld)	4	4	8	8	20	NA	90	1000
Monitor Service (db-monitor-svc)	4	4	4	4	0	NA	90	1000
db-connectivity-service	0	0	0	0	0	NA	0	0
Replication Service(db-replication-svc)	2	2	12	12	190	NA	90	1000
Replication Service - Other(db-replication-svc)	1.1	1.1	1	2	NA	NA	90	1000
Backup Manager Service (db-backup-manager-svc)	1.1	1.1	1	1	0	NA	90	1000

Table 2-11 cnDBTier Resource Requirements (ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
postInstallJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
postInstallJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postInstallJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
postInstallJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postInstallJob sevice mesh sidecar (envoy)	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preUpgradeJob sevice mesh sidecar (envoy)	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
preRollbackJob sevice mesh sidecar (envoy)	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-11 (Cont.) cnDBTier Resource Requirements (ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
postUpgradeJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postUpgradeJob sevice mesh sidecar (envoy)	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
postRollbackJob sevice mesh sidecar (envoy)	NA	NA	NA	NA	NA	NA	NA	NA
helm-test init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
helm-test db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
helm-test init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
helm-test db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
helm-test sevice mesh sidecar (envoy)	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
MGMT (ndbmgmd) db-infra-monitor-svc	0.2	0.2	0.256	0.256	14	NA	90	1000

Table 2-11 (Cont.) cnDBTier Resource Requirements (ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
MGMT (ndbmgmd) sevice mesh sidecar (envoy)	2	2	1	1	14	NA	90	1000
DB (ndbmtd) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
DB (ndbmtd) db-executor-svc	2	2	2	2	14	6	90	1000
DB (ndbmtd) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
DB (ndbmtd) db-infra-monitor-svc	0.2	0.2	0.256	0.256	14	6	90	1000
DB (ndbmtd) sevice mesh sidecar (envoy)	2	2	1	1	14	6	90	1000
SQL - Replication (ndbmysqld) init-sidecar	0.1	0.1	0.256	0.256	25	NA	90	1000
SQL - Replication (ndbmysqld) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
SQL - Replication (ndbmysqld) init-discover-sql-ips	0.2	0.2	0.256	0.256	25	NA	90	1000
SQL - Replication (ndbmysqld) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
SQL - Replication (ndbmysqld) sevice mesh sidecar (envoy)	2	2	2	2	25	NA	90	1000
SQL - Access (ndbappmysqld) init-sidecar	0.1	0.1	0.256	0.256	20	NA	90	1000
SQL - Access (ndbappmysqld) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
SQL - Access (ndbappmysqld) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-11 (Cont.) cnDBTier Resource Requirements (ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
SQL - Access (ndbappmysqld) db-infra-monitor-svc	0.2	0.2	0.256	0.256	20	NA	90	1000
SQL - Access (ndbappmysqld) sevice mesh sidecar (envoy)	2	2	2	2	20	NA	90	1000
Monitor Service (db-monitor-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
Monitor Service (db-monitor-svc) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Monitor Service (db-monitor-svc) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
Monitor Service (db-monitor-svc) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Monitor Service (db-monitor-svc) sevice mesh sidecar (envoy)	2	2	1	1	NA	NA	NA	NA
db-connectivity-service init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
db-connectivity-service sevice mesh sidecar (envoy)	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service(db-replication-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA

Table 2-11 (Cont.) cnDBTier Resource Requirements (ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
Replication Service(db-replication-svc) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service(db-replication-svc) init-discover-sql-ips	0.2	0.2	0.5	0.5	190	NA	90	1000
Replication Service(db-replication-svc) db-infra-monitor-svc	0.2	0.2	0.256	0.256	190	NA	90	1000
Replication Service(db-replication-svc) sevice mesh sidecar (envoy)	2	2	1	1	190	NA	90	1000
Replication Service - Other(db-replication-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service - Other(db-replication-svc) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service - Other(db-replication-svc) init-discover-sql-ips	0.2	0.2	0.5	0.5	NA	NA	90	1000
Replication Service - Other(db-replication-svc) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Replication Service - Other(db-replication-svc) sevice mesh sidecar (envoy)	2	2	1	1	NA	NA	90	1000

Table 2-11 (Cont.) cnDBTier Resource Requirements (ASM with Sidecar)

Service Name with Sidecar	CPU/Pod		Memory/Pod (in GB)		PVC Size (in GB)		Ephemeral Storage	
	Min	Max	Min	Max	PVC1	PVC2	Min (MB)	Max (MB)
Backup Manager Service (db-backup-manager-svc) init-sidecar	NA	NA	NA	NA	NA	NA	NA	NA
Backup Manager Service (db-backup-manager-svc) db-executor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Backup Manager Service (db-backup-manager-svc) init-discover-sql-ips	NA	NA	NA	NA	NA	NA	NA	NA
Backup Manager Service (db-backup-manager-svc) db-infra-monitor-svc	NA	NA	NA	NA	NA	NA	NA	NA
Backup Manager Service (db-backup-manager-svc) sevice mesh sidecar (envoy)	2	2	1	1	NA	NA	90	1000

2.1.3.7 OSO Resources

This section describes the OSO resources required to deploy SCP.

Table 2-12 OSO Resource Requirement

Microservice Name	CPU		Memory (GB)		Replica
	Min	Max	Min	Max	
prom-alertmanager	0.5	0.5	2	2	2
prom-server	16	16	64	64	1

2.1.3.8 OCCM Resources

OCCM manages certificate creation, recreation, renewal, and so on for SCP. For information about OCCM resources required by SCP, see *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*.

2.2 Installation Sequence

This section describes preinstallation, installation, and postinstallation tasks for SCP.

You must perform these tasks after completing Prerequisites and in the same sequence as outlined in the following table.

Table 2-13 SCP Installation Sequence

Installation Sequence	Applicable for CNE Deployment	Applicable for OCI Deployment
Preinstallation Tasks	Yes	Yes
Installation Tasks	Yes	Yes
Postinstallation Tasks	Yes	Yes

2.2.1 Preinstallation Tasks

To install SCP, perform the tasks described in this section.

2.2.1.1 Downloading the SCP Package

To download the SCP package from My Oracle Support (MOS), perform the following procedure:

1. Log in to My Oracle Support (MOS) using your login credentials.
2. Click the **Patches & Updates** tab to locate the patch.
3. In the Patch Search console, click **Product or Family (Advanced)**.
4. In the **Product** field, enter `Oracle Communications Cloud Native Core - 5G`.
5. From the **Release** drop-down list, select `Oracle Communications Cloud Native Core Service Communication Proxy <release_number>`.
   Where, `<release_number>` indicates the required release number of SCP.
6. Click **Search**.
   The Patch Advanced Search Results list appears.
7. From the Patch Name column, select the required patch number.
   The Patch Details window appears.
8. Click **Download**.
   The File Download window appears.
9. Click the `<p********>_<release_number>_Tekelec.zip` file to download the release package.
   Where, `<p********>` is the MOS patch number and `<release_number>` is the release number of SCP.

2.2.1.2 Pushing the Images to Customer Docker Registry

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

SCP Images

The following table lists the Docker images of SCP:

Table 2-14 Images for SCP

Microservices	Image	Tag
<helm-release-name>-SCP-Worker	ocscp-worker	25.2.201
<helm-release-name>-SCPC-Configuration	ocscp-configuration	25.2.201
<helm-release-name>-SCPC-Notification	ocscp-notification	25.2.201
<helm-release-name>-SCPC-Subscription	ocscp-subscription	25.2.201
<helm-release-name>-SCPC-Audit	ocscp-audit	25.2.201
<helm-release-name>-SCPC-Alternate-Resolution	ocscp-alternate-resolution	25.2.201
<helm-release-name>-SCP-Cache	ocscp-cache	25.2.201
<helm-release-name>-SCP-nrfproxy	ocscp-nrfproxy	25.2.201
<helm-release-name>-SCP-nrfProxy-oauth	ocscp-nrfproxy-oauth	25.2.201
<helm-release-name>-SCP-Mediation	ocmed-nfmediation	25.2.201
<helm-release-name>-SCP-loadManager	ocscp-load-manager	25.2.201

> **Note**
>
> <helm-release-name> will be prefixed in each microservice name. For example, if the Helm release name is OCSCP, then the SCPC-Subscription microservice name will be "OCSCP-SCPC-Subscription".

To push the images to the registry:

1. Navigate to the location where you want to install SCP, and then unzip the SCP release package (`<p********>_<release_number>_Tekelec.zip`) to retrieve the following CSAR package.
   The SCP 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, `ocscp_csar_25_2_2_0_1_0.zip`.
2. Untar the SCP package to retrieve the OCSCP image tar file: `unzip <ReleaseName>_csar_<Releasenumber>.zip`.
   For example, `unzip ocscp_csar_25_2_2_0_1_0.zip`

   The zip file consists of the following:

```
|—— Definitions
|    ├—— ocscp_cne_compatibility.yaml
```

```
│   └── ocscp.yaml
├── Files
│   ├── ChangeLog.txt
│   ├── Helm
│   │   ├── ocscp-25.2.201.tgz
│   │   └── ocscp-network-policy-25.2.201.tgz
│   ├── Licenses
│   ├── nf-test-25.2.201.tar
│   ├── ocdebug-tools-25.2.201.tar
│   ├── ocmed-nfmediation-25.2.201.tar
│   ├── ocscp-alternate-resolution-25.2.201.tar
│   ├── ocscp-audit-25.2.201.tar
│   ├── ocscp-cache-25.2.201.tar
│   ├── ocscp-configuration-25.2.201.tar
│   ├── ocscp-load-manager-25.2.201.tar
│   ├── ocscp-notification-25.2.201.tar
│   ├── ocscp-nrfproxy-25.2.201.tar
│   ├── ocscp-subscription-25.2.201.tar
│   ├── ocscp-nrfProxy-oauth-25.2.201.tar
│   ├── ocscp-worker-25.2.201.tar
│   ├── Oracle.cert
│   └── Tests
├── ocscp.mf
├── Scripts
│   ├── ocscp_alerting_rules_promha.yaml
│   ├── ocscp_alertrules.yaml
│   ├── ocscp_configuration_openapi_25.2.201.json
│   ├── ocscp_custom_values_25.2.201.yaml
│   ├── ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml
│   ├── ocscp_metric_dashboard_25.2.201.json
│   ├── ocscp_metric_dashboard_promha_25.2.201.json
│   ├── ocscp_mib_25.2.201.mib
│   ├── ocscp_mib_tc_25.2.201.mib
│   ├── ocscp_network_policies_values_25.2.201.yaml
│   ├── ocscp_servicemesh_config_values_25.2.201.yaml
│   └── toplevel.mib
├── Scripts
│   ├── oci
│   │   └── ocscp_oci_alertrules_25.2.201.zip
│   │   └── ocscp_oci_metric_dashboard_25.2.201.zip
└── TOSCA-Metadata
    └── TOSCA.meta
```

3. Open the `Files` folder and run one of the following commands to load `ocscp-images-25.2.201.tar`:

   ```
   podman load --input /IMAGE_PATH/ocscp-images-<release_number>.tar
   ```

   ```
   docker load --input /IMAGE_PATH/ocscp-images-<release_number>.tar
   ```

   Example:

   ```
   docker load --input /IMAGE_PATH/ocscp-images-25.2.201.tar
   ```

4. Run one of the following commands to verify that the images are loaded:

   ```
   podman images
   ```

   ```
   docker images
   ```

   Sample Output:

   ```
   docker.io/ocscp/ocscp-cache                              25.2.201
   98fc90defb56        2 hours ago         725MB
   docker.io/ocscp/ocscp-nrfproxy-oauth                     25.2.201
   0d92bfbf7c14        2 hours ago         720MB
   docker.io/ocscp/ocscp-configuration                      25.2.201
   f23cddb3ec83        2 hours ago         725MB
   docker.io/ocscp/ocscp-worker                             25.2.201
   16c8f423c3b9        2 hours ago         877MB
   docker.io/ocscp/ocscp-load-manager                       25.2.201
   dab875c4179a        2 hours ago         724MB
   docker.io/ocscp/ocscp-nrfproxy                           25.2.201
   85029929a670        2 hours ago         690MB
   docker.io/ocscp/ocscp-alternate-resolution               25.2.201
   2c38646f8bd7        2 hours ago         695MB
   docker.io/ocscp/ocscp-audit                              25.2.201
   039e25297115        2 hours ago         694MB
   docker.io/ocscp/ocscp-notification                       25.2.201
   a21e6bed6177        2 hours ago         710MB
   docker.io/ocscp/ocmed-nfmediation                        25.2.201
   772e01a41584        2 hours ago         710MB
   ```

5. Verify the list of images shown in the output with the list of images shown in Table 2-14. 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:

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

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

   Where,

   - `<image-name>` is the image name.
   - `<image-tag>` is the image release number.
   - `<docker-repo>` is the docker registry address with Port Number if registry has port attached. This is a repository to store the images.
   - `<podman-repo>` is the Podman registry address with Port Number if registry has port attached. This is a repository to store the images.

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

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

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

> **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 SCP Images to OCI Docker Registry

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

SCP Images

The following table lists the Docker images of SCP:

Table 2-15 Images for SCP

Microservices	Image	Tag
<helm-release-name>-SCP-Worker	ocscp-worker	25.2.201
<helm-release-name>-SCPC-Configuration	ocscp-configuration	25.2.201
<helm-release-name>-SCPC-Notification	ocscp-notification	25.2.201
<helm-release-name>-SCPC-Subscription	ocscp-subscription	25.2.201
<helm-release-name>-SCPC-Audit	ocscp-audit	25.2.201
<helm-release-name>-SCPC-Alternate-Resolution	ocscp-alternate-resolution	25.2.201
<helm-release-name>-SCP-Cache	ocscp-cache	25.2.201
<helm-release-name>-SCP-nrfproxy	ocscp-nrfproxy	25.2.201
<helm-release-name>-SCP-nrfProxy-oauth	ocscp-nrfproxy-oauth	25.2.201
<helm-release-name>-SCP-Mediation	ocmed-nfmediation	25.2.201
<helm-release-name>-SCP-loadManager	ocscp-load-manager	25.2.201

> **Note**
>
> <helm-release-name> will be prefixed in each microservice name. For example, if the Helm release name is OCSCP, then the SCPC-Subscription microservice name will be "OCSCP-SCPC-Subscription".

To push the images to the registry:

1. Navigate to the location where you want to install SCP, and then unzip the SCP release package (`<p********>_<release_number>_Tekelec.zip`) to retrieve the following CSAR package.
   The SCP 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, `ocscp_csar_25_2_2_0_1_0.zip`.
2. Untar the SCP package to retrieve the OCSCP image tar file: `unzip <ReleaseName>_csar_<Releasenumber>.zip`.
   For example, `unzip ocscp_csar_25_2_2_0_1_0.zip`

   The zip file consists of the following:

```
|—— Definitions
|    ├—— ocscp_cne_compatibility.yaml
|    └—— ocscp.yaml
├—— Files
|    ├—— ChangeLog.txt
|    ├—— Helm
|    |    ├—— ocscp-25.2.201.tgz
|    |    └—— ocscp-network-policy-25.2.201.tgz
|    ├—— Licenses
|    ├—— nf-test-25.2.201.tar
|    ├—— ocdebug-tools-25.2.201.tar
|    ├—— ocmed-nfmediation-25.2.201.tar
|    ├—— ocscp-alternate-resolution-25.2.201.tar
|    ├—— ocscp-audit-25.2.201.tar
|    ├—— ocscp-cache-25.2.201.tar
|    ├—— ocscp-configuration-25.2.201.tar
|    ├—— ocscp-load-manager-25.2.201.tar
|    ├—— ocscp-notification-25.2.201.tar
|    ├—— ocscp-nrfproxy-25.2.201.tar
|    ├—— ocscp-subscription-25.2.201.tar
|    ├—— ocscp-nrfProxy-oauth-25.2.201.tar
|    ├—— ocscp-worker-25.2.201.tar
|    ├—— Oracle.cert
|    └—— Tests
├—— ocscp.mf
├—— Scripts
|    ├—— ocscp_alerting_rules_promha.yaml
|    ├—— ocscp_alertrules.yaml
|    ├—— ocscp_configuration_openapi_25.2.201.json
|    ├—— ocscp_custom_values_25.2.201.yaml
|    ├—— ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml
|    ├—— ocscp_metric_dashboard_25.2.201.json
|    ├—— ocscp_metric_dashboard_promha_25.2.201.json
|    ├—— ocscp_mib_25.2.201.mib
|    ├—— ocscp_mib_tc_25.2.201.mib
|    ├—— ocscp_network_policies_values_25.2.201.yaml
|    ├—— ocscp_servicemesh_config_values_25.2.201.yaml
|    └—— toplevel.mib
├—— Scripts
```

```
│     ├──── oci
│     │       └──── ocscp_oci_alertrules_25.2.201.zip
│     │       └──── ocscp_oci_metric_dashboard_25.2.201.zip
└──── TOSCA-Metadata
    └──── TOSCA.meta
```

3. Open the `Files` folder and run one of the following commands to load `ocscp-images-25.2.201.tar`:

   ```
   podman load --input /IMAGE_PATH/ocscp-images-<release_number>.tar
   ```

   ```
   docker load --input /IMAGE_PATH/ocscp-images-<release_number>.tar
   ```

   Example:

   ```
   docker load --input /IMAGE_PATH/ocscp-images-25.2.201.tar
   ```

4. Run one of the following commands to verify that the images are loaded:

   ```
   podman images
   ```

   ```
   docker images
   ```

   Sample Output:

   ```
   docker.io/ocscp/ocscp-cache                              25.2.201
   98fc90defb56        2 hours ago         725MB
   docker.io/ocscp/ocscp-nrfproxy-oauth                     25.2.201
   0d92bfbf7c14        2 hours ago         720MB
   docker.io/ocscp/ocscp-configuration                      25.2.201
   f23cddb3ec83        2 hours ago         725MB
   docker.io/ocscp/ocscp-worker                             25.2.201
   16c8f423c3b9        2 hours ago         877MB
   docker.io/ocscp/ocscp-load-manager                       25.2.201
   dab875c4179a        2 hours ago         724MB
   docker.io/ocscp/ocscp-nrfproxy                           25.2.201
   85029929a670        2 hours ago         690MB
   docker.io/ocscp/ocscp-alternate-resolution               25.2.201
   2c38646f8bd7        2 hours ago         695MB
   docker.io/ocscp/ocscp-audit                              25.2.201
   039e25297115        2 hours ago         694MB
   docker.io/ocscp/ocscp-notification                       25.2.201
   a21e6bed6177        2 hours ago         710MB
   docker.io/ocscp/ocmed-nfmediation                        25.2.201
   772e01a41584        2 hours ago         710MB
   ```

5. Verify the list of images shown in the output with the list of images shown in Table 2-14. If the list does not match, reload the image tar file.

6. Run the following commands to log in to the OCI 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 *Oracle Communications Cloud Native Core, OCI Deployment Guide*.
   - `<Object Storage Namespace>` can be obtained from the OCI Console by navigating to **Governance & Administration** > **Account Management** > **Tenancy Details** > **Object Storage Namespace**.
   - `<Identity Domain>` is the domain of the user.
   - In OCI, each region is associated with a key. For more information, see Regions and Availability Domains.

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

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

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

   Where,

   - `<image-name>` is the image name.
   - `<image-tag>` is the image release number.
   - `<docker-repo>` is the docker registry address with Port Number if registry has port attached. This is a repository to store the images.
   - `<podman-repo>` is the Podman registry address with Port Number if registry has port attached. This is a repository to store the images.

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

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

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

   Where, `<oci-repo>` is the OCI registry path.

9. Make all the image repositories public by performing the following steps:

   > **Note**
   >
   > All the image repositories must be public.

a. Log in to the OCI Console using your login credentials.
b. From the left navigation pane, click **Developer Services**.
c. On the preview pane, click **Container Registry**.
d. From the **Compartment** drop-down list, select **networkfunctions5G (root)**.
e. From the **Repositories and images** drop-down list, select the required image and click **Change to Public**.
   The images details are displayed under the Repository information tab and the image changes to public. For example, the `25.2.201db/occne/cndbtier-mysqlndb-client (Private)` changes to `25.2.201db/occne/cndbtier-mysqlndb-client (Public)`.
f. Repeat substep 9e to make all image repositories public.

2.2.1.4 Verifying and Creating Namespace

To verify and create a namespace:

> **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.

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

   ```
   kubectl get namespaces
   ```

   In the output of the above command, if the namespace exists, continue with Manually Creating Service Account, Role, and Rolebinding.
2. If the required namespace is unavailable, create the namespace by running the following command:

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

   Where, `<required namespace>` is the name of the namespace.

   For example, the following command creates the namespace, `ocscp`:

   ```
   kubectl create namespace ocscp
   ```
3. Update the namespace for the required deployment Helm parameters as described in Configuration Parameters.

   Naming Convention for Namespaces

   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.

2.2.1.5 Manually Creating Service Account, Role, and Rolebinding

This section is optional and it describes how to manually create a service account, role, and rolebinding. It is required only when customer needs to create a role, rolebinding, and service account manually before installing SCP.

> **Note**
>
> The secrets should exist in the same namespace where SCP is getting deployed. This helps to bind the Kubernetes role with the given service account.

1. Run the following command to create an SCP resource file:

   ```
   vi <ocscp-resource-file>
   ```

   Example:

   ```
   vi ocscp-resource-template.yaml
   ```

2. Update the `ocscp-resource-template.yaml` file with release specific information:
   A sample template to update the `ocscp-resource-template.yaml` file is as follows:

   ```
   rules:
   - apiGroups: [""]
     resources: #resources under api group to be tested. Added for helm test.
   Helm test dependency are services,configmaps,pods,pvc,serviceaccounts
     - services
     - configmaps
     - pods
     - secrets
     - endpoints
     - persistentvolumeclaims
     - serviceaccounts

     verbs: ["get", "list", "watch", "delete"] # permissions of resources
   under api group, delete added to perform rolling restart of cache pods.
   - apiGroups:
     - "" # "" indicates the core API group
     resources: # Added for helm test. Helm test dependency
     - services
     - configmaps
     - pods
     - secrets
     - endpoints
     - persistentvolumeclaims
     - serviceaccounts

     verbs: ["get", "list", "watch", "delete"] # permissions of resources
   ```

```
under api group, delete added to perform rolling restart of cache pods.
#APIGroups that are added due to helm test dependency are apps,
autoscaling, rbac.authorization and monitoring.coreos
- apiGroups:
  - apps
  resources:
  - deployments
  verbs: # permissions so that resources under api group has
  - get
  - watch
  - list
- apiGroups:
  - autoscaling
  resources: # Added for helm test. Helm test dependency
  - horizontalpodautoscalers
  verbs: # permissions so that resources under api group has
  - get
  - watch
  - list

- apiGroups:
  - rbac.authorization.k8s.io
  resources: # Added for helm test. Helm test dependency
  - roles
  - rolebindings
  verbs:
  - get
  - watch
  - list
- apiGroups:
  - monitoring.coreos.com
  resources: # Added for helm test. Helm test dependency
  - prometheusrules
  verbs:
  - get
  - watch
  - list
```

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

   ```
   kubectl -n <ocscp-namespace> create -f ocscp-resource-template.yaml
   ```

   Example:

   ```
   kubectl -n ocscp create -f ocscp-resource-template.yaml
   ```

4. Update the `scpServiceAccountName` parameter in the ocscp_values_25.2.201.yaml file with the value updated in the name field under `kind: ServiceAccount`.
   Sample configuration:

   ```
   global:
   #Keyname to give custom service account name
   scpServiceAccountName: &scpServiceAccountName
   "<custom_service_account_name>"
   #Flag for auto-creation of resource, disabled by default
   autoCreateResources:
   ```

```
enabled: true
serviceAccounts:
create: false #internal flag to decide if the following resources should
be automated
accounts:
- scpServiceAccountName: *scpServiceAccountName
type: SCP
```

5. Set `autoCreateResources.enabled` to true and `serviceAccounts.create` to false so that no service account is created by SCP, and SCP uses the service account created by the user.
   For more information about the `scpServiceAccountName`, `autoCreateResources.enabled`, and `serviceAccounts.create` parameters, see Global Parameters.

2.2.1.6 Automatically Creating Service Account, Role, and Rolebinding

This section describes how to automatically create service account, role, and role binding by enabling the following Helm parameters:

- Global parameter (`autoCreateResources.enabled`): Controls the overall automation of resource creation. This parameter is disabled by default and must be set to true to enable automation.
- Resource-specific Parameter (`serviceAccounts.create`): Controls service account creation at the resource level. This parameter is enabled by default. Ensure that it is set to true alongside the global parameter to enable ServiceAccount automation. This parameter is conditional on the global parameter and will only take effect if the global parameter is set to true. If this parameter is disabled, you must create the service accounts manually. The role and role binding resources are created along with the service account as part of this automation.

The service account automation is disabled by default in the `custom-values.yaml` file. Perform the following procedure to enable the service account automation:

> **Note**
>
> You must perform the following procedure during the upgrade.

1. Provide the `scpServiceAccountName` parameter in the `custom-values.yaml` file to create the service account.
2. Enable `autoCreateResources.enabled` and `serviceAccounts.create` parameters in the global section of the `custom-values.yaml` file.
3. Perform Helm installation.
   The service account is created with the name provided in the `custom-values.yaml` file.

The existing `scpServiceAccountName` parameter in the `custom-values.yaml` file is used for service account automation to minimize the changes in the `custom-values.yaml` file.

```
global:

  #Keyname to give custom service account name
  scpServiceAccountName: &scpServiceAccountName ""

  #Flag for auto-creation of resource, disabled by default
```

```
  autoCreateResources:
    enabled: false

    serviceAccounts:
      create: true #internal flag to decide if the following resources should
be automated
      accounts:
        - scpServiceAccountName: *scpServiceAccountName
          type: SCP
```

For more information about the `scpServiceAccountName`, `autoCreateResources.enabled`, and `serviceAccounts.create` parameters, see Global Parameters.

The following table describes service account creation using different combinations of Helm parameters:

Table 2-16 Service Account Creation using Different Combinations

Parameter	scpServiceAccountName	Result
`autoCreateResources.enabled`: true `serviceAccounts.create`: true	Provided	Service account is created or updated with the provided `scpServiceAccountName`.
`autoCreateResources.enabled`: true `serviceAccounts.create`: true	Not provided	Service account is created or updated with `.Release.name.`
`autoCreateResources.enabled`: true `serviceAccounts.create`: false	Provided	The service account is not created. It must be created manually.
`autoCreateResources.enabled`: true `serviceAccounts.create`: false	Not provided	The deployment fails. The `scpServiceAccountName` is mandatory.
`autoCreateResources.enabled`: false `serviceAccounts.create`: true or false	Provided	The service account is not created. It must be created manually.
`autoCreateResources.enabled`: false `serviceAccounts.create`: true or false	Not Provided	Service account is created or updated with `.Release.name`.

> **Note**
>
> - If the `scpServiceAccountName` is set during the installation but omitted during the upgrade, a new service account is created using `.Release.name`. If `scpServiceAccountName` was missing during the installation but provided during the upgrade, a new service account is created with the specified name. The original service account will not be present in the current release. However, it will be restored if the release is rolled back to its previous version.
> - When upgrading from a version that supports automated service account creation without Helm automation to a version with Helm automation, you must retain the same service names in the `custom-values.yaml` file.
> - If you are upgrading from an existing version that uses manually created single or multiple service accounts to a version that supports automated service account creation, where one or more service accounts are automatically generated per component, you must specify the new service account names in the `custom-values.yaml` file to switch to these automated service accounts. This task triggers the creation of the new service accounts, roles, and role bindings through the Helm charts. The old service accounts should be retained for rollback scenarios and should only be removed when SCP is uninstalled as part of the cleanup process.

Sample configuration of service account created with `.Release.name`:

```
global:
#Keyname to give custom service account name
scpServiceAccountName: &scpServiceAccountName ""
#Flag for auto-creation of resource, disabled by default
autoCreateResources:
enabled: true
serviceAccounts:
create: true #internal flag to decide if the following resources should
be automated
accounts:
- scpServiceAccountName: *scpServiceAccountName
type: SCP
```

Sample configuration of service account created with `<custom_name>`:

> **Note**
>
> Ensure that any service account with `<custom_name>` does not exist.

```
global:
#Keyname to give custom service account name
scpServiceAccountName: &scpServiceAccountName "<custom_name>"
#Flag for auto-creation of resource, disabled by default
autoCreateResources:
enabled: true
serviceAccounts:
create: true #internal flag to decide if the following resources should
```

```
be automated
accounts:
- scpServiceAccountName: *scpServiceAccountName
type: SCP
```

Role and RoleBinding Name

When both `autoCreateResource.enabled` and `serviceAccounts.create` are enabled, and `scpserviceAccountName` is provided or left blank, the Role and RoleBinding names are created as `<serviceAccountName>-role`, `<serviceAccountName>-rolebinding`.

Hook Lifecycle

With service account automation enabled, hook-related service accounts are created separately for each hook phase (Preupgrade and Prerollback). These service accounts are managed by Helm and are automatically removed when the corresponding hook or job is complete. This is achieved by applying the required Helm hook annotations to the service accounts. To avoid conflicts, hook service accounts use a -hook suffix and must not have the same name as the primary pod service account.

2.2.1.7 Configuring Database for SCP

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

> **Note**
>
> While performing a fresh installation, if SCP is already deployed, purge the deployment and remove the database and users that were used for the previous deployment. For uninstallation procedure, see Uninstalling SCP.

1. Log in to the MySQL server and ensure that there is a privileged user (<privileged user>) with the privileges similar to a root user.
2. On each SQL node, run the following command to verify that the privileged user has the required permissions to allow connections from remote hosts:

   ```
   mysql>select host from mysql.user where User='<privileged username>';
   +------+
   | host |
   +------+
   | % |
   +------+
   1 rowinset(0.00 sec)
   ```

3. If you do not see '%' in the output of the above mentioned query, then run the following command to modify this field to allow connections to remote host:

   ```
   mysql>update mysql.user set host='%' where User='<privileged username>';
   Query OK, 0rowsaffected (0.00 sec)
   Rowsmatched: 1 Changed: 0 Warnings: 0
   mysql> flush privileges;
   Query OK, 0rowsaffected (0.06 sec)
   ```

> **Note**
>
> Perform this step on each SQL node.

4. To automatically create an application user, backup database, and application database, ensure that the `createUser` parameter in the `ocscp_values.yaml` file is set to `true`. To manually create an application user, application database, and backup database, set the `createUser` parameter to `false` in the `ocscp_values.yaml` file.

   By default, the `createUser` parameter value is set to `true`. For more information about this parameter, see Table 3-1.

5. Run the following commands to create an application and backup database:

   - For application database:

     ```
     CREATE DATABASE <scp_dbname>;
     ```

     Example:

     ```
     CREATE DATABASE ocscpdb;
     ```

   - For backup database:

     ```
     CREATE DATABASE <scp_backupdbname>;
     ```

     Example:

     ```
     CREATE DATABASE ocscpbackupdb;
     ```

6. Run the following command to create an application user and assign privileges:

   ```
   CREATE USER '<username>'@'%' IDENTIFIED BY '<password>';
   GRANT SELECT, INSERT, DELETE, UPDATE ON <scp_dbname>.* TO <username>@'%';
   ```

   Where,

   - `<scp_dbname>` is the database name.
   - `<username>` is the database username.

   Example:

   ```
   CREATE USER 'scpApplicationUsr'@'%' IDENTIFIED BY 'scpApplicationPasswd';
   GRANT SELECT, INSERT, DELETE, UPDATE ON ocscpdb.* TO scpApplicationUsr@'%';
   ```

7. Run the following command to grant NDB_STORED_USER permission to the application user:

   ```
   GRANT NDB_STORED_USER ON *.* TO '<username>'@'%' WITH GRANT OPTION ;
   ```

   Example:

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

> **Note**
>
> During a fresh SCP installation, the application database and backup database must be removed manually by running the following command:
>
> ```
> drop database <dbname>;
> ```

2.2.1.8 Configuring Kubernetes Secret for Accessing Database

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

> **Note**
>
> Do not use the same credentials in different Kubernetes secrets, and the passwords stored in the secrets must follow the password policy requirements as recommended in "Changing cnDBTier Passwords" in *Oracle Communications Cloud Native Core Security Guide*.

2.2.1.8.1 Creating and Updating Secret for Privileged Database User

This section explains how to create and update Kubernetes secret for privileged user to access the database.

1. Run the following command to create Kubernetes secret:

   ```
   kubectl create secret generic <secret name> --from-
   literal=DB_USERNAME=<privileged user> --from-
   literal=DB_PASSWORD=<privileged user password> --from-literal=DB_NAME=<scp
   application db> --from-literal=RELEASE_DB_NAME=<scp backup db> -n <scp
   namespace>
   ```

   Where,

   - `<secret name>` is the secret name of the Privileged User.
   - `<privileged user>` is the username of the Privileged User.
   - `<privileged user password>` is the password of the Privileged User.
   - `<scp backup db>` is the backup database name.
   - `<scp namespace>` is the namespace of SCP deployment.

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

   Example:

   ```
   kubectl create secret generic privilegeduser-secret --from-
   literal=DB_USERNAME=scpPrivilegedUsr --from-
   ```

```
literal=DB_PASSWORD=scpPrivilegedPasswd --from-literal=DB_NAME=ocscpdb --from-
literal=RELEASE_DB_NAME=ocscpbackupdb -n scpsvc
```

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

   ```
   kubectl describe secret <secret name> -n <scp namespace>
   ```

   Where,

   - `<secret name>` is the secret name of the Privileged User.
   - `<scp namespace>` is the namespace of SCP deployment.

   Example:

   ```
   kubectl describe secret privilegeduser-secret -n ocscp
   ```

   Sample output:

   ```
   Name:         privilegeduser-secret
   Namespace:    ocscp
   Labels:       <none>
   Annotations:  <none>

   Type:  Opaque

   Data
   ====
   mysql-password:  10 bytes
   mysql-username:  17 bytes
   ```

2.2.1.8.2 Creating and Updating Secret for Application Database User

This section explains how to create and update Kubernetes secret for application user to access the database.

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

   ```
   kubectl create secret generic <secret name> --from-
   literal=DB_USERNAME=<application user> --from-
   literal=DB_PASSWORD=<application user password> --from-
   literal=DB_NAME=<scp application db> -n <scp namespace>
   ```

   Where,

   - `<secret name>` is the secret name of the Privileged User.
   - `<application user>` is the username of the Application User.
   - `<application user password>` is the password of the Application User.
   - `<scp application db>` is the application database name.
   - `<scp namespace>` is the namespace of SCP deployment.

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

Example:

```
kubectl create secret generic appuser-secret --from-
literal=DB_USERNAME=scpApplicationUsr --from-
literal=DB_PASSWORD=scpApplicationPasswd --from-literal=DB_NAME=ocscpdb -n
scpsvc
```

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

   ```
   kubectl describe secret <application user secret name> -n <namespace>
   ```

   Where,

   - `<application user secret name>` is the secret name of the application user.
   - `<scp namespace>` is the namespace of SCP deployment.

   Example:

   ```
   kubectl describe secret appuser-secret -n ocscp
   ```

   Sample output:

   ```
   Name:         appuser-secret
   Namespace:    ocscp
   Labels:       <none>
   Annotations:  <none>

   Type:  Opaque

   Data
   ====
   mysql-password:  10 bytes
   mysql-username:  7 bytes
   ```

2.2.1.9 Configuring SSL or TLS Certificates to Enable HTTPS

The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) certificates must be configured in SCP to enable Hypertext Transfer Protocol Secure (HTTPS). These certificates must be stored in Kubernetes secret and the secret name must be provided in the `sbiProxySslConfigurations` section of the `custom-values.yaml` file.

Perform the following procedure to configure SSL or TLS certificates for enabling HTTPS in SCP. You must perform this procedure before:

- fresh installation of SCP.
- performing an SCP upgrade.

You must have the following files to create Kubernetes secret for HTTPS:

- ECDSA private key and CA signed certificate of SCP if initialAlgorithm is ES256
- RSA private key and CA signed certificate of SCP if initialAlgorithm is RS256

- TrustStore password file
- KeyStore password file
- CA Root file

> **Note**
>
> - The process to create the private keys, certificates, and passwords is at the operators' discretion.
> - The passwords for TrustStore and KeyStore must be stored in the respective password files.
> - Perform this procedure before enabling HTTPS in SCP.

You can create Kubernetes secret for enabling HTTPS in SCP using one of the following methods:

- Managing Kubernetes secret manually
- Managing Kubernetes secret through OCCM

Managing Kubernetes Secret Manually

1. To create Kubernetes secret manually, run the following command:

   ```
   kubectl create secret generic <ocscp-secret-name> --from-file=<rsa private
   key file name> --from-file=<ssl truststore file name> --from-file=<ssl
   keystore file name> --from-file=<CA root bundle> --from-file=<ssl rsa
   certificate file name> -n <Namespace of OCSCP deployment>
   ```

   > **Note**
   >
   > - Note down the command used during the creation of Kubernetes secret. This command is used for the subsequent updates.
   > - The secrets should exist in the same namespace where SCP is getting deployed.

   Example:

   ```
   kubectl create secret generic server-primary-ocscp-secret --from-
   file=server_rsa_private_key_pkcs1.pem --from-file=server_ocscp.cer --from-
   file=server_caroot.cer --from-file=trust.txt --from-file=key.txt -
   n $NAMESPACE
   kubectl create secret generic default-primary-ocscp-secret --from-
   file=client_rsa_private_key_pkcs1.pem --from-file=client_ocscp.cer --from-
   file=caroot.cer --from-file=trust.txt --from-file=key.txt -n $NAMESPACE
   ```

> **Note**
>
> It is recommended to use the same Kubernetes secret name for the primary client and the primary server as mentioned in the example. In case you change `<ocscp-secret-name>`, then update the `k8SecretName` parameter under the `sbiProxySslConfigurations` section in the `custom-values.yaml` file. For more information about `sbiProxySslConfigurations` parameters, see Global Parameters.

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

   ```
   kubectl describe secret <ocscp-secret-name> -n <Namespace of OCSCP
   deployment>
   ```

   Example:

   ```
   kubectl describe secret ocscp-secret -n ocscp
   ```

3. Optional: Perform the following tasks to add, remove, or modify TLS or SSL certificates in Kubernetes secret:

   > **Note**
   >
   > You must have the certificates and files that you want to add or update in the Kubernetes secret.

   - To add a certificate, run the following command:

     ```
     TLS_CRT=$(base64 < "<certificate-name>" | tr -d '\n')
     kubectl patch secret <secret-name> -p "{\"data\":{\"<certificate-
     name>\":\"${TLS_CRT}\"}}"
     ```

     Where,

     – `<certificate-name>` is the certificate file name.

     – `<secret-name>` is the name of the Kubernetes secret, for example, ocscp-secret.

     Example:

     If you want to add a Certificate Authority (CA) Root from the `caroot.cer` file to the ocscp-secret, run the following command:

     ```
     TLS_CRT=$(base64 < "caroot.cer" | tr -d '\n')
     kubectl patch secret ocscp-secret  -p "{\"data\":{\"caroot.cer\":\"$
     {TLS_CRT}\"}}" -n scpsvc
     ```

     Similarly, you can also add other certificates and keys to the ocscp-secret.

   - To update an existing certificate, run the following command:

     ```
     TLS_CRT=$(base64 < "<updated-certificate-name>" | tr -d '\n')
     kubectl patch secret <secret-name> -p "{\"data\":{\"<certificate-
     name>\":\"${TLS_CRT}\"}}"
     ```

Where, `<updated-certificate-name>` is the certificate file that contains the updated content.

Example:

If you want to update the privatekey present in the `rsa_private_key_pkcs1.pem` file to the ocscp-secret, run the following command:

```
TLS_CRT=$(base64 < "rsa_private_key_pkcs1.pem" | tr -d '\n')
kubectl patch secret ocscp-secret -p "{\"data\":
{\"rsa_private_key_pkcs1.pem\":\"${TLS_CRT}\"}}" -n scpsvc
```

Similarly, you can also update other certificates and keys to the ocscp-secret.

- To remove an existing certificate, run the following command:

  ```
  kubectl patch secret <secret-name> -p "{\"data\":{\"<certificate-
  name>\":null}}"
  ```

  Where, `<certificate-name>` is the name of the certificate to be removed.

  The certificate must be removed when it expires or needs to be revoked.

  Example:

  To remove the CA Root from the ocscp-secret, run the following command:

  ```
  kubectl patch secret ocscp-secret  -p "{\"data\":
  {\"caroot.cer\":null}}" -n scpsvc
  ```

  Similarly, you can also remove other certificates and keys from the ocscp-secret.

The certificate update and renewal impacts are as follows:

- Updating, adding, or deleting the certificate, terminates all the existing connections gracefully and reestablishes new connections for new requests.
- When the certificates expires, no new connections are established for new requests, however, the existing connections remain active. After the renewal of the certificates as described in Step 3, all the existing connections are gracefully terminated. And, new connections are established with the renewed certificates.

Managing Kubernetes Secret Through OCCM

To create the Kubernetes secret using OCCM, see "Managing Certificates" in *Oracle Communications Cloud Native Core, Certificate Management User Guide*, and then patch the Kubernetes secret created by OCCM to add keyStore password and trustStore password files by running the following commands:

1. To patch the Kubernetes secret created with the keyStore password file:

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

   Where, `key.txt` is the KeyStore password file that contains KeyStore password.

2. To patch the Kubernetes secret created with the trustStore password file:

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

Where, `trust.txt` is the TrustStore password file that contains TrustStore password.

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

2.2.1.10 Configuring SSL or TLS Certificates for OCNADD

Perform the following procedure to ensure successful TLS and SASL handshake with Oracle Communications Network Analytics Data Director (OCNADD) or Kafka:

1. To create Kubernetes secret for the OCNADD TLS certificate, run the following command:

```
kubectl create secret generic primary-ocscpdd-secret --from-file=<CA root
bundle> --from-file=<ssl truststore file name> --from-file=<rsa private
key file name> --from-file=<ssl rsa certificate file name> --from-
file=<ssl keystore file name> -n <Namespace of SCP deployment>
```

Example:

```
kubectl create secret generic primary-ocscpdd-secret --from-
file=cacert.pem --from-file=ddtrust.txt --from-
file=dd_rsa_private_key_pkcs1.pem --from-file=dd_certificate.cer --from-
file=ddkey.txt -n scpsvc
```

2. To create the secret for OCNADD SASL credentials, run the following command:

```
kubectl create secret generic ocscpddsasl-secret --from-file=<user name
file> --from-file=<password file> -n <Namespace of SCP deployment>
```

Example:

```
kubectl create secret generic ocscpddsasl-secret --from-file=userName.txt
--from-file=password.txt -n scpsvc
```

3. Run the following command to verify the OCNADD secret created:

```
kubectl describe secret ocscpddsasl-secret -n <Namespace of OCSCP
deployment>
```

Example:

```
kubectl describe secret ocscpddsasl-secret -n scpsvc
```

2.2.1.11 Configuring SCP to Support Aspen Service Mesh

SCP leverages the Platform Service Mesh (for example, Aspen Service Mesh (ASM)) for all internal and external TLS communication by deploying a special sidecar proxy in each pod to intercept all the network communications. The service mesh integration provides inter-NF communication and allows API gateway to co-work with service mesh. The service mesh integration supports the services by deploying a special sidecar proxy in each pods to intercept all the network communications between microservices.

Supported ASM version: 1.14.6, 1.11.8, and 1.21.6.

For ASM installation and configuration, see 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.

Data Plane Configuration

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

- Service Entry (SE)
- Destination Rule (DR)
- Envoy Filter (EF)

> **Note**
>
> Use 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:

- **NF to NF Communication**: During NF to NF communication, where sidecar is injected to both the NFs, SE and DR must communicate with the corresponding SE and DR of the other NF. Otherwise, the sidecar rejects the communication. All egress communications of NFs must have a configured entry for SE and DR.

  > **Note**
  >
  > Configure the core DNS with the producer NF endpoint to enable the sidecar access for establishing communication between cluster.

- **Kube-api-server**: For Kube-api-server, there are a few NFs that require access to the Kubernetes API server. The ASM proxy (mTLS enabled) may block this. As per F5 recommendation, the NF must add SE for the Kubernetes API server for its own namespace.

- **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.

ASM Configuration File

A sample `ocscp_servicemesh_config_values_25.2.201.yaml` is available in the `Scripts` folder of `ocscp_csar_25_2_2_0_1_0.zip`. For downloading the file, see Customizing SCP. To view ASM EnvoyFilter configuration enhancements, see ASM Configuration.

> **Note**
>
> To connect to vDBTier, create an SE and 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 SCP with ASM support.

> **Note**
>
> - For information about ASM parameters, see ASM Resource. You can log in to ASM using ASPEN credentials.
> - On the ASM setup, create service entries for respective namespace.

1. Run the following command to create a namespace for SCP deployment if not already created:

   ```
   kubectl create ns <scp-namespace-name>
   ```

2. Run the following command to configure access to Kubernetes API Service and create a service entry in pod networking so that pods can access Kubernetes api-server:

   ```
   kubectl apply -f kube-api-se.yaml
   ```

   Sample `kube-api-se.yaml` file is as follows:

   ```
   # service_entry_kubernetes.yaml
   apiVersion: networking.istio.io/v1alpha3
   kind: ServiceEntry
   metadata:
     name: kube-api-server
     namespace: <scp-namespace>
   spec:
     hosts:
     - kubernetes.default.svc.<domain>
     exportTo:
     - "."
     addresses:
   ```

```
  - <10.96.0.1> # cluster IP of kubernetes api server
  location: MESH_INTERNAL
  ports:
  - number: 443
    name: https
    protocol: HTTPS
  resolution: NONE
```

3. Run the following command to set Network Repository Function (NRF) connectivity by creating **ServiceEntry** and **DestinationRule** and access external or public NRF service that is not part of Service Mesh Registry:

   ```
   kubectl apply -f nrf-se-dr.yaml
   ```

   Sample `nrf-se-dr.yaml` file is as follows:

   ```
   apiVersion: networking.istio.io/v1alpha3
   kind: DestinationRule
   metadata:
     name: nrf-dr
     namespace: <scp-namespace>
   spec:
     exportTo:
     - .
     host: ocnrf.3gpp.oracle.com
     trafficPolicy:
       tls:
         mode: MUTUAL
         clientCertificate: /etc/certs/cert-chain.pem
         privateKey: /etc/certs/key.pem
         caCertificates: /etc/certs/root-cert.pem
   ---
   apiVersion: networking.istio.io/v1alpha3
   kind: ServiceEntry
   metadata:
     name: nrf-se
     namespace: <scp-namespace>
   spec:
     exportTo:
     - .
     hosts:
     - "ocnrf.3gpp.oracle.com"
     ports:
     - number: <port number of host in hosts section>
       name: http2
       protocol: HTTP2
     location: MESH_EXTERNAL
     resolution: NONE
   ```

4. Run the following command to enable communication between internal Network Functions (NFs):

> **Note**
>
> If Consumer and Producer NFs are not part of Service Mesh Registry, create **Destination Rules** and **Service Entries** in SCP namespace for all known call flows to enable inter NF communication.

```
kubectl apply -f known-nf-se-dr.yaml
```

Sample `known-nf-se-dr.yaml` file is as follows:

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: udm1-dr
  namespace: <scp-namespace>
spec:
  exportTo:
  - .
  host: s24e65f98-bay190-rack38-udm-11.oracle-ocudm.cnc.us-east.oracle.com
  trafficPolicy:
    tls:
      mode: MUTUAL
      clientCertificate: /etc/certs/cert-chain.pem
      privateKey: /etc/certs/key.pem
      caCertificates: /etc/certs/root-cert.pem
---
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: udm1-se
  namespace: <scp-namespace>
spec:
  exportTo:
  - .
  hosts:
  - "s24e65f98-bay190-rack38-udm-11.oracle-ocudm.cnc.us-east.oracle.com"
  ports:
  - number: 16016
    name: http2
    protocol: HTTP2
  location: MESH_EXTERNAL
  resolution: NONE
```

> **Note**
>
> Create DestinationRule and ServiceEntry ASM resources for the following scenarios:
>
> - When an NF is registered with callback URIs or notification URIs which is not part of Service Mesh Registry
> - When a callbackReference is used in a known call flow and contains URI which is not part of Service Mesh Registry
>
> Run the following command:
>
> ```
> kubectl apply -f callback-uri-se-dr.yaml
> ```

Sample `callback-uri-se-dr.yaml` file is as follows:

```
apiVersion: networking.istio.io/v1alpha3
 kind: DestinationRule
 metadata:
 name: udm-callback-dr namespace: <scp-namespace>
 spec:
  exportTo: - .
  host: udm-notifications-processor-03.oracle-ocudm.cnc.us-east.oracle.com
  trafficPolicy:
   tls:
    mode: MUTUAL
    clientCertificate: /etc/certs/cert-chain.pem
    privateKey: /etc/certs/key.pem
    caCertificates: /etc/certs/root-cert.pem
 ---
 apiVersion: networking.istio.io/v1alpha3
 kind: ServiceEntry
 metadata:
 name: udm-callback-se
 namespace: <scp-namespace>
 spec:
  exportTo: - .
  hosts: - "udm-notifications-processor-03.oracle-ocudm.cnc.us-
east.oracle.com"
  ports:
  - number: 16016
    name: http2
    protocol: HTTP2
    location: MESH_EXTERNAL
    resolution: NONE
```

5. To equally distribute ingress connections among the SCP worker threads, run the following command to create a new YAML file with EnvoyFilter on ASM sidecar:
   You must apply EnvoyFilter to process inbound connections on ASM sidecar when SCP is deployed with ASM.

   ```
   kubectl apply -f envoy_inbound.yaml
   ```

Sample `envoy_inbound.yaml` file is as follows:

```
apiVersion: networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: inbound-envoyfilter
  namespace: <scp-namespace>
spec:
  workloadSelector:
    labels:
      app: ocscp-scp-worker
  configPatches:
    - applyTo: LISTENER
      match:
        context: SIDECAR_INBOUND
        listener:
          portNumber: 15090
      patch:
        operation: MERGE
        value:
          connection_balance_config:
            exact_balance: {}
```

Note

- The ASM sidecar `portNumber` can be configured depending on the deployment. For example, `15090`.
- Do not configure any virtual service that applies connection or transaction timeout between various SCP services.

2.2.1.11.2 Enabling Dual Stack Networking for ASM

Perform the following procedure before deploying Aspen Service Mesh (ASM) to enable dual stack networking for ASM. Using the dual stack functionality, SCP with sidecar can use IPv4, IPv6, or both to establish connections with pods and services.

Note

- ASM should be deployed in dual stack mode.
- To enable Dual Stack, perform a fresh installation of SCP. An upgrade from a single stack to a dual stack is not supported.

1. Open the `aspen-mesh-override-values.yaml` file.

   For more information about the `aspen-mesh-override-values.yaml` file and ASM installation, see https://clouddocs.f5.com/products/aspen-service-mesh/1.11/.
2. In the `global` section, do the following:
   a. To enable dual stack functionality in Istio to work in Kubernetes, set the `dualStack` parameter to true.

b. To establish communication between gateway and external sources, set the `ingressGatewayDualStack` parameter to true.

3. Save the `aspen-mesh-override-values.yaml` file.

2.2.1.11.3 Deploying SCP with ASM

Deployment Configuration

You must complete the following deployment configuration before performing the Helm install.

1. Run the following command to create namespace label for auto sidecar injection and to automatically add the sidecars in all pods spawned in SCP namespace:

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

2. Create a Service Account for SCP and a role with **appropriate security policies for sidecar proxies to work** by referring to the `sa-role-rolebinding.yaml` file mentioned in the next step.
3. Map the role and service accounts by creating a role binding as specified in the sample `sa-role-rolebinding.yaml` file:

   ```
   kubectl apply -f sa-role-rolebinding.yaml
   ```

   Sample `sa-role-rolebinding.yaml` file is as follows:

   ```
   apiVersion: rbac.authorization.k8s.io/v1
   kind: Role
   metadata:
     name: {{ template "noncluster.role.name" . }}
     namespace: {{ .Release.Namespace }}
     labels:
       {{- include "labels.allResources" . }}
     annotations:
       {{- include "annotations.allResources" . }}
   rules:
   - apiGroups: [""]
     resources:
     - pods
     - services
     - configmaps
     verbs: ["get", "list", "watch"]
   - apiGroups:
     - "" # "" indicates the core API group
     resources:
     - secrets
     - endpoints
     verbs: ["get", "list", "watch"]
   ---
   apiVersion: rbac.authorization.k8s.io/v1
   kind: RoleBinding
   metadata:
     name: {{ template "noncluster.rolebinding.name" . }}
     namespace: {{ .Release.Namespace }}
     labels:
   ```

```
    {{- include "labels.allResources" . }}
  annotations:
    {{- include "annotations.allResources" . }}
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: {{ template "noncluster.role.name" . }}
subjects:
- kind: ServiceAccount
  name: {{ template "noncluster.serviceaccount.name" . }}
  namespace: {{ .Release.Namespace }}
---
apiVersion: v1
kind: ServiceAccount
{{- if .Values.imagePullSecrets }}
imagePullSecrets:
{{- range .Values.imagePullSecrets }}
  - name: {{ . }}
{{- end }}
{{- end }}
metadata:
  name: {{ template "noncluster.serviceaccount.name" . }}
  namespace: {{ .Release.Namespace }}
  labels:
    {{- include "labels.allResources" . }}
  annotations:
    {{- include "annotations.allResources" . }}
```

4. Update `ocscp_custom_values_25.2.201.yaml` with the following annotations:

> **Note**
>
> Update other values such as DB details and service account as created in the previous steps.

```
global:
  customExtension:
    allResources:
      annotations:
        sidecar.istio.io/inject: "true"
    lbDeployments:
      annotations:
        sidecar.istio.io/inject: "true"
        oracle.com/cnc: "true"
    nonlbDeployments:
      annotations:
        sidecar.istio.io/inject: "true"
        oracle.com/cnc: "true"

  scpServiceAccountName: <"ocscp-release-1-10-2-scp-serviceaccount">
  database:
    dbHost: <"scp-db-connectivity-service"> #DB Service FQDN

scpc-configuration:
```

```
  service:
    type: ClusterIP

scp-worker:
  tracingenable: false
  service:
    type: ClusterIP
```

> **Note**
>
> a. The `Sidecar inject = "false"` annotation on all resources prevents sidecar injection on pods created by Helm jobs or hooks.
>
> b. Deployment overrides re-enable auto sidecar injection on all deployments.
>
> c. SCP-Worker override disables automatic sidecar injection for the SCP-Worker microservice because it is done manually in later stages. This override is only required for ASM release 1.4 or 1.5. If integrating with ASM release 1.6 or later, it must be removed.
>
> d. The `oracle.com/cnc` annotation is required for integration with OSO services.
>
> e. Jaeger tracing must be disabled because it may interfere with SM end-to-end traces.

5. To set sidecar resources for each microservice in the `ocscp_custom_values_25.2.201.yaml` file under `deployment.customExtension.annotations`, configure the following ASM annotations with the resource values for the services:
   SCP uses these annotations to assign the resources of the sidecar containers.
   - `sidecar.istio.io/proxyMemory`: Indicates the memory requested for the sidecar.
   - `sidecar.istio.io/proxyMemoryLimit`: Indicates the maximum memory limit for the sidecar.
   - `sidecar.istio.io/proxyCPU`: Indicates the CPU requested for the sidecar.
   - `sidecar.istio.io/proxyCPULimit`: Indicates the CPU limit for the sidecar.
6. Define the concurrency setting for the sidecar container. A sidecar container concurrency value must be at least equal to or a multiple of the number of maximum vCPUs allocated to the sidecar:

   ```
   proxy.istio.io/config: |-
            concurrency: 4
   ```

   a. Set the concurrency of SCPC-Notification pods to 18.
   b. Set the concurrency of SCP-Worker pods as follows:
      - Concurrency value of 4 for a 4vCPU SCP-Worker profile and the sidecar maximum vCPU of 4.
      - Concurrency value of 8 for a 8vCPU SCP-Worker profile and the sidecar maximum vCPU of 8.
      - Concurrency value of 20 for a 12vCPU SCP-Worker profile and the sidecar maximum vCPU of 10

2.2.1.11.4 Deployment Configurations

ASM Configuration to Allow XFCC Header

Envoy Filter should be added to allow the XFCC header on ASM sidecar.

Sample file:

```
apiVersion: networking.istio.io/v1alpha3
kind: EnvoyFilter
metadata:
  name: <name>
  namespace: <namespace>
spec:
  workloadSelector:
    labels:
      app.kubernetes.io/instance: <SCP Deployment name>
  configPatches:
  - applyTo: NETWORK_FILTER
    match:
      listener:
        filterChain:
          filter:
            name: "envoy.filters.network.http_connection_manager"
    patch:
      operation: MERGE
      value:
        typed_config:
          '@type': type.googleapis.com/
envoy.config.filter.network.http_connection_manager.v3.HttpConnectionManager
          forward_client_cert_details: ALWAYS_FORWARD_ONLY
          use_remote_address: true
          xff_num_trusted_hops: 1
```

Inter-NF Communication

For every new NF participating in new call flows, DestinationRule and ServiceEntry must be created in SCP namespace to enable communication. This can be done in the same way as done earlier for known call flows.

Run the following command to create DestinationRule and ServiceEntry:

```
kubectl apply -f new-nf-se-dr.yaml
```

Sample *new-nf-se-dr.yaml* file for DestinationRule and ServiceEntry:

```
apiVersion: networking.istio.io/v1alpha3
kind: DestinationRule
metadata:
  name: <unique DR name for NR>
  namespace: <scp-namespace>
spec:
  exportTo:
  - .
  host: <NF-public-FQDN>
```

```
  trafficPolicy:
    tls:
      mode: MUTUAL
      clientCertificate: /etc/certs/cert-chain.pem
      privateKey: /etc/certs/key.pem
      caCertificates: /etc/certs/root-cert.pem
---
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: <unique SE name for NR>
  namespace: <scp-namespace>
spec:
  exportTo:
  - .
  hosts:
  - <NF-public-FQDN>
  ports:
  - number: <NF-public-port>
    name: http2
    protocol: HTTP2
  location: MESH_EXTERNAL
  resolution: NONE
```

Operations Services Overlay Installation

For Operations Services Overlay (OSO) installation instructions, see *Oracle Communications Cloud Native Core, Operations Services Overlay Installation Guide*.

> **Note**
>
> If OSO is deployed in the same namespace as SCP, ensure that all deployments of OSO have the annotation to skip sidecar injection as OSO does not support ASM sidecar proxy.

CNE Common Services for Logging

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

> **Note**
>
> If CNE is deployed in the same namespace as SCP, ensure that all deployments of CNE have the annotation to skip sidecar injection as CNE does not support ASM sidecar proxy.

2.2.1.11.5 Deleting ASM

This section describes the steps to delete ASM.

To delete ASM, 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 the Helm command.

For example:

```
helm delete ocscp-servicemesh-config -n ocscp
```

To disable ASM, run the following command:

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

To verify if ASM is disabled, run the following command:

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

2.2.1.12 Configuring Network Policies for SCP

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 a recommended step. Based on the security requirements, network policies may or may not be configured.

For more information about this functionality, 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 is overridden, update them in the corresponding network policies.

Configuring Network Policies

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 be using a networking solution which supports Network Policy.

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

To install network policy:

1. Open the `ocscp-network-policy-custom-values-25.2.201.yaml` file provided in the release package zip file. For downloading the file, see Downloading the SCP Package and Pushing the Images to Customer Docker Registry.
2. The file is provided with the default network policies. If required, update the `ocscp-network-policy-custom-values-25.2.201.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 `ocscp-network-policy-custom-values-25.2.201.yaml`:
   >
   > - allow-ingress-traffic-to-notification
   > - allow-egress-for-ats
   > - allow-ingress-to-ats

   - To connect with CNC Console, update the below parameter in the allow-ingress-from-console network policy in the `ocscp-network-policy-custom-values-25.2.201.yaml` file:
     - `kubernetes.io/metadata.name`: <namespace in which CNCC is deployed>
   - In allow-ingress-prometheus policy, `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.
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 ocscp-network-policy ocscp-network-policy/ -n scpsvc -f ocscp-
   network-policy-custom-values-25.2.201.yaml
   ```

- `helm-release-name`: ocscp-network-policy Helm release name.
- `custom-value-file`: ocscp-network-policy custom value file.
- `namespace`: SCP 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 <NF acronym> and ATS in the same namespace.

2.2.1.12.2 Upgrading Network Policies

To add, delete, or update network policy:

1. Modify the `ocscp-network-policy-custom-values-25.2.201.yaml` file to update, add, and delete the network policies.
2. Run the following command to upgrade the network policies:

   ```
   helm upgrade <helm-release-name> <network-policy>/ -n <namespace> -f
       <values.yaml>
   ```

   For example:

   ```
   helm upgrade ocscp-network-policy ocscp-network-policy/ -n ocscp -f
    ocscp-network-policy-custom-values-25.2.201.yaml
   ```

   where,

   - `helm-release-name`: ocscp-network-policy Helm release name.
   - `custom-value-file`: ocscp-network-policy custom value file.
   - `namespace`: SCP 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 if the network policies are deployed successfully:

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

For Example:

```
kubectl get ocscp-network-policy -n ocscp
```

where,

- `helm-release-name`: ocscp-network-policy Helm release name.
- `namespace`: SCP namespace.

2.2.1.12.4 Uninstalling Network Policies

Run the following command to uninstall all the network policies:

```
helm uninstall <release_name> --namespace <namespace>
```

For example:

```
helm uninstall occncc-network-policy --scp
    cncc
```

> **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

Table 2-17 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.	Data Type: string Default Value: `networking.k8s.io/v1`
kind	This is a mandatory parameter. Represents the REST resource this object represents. **Note**: This is a read-only parameter.	Data Type: string Default Value: NetworkPolicy

Table 2-18 Configuration Parameters for Network Policy

Parameter	Description	Details
metadata.name	This is a mandatory parameter. Specifies a unique name for the network policy.	`{{ .metadata.name }}`

Table 2-18 (Cont.) Configuration Parameters for Network Policy

Parameter	Description	Details
spec.{}	This is a mandatory parameter. This consists of all the information needed to define a particular network policy in the given namespace. **Note**: SCP supports the spec parameters defined in "Supported Kubernetes Resource for Configuring Network Policies".	Default Value: NA

For more information about this functionality, see "Network Policies" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

2.2.2 Installation Tasks

This section provides installation procedures to install Oracle Communications Cloud Native Core, Service Communication Proxy (SCP).

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

2.2.2.1 Installing SCP Package

To install the SCP package:

> **Note**
>
> For each SCP deployment in the network, use a unique SCP database name during the installation.

1. Run the following command to access the extracted package:

   ```
   cd ocscp-<release_number>
   ```

   Example:

   ```
   cd ocscp-25.2.201
   ```

2. Customize the `ocscp_values_25.2.201.yaml` file with the required deployment parameters. See the Customizing SCP chapter to customize the file. For more information about predeployment parameter configurations, see Preinstallation Tasks.

   > **Note**
   >
   > In case NRF configuration is required, see Configuring Network Repository Function Details.

3. (Optional) If you want to install SCP with Aspen Service Mesh (ASM), perform the predeployment tasks as described in Configuring SCP to Support Aspen Service Mesh.

4. Open the `ocscp_values_25.2.201.yaml` file and enable Release 16 with Model C Indirect 5G SBI Communication support by adding `- rel16` manually under `releaseVersion`, and then uncomment `scpProfileInfo.servingScope` and `scpProfileInfo.nfSetIdList` parameters.

   > **Note**
   >
   > `- rel16` is the default release version. For more information about Release 16, see 3GPP TS 23.501.

   Sample `custom-values.yaml` file output:

```
global:
  domain: svc.cluster.local
  clusterDomain: cluster.local
  # If ingress gateway is available then set ingressGWAvailable flag to
true
  # and provide ingress gateway IP and Port in publicSignalingIP and
publicSignalingPort respectively.
  # If ingressGWAvailable flag is true then service type for scp-worker
will be ClusterIP
  # otherwise it will be LoadBalancer.
  # We can not set ingressGWAvailable flag true and at the same time
publicSignalingIPSpecified flag as false.
  # If you want to assign a load balancer IP,set loadbalanceripenbled flag
to true and
  # provide value for flag loadbalancerip
  # else a random IP will be assigned if loadbalanceripenbled is false
  # and it will not use loadbalancerip flag
  adminport: 8001
  # enable or disable jaeger tracing
  tracingEnable: &scpworkerTracingEnabled false
  enableTraceBody: &scpworkerJaegerBodyEnabled false
  #otelTracingEnabled: &scpworkerOtelTracingEnabled false
  releaseVersion:
  - rel16
```

5. Run the following command to install SCP using charts from the Helm repository:

```
helm install <release name> -f <custom_values.yaml> --namespace
<namespace> <helm-repo>/chart_name --version <helm_version>
```

   a. In case charts are extracted:

```
helm install <release name> -f <custom_values.yaml> --namespace
<namespace> <chartpath>
```

   Example:

```
helm install ocscp-helm-repo/ocscp -f <custom values.yaml> ocscp --namespace
scpsvc --version <helm version>
```

> **⚠ Caution**
>
> Do not exit from the `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 the `helm install` command. It leads to some anomalous behavior.

2.2.3 Postinstallation Tasks

This section explains the postinstallation tasks for SCP.

2.2.3.1 Verifying SCP Installation

To verify the installation:

1. Run the following command to verify the installation status:

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

   Where,

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

   Example:

   ```
   helm status ocscp --namespace ocscp
   ```

   The system displays the status as `deployed` if the deployment is successful.

2. Run the following command to check whether all the services are deployed and active:

   ```
   kubectl -n <namespace_name> get services
   ```

   Example:

   ```
   NAME                                                    TYPE
   CLUSTER-IP      EXTERNAL-IP   PORT(S)
   <helm-release-name>-scp-cache                           LoadBalancer
   10.96.65.127    <pending>     8091:31668/TCP,9000:31087/
   TCP,30001:31028/TCP
   <helm-release-name>-scp-cache-headless                  ClusterIP
   None            <none>
   8010/TCP
   <helm-release-name>-scp-load-manager                    ClusterIP
   10.96.217.195   <none>        8091/TCP,8040/
   TCP,9000/TCP
   <helm-release-name>-scp-mediation                       ClusterIP
   10.96.197.99    <none>        9090/TCP,9091/
   TCP,8091/TCP
   <helm-release-name>-scp-nrfproxy                        ClusterIP
   10.96.139.20    <none>        8091/
   TCP,8086/TCP
   <helm-release-name>-scp-nrfproxy-oauth                  ClusterIP
   10.96.36.166    <none>        8091/TCP,8040/
   ```

```
TCP,9000/TCP
<helm-release-name>-scp-worker                              LoadBalancer
10.96.65.218    <pending>     8091:31259/TCP,8000:31790/TCP,9000:31115/
TCP,9443:30113/TCP
<helm-release-name>-scp-worker-int                          ClusterIP
10.96.64.254    <none>
8092/TCP
<helm-release-name>-scpc-alternate-resolution               ClusterIP
10.96.69.12     <none>        8091/
TCP,8084/TCP
<helm-release-name>-scpc-alternate-resolution-int           ClusterIP
10.96.91.133    <none>
8092/TCP
<helm-release-name>-scpc-audit                              ClusterIP
10.96.178.49    <none>        8091/
TCP,8083/TCP
<helm-release-name>-scpc-audit-int                          ClusterIP
10.96.170.31    <none>
8092/TCP
<helm-release-name>-scpc-configuration                      LoadBalancer
10.96.247.33    <pending>     8091:32070/
TCP,8081:30308/TCP
<helm-release-name>-scpc-configuration-int                  ClusterIP
10.96.230.133   <none>
8092/TCP
<helm-release-name>-scpc-notification                       ClusterIP
10.96.72.44     <none>        8091/TCP,8082/
TCP,9000/TCP
<helm-release-name>-scpc-notification-int                   ClusterIP
10.96.139.117   <none>
8092/TCP
<helm-release-name>-scpc-subscription                       ClusterIP
10.96.91.150    <none>        8091/TCP,8080/TCP
```

3. Run the following command to check whether all the pods are up and active:

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

Example:

```
kubectl get pods -n scpsvc
NAME                                        READY   STATUS    RESTARTS   AGE
ocscp-scp-cache-8444cd8f6d-gfsmx              1/1     Running
0             2d23h
ocscp-scp-load-manager-5664c7c8b4-rmrd2       1/1     Running
0             2d23h
ocscp-scp-nrfproxy-5f44ff5f55-84f44           1/1     Running
0             2d23h
ocscp-scp-nrfproxy-oauth-5dbc78689d-mkhnt     1/1     Running
0             3m2s
ocscp-scp-worker-6dc45b7cfc-2tfz5             1/1     Running
0             28h
ocscp-scpc-audit-6ff496fcc9-jkwj5             1/1     Running
0             2d23h
ocscp-scpc-configuration-5d66df6f4-6hdll      1/1     Running
```

```
0             2d23h
ocscp-scpc-notification-7f49b85c99-c4p9v             1/1     Running
0             2d23h
ocscp-scpc-subscription-6b785f77b4-9rtn2             1/1     Running
0             2d23h
```

> **Note**
>
> If the installation is unsuccessful or the STATUS of all the pods is not in the Running state, perform the troubleshooting steps provided in *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.

2.2.3.2 Performing Helm Test

This section describes how to perform sanity check for SCP 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 installation of SCP and determines if the NF is ready to accept 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 `ocscp_custom_values_25.2.201.yaml` file as follows:

```
nfName: ocscp
image:
  name: nf_test
  tag: <string>
  pullPolicy: Always
config:
  logLevel: WARN
  timeout: 180
resources:
    - horizontalpodautoscalers/v1
    - deployments/v1
    - configmaps/v1
    - serviceaccounts/v1
    - roles/v1
    - services/v1
    - rolebindings/v1
```

For more information, see Customizing SCP.

2. Run the following Helm test command:

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

Example:

```
helm test ocscp -n ocscp
```

Sample Output:

```
NAME: ocscp
LAST DEPLOYED: Fri Sep 18 10:08:03 2020
NAMESPACE: ocscp
STATUS: deployed
REVISION: 1
TEST SUITE:     ocscp-test
Last Started:   Fri Sep 18 10:41:25 2020
Last Completed: Fri Sep 18 10:41:34 2020
Phase:          Succeeded
NOTES:
# Copyright 2020 (C), Oracle and/or its affiliates. All rights reserved.
```

Note

- After running the helm test, the pod moves to a completed state. Hence, to remove the pod, run the following command:

  ```
  kubectl delete pod <releaseName>-test -n <namespace>
  ```

- The Helm test only verifies whether all pods running in the namespace are in the Ready state, such as 1/1 or 2/2 states. It does not check the deployment.
- If the Helm test fails, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.

2.2.3.3 Taking Backup of Important Files

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

1. Updated the `ocscp_custom_values_25.2.201.yaml` file.
2. Updated Helm charts.
3. Secrets, certificates, and keys that are used during installation.

2.2.3.4 Alert Configuration

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

2.2.3.4.1 Applying Alerts Rule to CNE without Prometheus Operator

SCP Helm Chart Release Name: _NAME_

Prometheus NameSpace: _Namespace _

Perform the following procedure to configure Service Communication Proxy alerts in Prometheus.

1. Run the following command to check the name of the config map used by Prometheus:

   ```
   $kubectl get configmap -n <_Namespace_>
   ```

   Example:

   ```
   $kubectl get configmap -n prometheus-alert2
   NAME                                  DATA   AGE
   lisa-prometheus-alert2-alertmanager   1      146d
   lisa-prometheus-alert2-server         4      146d
   ```

2. Take a backup of the current config map of Prometheus. This command saves the configmap in the provided file. In the following command, the configmap is stored in the */tmp/tempConfig.yaml* file:

   ```
   $ kubectl get configmaps <_NAME_>-server -o yaml -n <_Namespace_> /tmp/
   tempConfig.yaml
   ```

   Example:

   ```
   $ kubectl get configmaps lisa-prometheus-alert2-server -o yaml -n
   prometheus-alert2 > /tmp/tempConfig.yaml
   ```

3. Check and delete the "alertsscp" rule if it has already configured in the prometheus config map. If configured, this step removes the " alertsscp " rule. This is an optional step if configuring the alerts for the first time.

   ```
   $ sed -i '/etc\/config\/alertsscp/d' /tmp/tempConfig.yaml
   ```

4. Add the "alertsscp" rule in the configmap dump file under the ' rule_files ' tag.

   ```
   $ sed -i '/rule_files:/a\    \- /etc/config/alertsscp'  /tmp/
   tempConfig.yaml
   ```

5. Update the configmap using below command. Ensure to use the same configmap name that was used to take a backup of the prometheus configmap.

   ```
   $ kubectl replace configmap <_NAME_>-server -f /tmp/tempConfig.yaml
   ```

   Example:

   ```
   $ kubectl replace configmap lisa-prometheus-alert2-server -f /tmp/
   tempConfig.yaml
   ```

6. Run the following command to patch the configmap with a new "alertsscp" rule:

> **Note**
>
> The patch file provided is the `ocscp_csar_23_2_0_0_0.zip` folder provided with SCP, that is, `SCPAlertrules.yaml`.

```
$ kubectl patch  configmap _NAME_-server -n _Namespace_ --type merge --
patch "$(cat ~/SCPAlertrules.yaml)"
```

Example:

```
$ kubectl replace configmap lisa-prometheus-alert2-server -f /tmp/
tempConfig.yaml
```

> **Note**
>
> Prometheus takes about 20 seconds to apply the updated Config map.

2.2.3.4.2 Applying Alerts Rule to CNE with Prometheus Operator

Perform the following procedure to apply alerts rule to Cloud Native Environment (CNE) with Prometheus Operator (CNE 1.9.0 and later).

- Run the following command to apply SCP alerts file to create Prometheus rules Custom Resource Definition (CRD):

  ```
  kubectl apply -f <file_name> -n <scp namespace>
  ```

  Where,

  - `<file_name>` is the SCP alerts file.
  - `<scp namespace>` is the SCP namespace.

  Example:

  ```
  kubectl apply -f ocscp_alerting_rules_promha_25.2.201.yaml -n scpsvc
  ```

  Sample file delivered with SCP package:

  ```
  ocscp_alerting_rules_promha_25.2.201.yaml
  ```

2.2.3.4.3 Configuring Service Communication Proxy Alert using the SCPAlertrules.yaml file

> **Note**
>
> Default NameSpace is **scpsvc** for Service Communication Proxy. You can update the NameSpace as per the deployment.

To access the `scpAlertsrules_<scp release number>.yaml` file from the `Scripts` folder of `ocscp_csar_25_1_1_0_0_0.zip`, download the SCP package from My Oracle Support as described in "Downloading the SCP Package " in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

Alerts Details

Description and summary for alerts are added by the Prometheus alert manager.

Alerts are supported for three different resources/routing crosses threshold.

- SCPIngress Traffic Rate Above Threshold
  - Has three threshold level Minor (above 9800 mps to 11200 mps), Major (11200 to 13300 mps), Critical (above 13300 mps). These values are configurable.
  - In the description, information is presented similar to: "Ingress Traffic Rate at Locality: <Locality of scp> is above <threshold level (minor/major/critical> threshold (i.e. <value of threshold>)"
  - In Summary: "Namespace: <Namespace of scp deployment that Locality>, Pod: <SCP-worker Pod name>: Current Ingress Traffic Rate is <Current rate of Ingress traffic > mps which is above 70 Percent of Max MPS(<upper limit of ingress traffic rate per pod>)"

    > **Note**
    >
    > Ingress traffic rate is per scp-worker pod in a namespace at particular SCP-Locality. Currently, 14000mps is the upper limit for per scp-worker pod.

- SCP Routing Failed For Service
  - It alerts for which NF Service Type and NF Type at particular locality, Routing failed
  - Description: "Routing failed for service"
  - Summary: "Routing failed for service: NFService Type = <Message NF Service Type>, NFType = <Message NF Type>, Locality = <SCP Locality where Routing Failed> and value = <Accumulated failure till now, of such message for NFType and NFService Type>"

    > **Note**
    >
    > The value field currently does not provide the number of failures in particular time interval, instead it provides the total number of Routing failures.

- SCP Pod Memory Usage: Type of alert is SCPWorkerPodMemoryUsage.
  - Pod memory usage for SCP Pods (Soothsayer and Worker) deployed at a particular node instance is provided.
  - The Soothsayer pod threshold is 8 GB
  - The Worker pod threshold is 16 Gi
  - Summary: Instance: "<Node Instance name>, NameSpace: <Namespace of SCP deployment>, Pod: <(Soothsayer/Worker) Pod name>: <Soothsayer/Worker> Pod High Memory usage detected"

– Summary: "Instance: "<Node Instance name>, Namespace: <Namespace of SCP deployment>, Pod: <(Soothsayer/Worker) Pod name>: Memory usage is above <threshold value>G (current value is: <current value of memory usage>)"

2.2.3.4.4 Configuring Alert Manager for SNMP Notifier

Grouping of alerts is based on:

- podname
- alertname
- severity
- namespace
- nfServiceType
- nfServiceInstanceId

User needs to add subroutes for SCP alerts in AlertManager config map as below:

1. Take a backup of the current config map of Alertmanager by running the following command:

   ```
   kubectl get configmaps <NAME-alertmanager> -oyaml -n <Namespace> > /tmp/
   bkupAlertManagerConfig.yaml
   ```

   Example:

   ```
   kubectl get configmaps occne-prometheus-alertmanager -oyaml -n occne-infra
   > /tmp/bkupAlertManagerConfig.yaml
   ```

2. Edit Configmap to add subroute for SCP Trap OID:

   ```
   kubectl edit configmaps <NAME-alertmanager> -n <Namespace>
   ```

   Example:

   ```
   kubectl edit configmaps occne-prometheus-alertmanager -n occne-infra
   ```

3. Add the subroute under 'route' in configmap:

   ```
   routes:
         - receiver: default-receiver
           group_interval: 1m
           group_wait: 10s
           repeat_interval: 9y
           group_by: [podname, alertname, severity, namespace, nfservicetype,
   nfserviceinstanceid, servingscope, nftype]
           match_re:
             oid: ^1.3.6.1.4.1.323.5.3.35.(.*)
   ```

MIB Files for SCP

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

- ocscp_mib_tc_25.2.201.mib: This is considered as SCP top level mib file, where the Objects and their data types are defined.
- ocscp_mib_25.2.201.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.

> **Note**
>
> MIB files are packaged with `ocscp_csar_25_2_2_0_1_0.zip`. You can download the file from MOS as described in *Oracle Communications Cloud Native Core, Service Communication Proxy Installation, Upgrade, and Fault Recovery Guide*.

2.2.3.4.5 Configuring SCP Alerts for OCI

To configure SCP alerts for OCI, OCI supports metric expressions written in MQL (Metric Query Language) and therefore requires `ocscp_oci_alertrules_25.2.201.zip` file for configuring alerts in OCI observability platform. For more information, see *Oracle Communications Cloud Native Core, OCI Deployment Guide*.

2.2.3.4.6 OSO Alerts Automation

Alerts are automated by using the Helm upgrade command with the Helm chart provided as part of OSO software package. A new `oso-alr-config` Helm chart is provided as part of OSO software package from 25.1.200 release onwards. For information to download OSO software package, see *Oracle Communications, Cloud Native Core, Operations Services Overlay Installation and Upgrade Guide*.

The alerts automation procedure is as follows:

1. Deployed the `oso-alr-config` Helm chart when OSO is installed.
   This separate Helm chart allows the Helm install command to run with an input alert file.

   ```
   helm install oso-alr-config oso-alr-config/ -f custom-oso-alr-config-values.yaml -f ocscp_alertrules.yaml
   ```

2. When the `oso-alr-config` Helm chart is installed, `oso-alr-config` is ready to use.
3. Run the following Helm upgrade command in the `oso-alr-config` file to apply SCP alert file if you are enabling this feature after SCP deployment is complete:

   ```
   helm upgrade oso-alr-config oso-alr-config/ -f custom-oso-alr-config-values.yaml - f ocscp_alertrules.yaml
   ```

4. When the Helm upgrade is completed, you can view the alerts file that is applied to OSO **Prometheus ConfigMap**. This can be viewed in the Prometheus Graphical User Interface (GUI).
5. You can also update the changes in the same alert file and perform a Helm upgrade. The alert file will be updated with the latest changes.

Cleaning Up the Alerts

Perform the following procedure to clean up the alerts:

1. An empty `ocscp_alertrules_empty.yaml` file is delivered as part of the OSO software package. For information to download OSO software package, see *Oracle Communications, Cloud Native Core, Operations Services Overlay Installation and*

Upgrade Guide. You must provide this `ocscp_alertrules_empty.yaml` file during the Helm upgrade.

2. This `ocscp_alertrules_empty.yaml` file is used to remove all the alerts using the Helm upgrade command by providing `ocscp_alertrules_empty.yaml` file as an input file. This removes the alerts from the OSO **Prometheus ConfigMap** and **Prometheus GUI** and keeps the references under rule_files `"/etc/config/alertsscp"` and the alert rules will be empty `"alertsscp: { }"`.
3. Run the following Helm upgrade command to clean up alert rules:

   ```
   helm upgrade oso-alr-config oso-alr-config/ -f custom-oso-alr-config-
   values.yaml - f ocscp_alertrules_empty.yaml
   ```

Sample empty alert file is as follows:

```
apiVersion: v1
data:
  alerts: |
    {}
```

2.2.4 Configuring Network Repository Function Details

Network Repository Function (NRF) details must be defined during the SCP installation using the `values.yaml` file. You must update the NRF details in the `values.yaml` file.

> **Note**
>
> You can configure a primary NRF and an optional secondary NRF. NRFs must have the back-end DB synchronized.

An IPv4 or IPv6 address of NRF must be configured in case NRF is outside the Kubernetes cluster. If NRF is inside the Kubernetes cluster, you can configure FQDN. If both IP address (IPv4 or IPv6) and FQDN are provided, IP address takes precedence over FQDN.

> **Note**
>
> - You must configure or remove the `apiPrefix` parameter based on the APIPrefix supported or not supported by NRF.
> - You must update the FQDN, IP address, and Port of NRF to point to NRF's FQDN or IP and Port. The primary NRF profile must be always set to higher, that is, 0. Ensure that the priority value of both primary and secondary profiles are not set to the same priority.

2.2.5 Configuring SCP as HTTP Proxy

To route messages towards SCP, Consumer NFs must use `<FQDN or IP Address>:<PORT of SCP-Worker>` of scp-worker in the `http_proxy/HTTP_PROXY` configuration.

> **Note**
>
> Run the following commands from where SCP worker and FQDN can be accessed.

Perform the following procedure to configure SCP as HTTP proxy:

1. To test successful deployment of SCP, run the following curl command:

   ```
   $ curl -v -X GET --url 'http://<FQDN:PORT of SCP-Worker>/nnrf-nfm/v1/
   subscriptions/' --header 'Host:<FQDN:PORT of NRF>'
   ```

2. Fetch the current subscription list as a client from NRF by sending the request to NRF through SCP:
   Example:

   ```
   $ curl -v -X GET --url 'http://scp-worker.scpsvc:8000/nnrf-nfm/v1/
   subscriptions/' --header 'Host:ocnrf-ambassador.nrfsvc:80'
   ```

2.2.6 Configuring Multus Container Network Interface

Perform the following procedure to configure Multus Container Network Interface (CNI) after SCP installation is complete.

> **Note**
>
> To verify whether this feature is enabled, see "Verifying the Availability of Multus Container Network Interface" in *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.

1. In the Kubernetes cluster, create a NetworkAttachmentDefinition (NAD) file.

   Example of a NAD file name: `ipvlan-sig.yaml`

   Sample NAD file:

   ```
   apiVersion: "k8s.cni.cncf.io/v1"

   kind: NetworkAttachmentDefinition

   metadata:

     name:ipvlan-siga

   spec:

     config: '{

         "cniVersion": "0.3.1",

         "type": "ipvlan",

         "primary": "eth1",
   ```

```
      "mode": "l2",
      "ipam": {
        "type": "host-local",
        "subnet": "<signaling-subnet>",
        "rangeStart": "x.x.x.x.",
        "rangeEnd": "x.x.x.x",
        "routes": [
          { "dst": "<nsx_lb_network_address_AMF>"}   ,
           { "dst":"<nsx_lb_network_address_SMF>"}  ,
            { "dst":"<nsx_lb_network_address_NRF>"} ,
            { "dst":"<nsx_lb_network_address_UDR>"} ,
             { "dst":"<nsx_lb_network_address_CHF>"} ,
             ],
        "gateway": "x.x.x.x"
      }
    }'
```

2. Run the following command to create a NetworkAttachmentDefinition custom resource for defining the Multus CNI network interfaces and their routing details:

   ```
   kubectl apply -f <NAD_file_name> –n <namespace>
   ```

   Example:

   ```
   kubectl apply -f ipvlan-sig.yaml –n scpsvc
   ```

3. Add the following annotation to the deployment for which additional network interfaces need to be added by Multus CNI:

   ```
   k8s.v1.cni.cncf.io/networks: <network as defined in NAD>
   ```

   Where, `<network as defined in NAD>` indicates the network as defined in NetworkAttachmentDefinition.

   Sample values.yaml file:

   ```
   scp-worker:
     deployment:
       # Labels and Annotations that are specific to deployment are added
   here.
   ```

```
    customExtension:
      labels: {}
      annotations: {k8s.v1.cni.cncf.io/networks: '[{ "name": "macvlan-
siga"}]'}
```

2.2.7 Adding and Removing IP-based Signaling Services

The following subsections describe how to add and remove IP-based Signaling Services as part of the Support for Multiple Signaling Service IPs feature.

2.2.7.1 Adding a Signaling Service

Perform the following procedure to add an IP-based signaling service.

1. Open the `ocscp_values.yaml` file.
2. In the `serviceSpecifications` section, add a new service under the `workerServices` list similar to the default service as follows:

```
name: "<service_name>"
#type:LoadBalancer
networkNameEnabled: false
networkName: "metallb.universe.tf/address-pool: signaling"
publicSignalingIPSpecified: true
publicSignalingIP: <IP address>
publicSignalingIPv6Specified: false
publicSignalingIPv6: <IP address>
ipFamilyPolicy: *workerIpFamilyPolicy
ipFamilies: *workerIpFamilies
port:
staticNodePortEnabled: false
nodePort: <Port number>
nodePortHttps: <Port number>
customExtension:
labels: {}
annotations: {}
```

Where,

- `<service_name>` is the name of the service.
- `<IP address>` is the signaling IP address of the service.
- `<Port number>` is the port number of the service.

Example:

```
name: "scp-worker-net1"
#type:LoadBalancer
networkNameEnabled: false
networkName: "metallb.universe.tf/address-pool: signaling"
publicSignalingIPSpecified: false
publicSignalingIP: 10.75.212.100
publicSignalingIPv6Specified: true
publicSignalingIPv6: 2001:db8:85a3::8a2e:370:7334
ipFamilyPolicy: *workerIpFamilyPolicy
ipFamilies: *workerIpFamilies
```

```
port:
staticNodePortEnabled: false
nodePort: 30075
nodePortHttps: 30076
customExtension:
labels: {}
annotations: {}
```

3. Optional: To add preferable IP addresses for NRF callback, in the `global` section, under the `scpSubscriptionInfo` parameter, add the IP address of the new service to `ip`.

   You can provide either IPv4 or IPv6 address.

   Example:

   ```
   scpSubscriptionInfo:
         ip: "10.75.212.100" # metallb or primaryIp, this ip will be obtained
   from metallb pool. Here either IPv4 or IPv6 address can be provided.
         Scheme to use in callbackURI, either http or https
         scheme: "http"
   ```

4. Save the file.
5. Run the following Helm upgrade command and wait until the upgrade is complete:

   > **Note**
   >
   > It is recommended to perform the Helm upgrade on the same version of SCP that contains the newly added IP-based signaling service.

   ```
   helm upgrade <release_name> <helm_repo/helm_chart>  --version
   <chart_version> -f <ocscp_values.yaml> --namespace  <namespace-name>
   ```

   Where,

   - `<release_name>` is the release name used by the Helm command.
   - `<helm_repo/helm_chart>` is the location of the Helm chart extracted from the target `ocscp_csar_25_2_2_0_1_0.zip` file.
   - `<chart_version>` is the version of the Helm chart extracted from the `ocscp_csar_25_2_2_0_1_0.zip` file.
   - `<ocscp_values.yaml>` is the SCP customized values.yaml file.
   - `<namespace-name>` is the SCP namespace in which the SCP release is deployed.

   Example:

   ```
   helm upgrade ocscp ocscp-helm-repo/ocscp --version 25.2.201 -f
   ocscp_values.yaml --namespace ocscp
   ```

6. Run the following command to check whether the service is available:

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

2.2.7.2 Removing a Signaling Service

Perform the following procedure to remove an IP-based signaling service.

Before removing any IP address, ensure that no traffic is routed to that IP. For more information, you can refer to SCP dashboard metrics in the *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

1. Open the `ocscp_values.yaml` file.
2. Locate the `publicSignalingIP` IP of the signaling service that you want to remove and set the corresponding `publicSignalingIPSpecified` parameter to `false`.

   Example:

   ```
   publicSignalingIPSpecified: false
   publicSignalingIP: 10.75.212.88
   ```

3. Optional: If the service `ip` being removed is already part of `scpSubscriptionInfo`, then do one of the following:
   - To update the alternate IP: In the `global` section, under the `scpSubscriptionInfo` parameter, update the `ip` parameter with the preferred service IP address.
   - To remove the alternate IP: In the `global` section, under the `scpSubscriptionInfo` parameter, remove the IP address.
4. Save the file.
5. Run the following Helm upgrade command and wait until the upgrade is complete:

   > **Note**
   >
   > It is recommended to perform the Helm upgrade on the same version of SCP that already contains IP-based signaling service.

   ```
   helm upgrade <release_name> <helm_repo/helm_chart>  --version
   <chart_version>
         -f <ocscp_values.yaml> --namespace  <namespace-name>
   ```

   Where,

   - `<release_name>` is the release name used by the Helm command.
   - `<helm_repo/helm_chart>` is the location of the Helm chart extracted from the target `ocscp_csar_25_2_2_0_1_0.zip` file.
   - `<chart_version>` is the version of the Helm chart extracted from the `ocscp_csar_25_2_2_0_1_0.zip` file.
   - `<ocscp_values.yaml>` is the SCP customized `values.yaml` file.
   - `<namespace-name>` is the SCP namespace in which the SCP release is deployed.

   Example:

   ```
   helm upgrade ocscp ocscp-helm-repo/ocscp --version 25.2.201 -f
   ocscp_values.yaml --namespace ocscp
   ```

6. Perform one of the following steps to clean up the deleted services:
   - To clean up Kubernetes services manually, run the following command:

     ```
     kubectl delete svc <svc_name> --namspace <namespace-name>
     ```

   - To clean up Kubernetes services through Helm upgrade, remove all the parameters of the removed IP-based service from the `serviceSpecifications` section of the `ocscp_values.yaml` file, and then perform the Helm upgrade as described in Step 7.

   Remove the following sample parameters manually from `serviceSpecifications`:

   ```
   name: "<service name>"
   #type:LoadBalancer
   networkNameEnabled: false
   networkName: "metallb.universe.tf/address-pool: signaling"
   publicSignalingIPSpecified: false
   publicSignalingIP: 10.75.212.88
   port:
   staticNodePortEnabled: true
   nodePort: 30075
   customExtension:
   labels: {}
   annotations: {}
   ```

3
Customizing SCP

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

The SCP deployment is customized by overriding the default values of various configurable parameters.

Perform the following procedure to customize the `ocscp_values.yaml` file as per the required parameters:

1. Unzip the `ocscp_csar_25_2_2_0_1_0.zip` folder available in the extracted release package. For more information about how to download the package from MOS, see Downloading the SCP Package.
2. Open the `Scripts` folder to get the following files that are used to customize the deployment parameters during installation:
   - `ocscp_values_25.2.201.yaml`: This file is used to customize the deployment parameters during installation.
   - `ocscp_servicemesh_config_values_25.2.201.yaml`: This file is used to configure ASM data plane in the ASM setup.
   - `ocscp_metric_dashboard_promha_25.2.201.json`: This file is used by Grafana to use for CNE with Prometheus Operator.
   - `ocscp_metric_dashboard_25.2.201.json`: This file is used by Grafana to use CNE with Prometheus.
   - `ocscp_alerting_rules_promha_25.2.201.yaml`: This file is used for Prometheus Operator.
   - `ocscp_alertrules_25.2.201.yaml`: This file is used for Prometheus.
   - `ocscp_oci_alertrules_25.2.201.zip`: This file is used for creating alerts from OCI terraform files.
   - `ocscp_oci_metric_dashboard_25.2.201.zip`: This file is used for viewing metrics information on the OCI monitoring dashboard.
   - `toplevel.mib`: This is a top level mib file that defines OIDs for all NFs.
   - `ocscp_mib_tc_25.2.201.mib`: This mib file defines Objects and their data types.
   - `ocscp_mib_25.2.201.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.
   - `ocscp_configuration_openapi_25.2.201.json`: This file is OPEN API specification for SCP configuration.
   - `ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml`: This file is used to install cnDBTier with resources recommended for SCP.
3. Customize the `ocscp_values_25.2.201.yaml` file available in the `Scripts` folder of `ocscp_csar_25_2_2_0_1_0.zip`.
4. Save the updated `ocscp_values_25.2.201.yaml` file in the `Files/Helm` folder.

For more information about the configurable parameters, see Configuration Parameters.

3.1 Configuration Parameters

The following sections provide configuration parameters in the Helm file.

3.1.1 Global Parameters

The following table lists the Global parameters:

> **Note**
>
> In the following table, the M/O/C column indicates Mandatory (M), Optional (O), and Conditional (C).

Table 3-1 Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`domain`	string	Labels can be letter a-z, number 0-9, hyphen (-). Hyphen cannot be first character. Label combined with dot (.) forms domain	svc.cluster.local	M	Option to configure the service domain of the Kubernetes cluster. To know cluster domain, run the following command: `kubectl -n kube-system get configmap kubeadm-config -o yaml | grep clusterName`
`clusterDomain`	string	Labels can be letter a-z, number 0-9, hyphen (-). Hyphen cannot be first character. Label combined with dot (.) forms domain	cluster.local	M	Option to configure the domain of the Kubernetes cluster. This value is similar to the domain value that excludes "svc". For example, if domain is `svc.cluster.local`, clusterDomain is `cluster.local`.
`serviceSpecifications.workerServices.publicSignalingIPSpecified`	Boolean	true/false	false	O	Option to enable or disable Loadbalancer IP configuration statically for the Signaling interface.
`serviceSpecifications.workerServices.publicSignalingIP`	IPv4 Address	Valid IPV4 address as per RFC 791	N/A	C	Option to configure static Signaling Loadbalancer IP. The configured value is used only if `signalingloadbalanceripenabled` is configured as `true`.
`serviceSpecifications.workerServices.ipFamilyPolicy`	*workerIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	C	ipFamilyPolicy to be allocated to scpWorker service. This value depends on global.serviceIpFamilyPolicy.scpWorker.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
serviceSpecifications.workerServices.ipFamilies	*workerIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	C	ipFamilies to be allocated to scpWorker service. This value depends on global.serviceIpFamilies.scpWorker.
serviceSpecifications.workerServices.publicSignalingIPv6	<IPv6 Address>	Valid IPv6 address	NA	C	Configures static signaling Loadbalancer IP. The configured value is used if publicSignalingIPv6Specified is configured as true.
serviceSpecifications.workerServices.publicSignalingIPv6Specified	<boolean>	true or false	false	O	Enables or disables Loadbalancer IPv6 configuration statically for Signaling interfaces.
adminport	integer	Min- 0, Max-65535	8001	M	Option to configure Admin Port that is used for debugging purpose.
imageRepository	string	valid repository	<scp_repository_path>:5000/ocscp	M	Set imageRepository to the repository where SCP images are loaded.
preventiveAuditOnLastNFInstanceDeletion	boolean	true/false	false	M	Flag to support preventive audit on the last NF instance deletion feature.
ignoreNrfRegionOrSetIdforNFProfileHash	boolean	true/false	false	M	Flag to include or exclude nrfRegionOrSetId in the nf profile hash calculation.
debugToolContainerMemoryLimit	string	2Gi	2Gi	M	Indicates container memory requests. This populates "resources.requests.memory" and "resources.limit.memory" sections.
extraContainersImageDetails.image	string	ocdebug-tools	ocdebug-tools	M	Indicates debug tool image name.
extraContainersImageDetails.tag	string	<debug_tools_tag>	<debug_tools_tag>	M	Indicates debug tool image tag.
extraContainersImageDetails.imagePullPolicy	string	Always	Always	M	Indicates Image Pull Policy.
extraContainersTpl.command	string array	/bin/sleep infinity	/bin/sleep infinity	M	Indicates string array used for container command.
extraContainersTpl.name	string	tools	tools	M	Indicates the name of the container.
extraContainersTpl.resources.limits	string	-	-	M	Limits describes the maximum amount of compute resources allowed.
extraContainersTpl.resources.requests	string	-	-	M	Requests describes the minimum amount of compute resources required.
extraContainersTpl.resources.limits.cpu	integer	1	1	M	Indicates CPU limits.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
extraContainersTpl.resources.limits.memory	string	2Gi	2Gi	M	Indicates memory limits.
extraContainersTpl.resources.limits.ephemeral-storage	string	4Gi	4Gi	M	Indicates ephemeral storage limits.
extraContainersTpl.resources.requests.cpu	integer	0.5	0.5	M	Indicates CPU requests.
extraContainersTpl.resources.requests.memory	string	1Gi	1Gi	M	Indicates memory requests.
extraContainersTpl.resources.requests.ephemeral-storage	string	2Gi	2Gi	M	Indicates ephemeral storage requests.
extraContainersTpl.volumeMounts	string	NA	NA	M	Mounts the volume.
extraContainersTpl.volumeMounts.mountPath	string	NA	/tmp/tools	M	Path for volume mount.
extraContainersTpl.volumeMounts.name	string	NA	debug-tools-dir	M	Name of the directory for debug tool logs storage.
extraContainersVolumesTpl.name	string	NA	debug-tools-dir	M	Name of the volume for debug tool logs storage. This should be the same as the extraContainersTpl.volumeMounts.name.
extraContainersVolumesTpl.emptyDir.medium	String	memory	memory	M	Location of the emptyDir volume.
extraContainersVolumesTpl.emptyDir.sizeLimit	String	NA	2Gi	M	Size of the emptyDir volume.
serviceMeshEnabled	boolean	true/false	false	M	Indicates if the service mesh is used.
serviceLogLevels.scpcAudit	string	DEBUG/ INFO/ WARN/ ERROR	&auditLogLevelRef INFO	M	Indicates the log level for scpc-audit microservice. **Note**: Do not change the reference variable (&auditLogLevelRef).
serviceLogLevels.scpcConfiguration	string	DEBUG/ INFO/ WARN/ ERROR	&configLogLevelRef INFO	M	Indicates the log level for scpc-configuration microservice. **Note**: Do not change the reference variable (&configLogLevelRef).
serviceLogLevels.scpcSubscription	string	DEBUG/ INFO/ WARN/ ERROR	&subsLogLevelRef INFO	M	Indicates the log level for scpc-subscription microservice. **Note**: Do not change the reference variable (&subsLogLevelRef).

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`serviceLogLevels.scpcNotification`	string	DEBUG/ INFO/ WARN/ ERROR	&notifLogLevelRef INFO	M	Indicates the log level for scpc-notification microservice. **Note**: Do not change the reference variable (&notifLogLevelRef).
`serviceLogLevels.scpNrfProxy`	string	DEBUG/ INFO/ WARN/ ERROR	&nrfproxyLogLevelRef WARN	M	Indicates the log level for scp-nrfproxy microservice. **Note**: Do not change the reference variable (&nrfproxyLogLevelRef).
`serviceLogLevels.scpcAlternateResolution`	string	NA	INFO	M	Identifies the log level of the scpc-alternate-resolution microservice. **Note**: You must enable `scpcAlternateResolution` and `rel16` parameters to use the scpc-alternate-resolution microservice.
`serviceLogLevels.scpCache`	string	DEBUG/ INFO/ WARN/ ERROR	&cacheLogLevelRef WARN	M	Indicates the log level for scp-cache microservice. **Note**: Do not change the reference variable (&cacheLogLevelRef).
`serviceLogLevels.scpWorker`	string	DEBUG/ INFO/ WARN/ ERROR	&workerLogLevelRef WARN	M	Indicates the log level for scp-worker microservice. **Note**: Do not change the reference variable (&workerLogLevelRef).
`serviceLogLevels.scpMediation`	string	DEBUG/ INFO/ WARN/ ERROR	WARN	M	Indicates the log level for scp-worker microservice. The reference variable **Note**: Do not change the reference variable (&mediationLogLevelRef).
`test.nfName`	string	NA	ocscp	M	NF name on which the helm test is performed.
`test.image.name`	string	NA	nf_test	M	Image name for the helm test container image.
`test.image.tag`	string	NA	25.2.201	M	Image tag to be used for helm test container.
`test.image.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Image pull policy.
`test.config.logLevel`	string	Possible Values - WARN INFO DEBUG	WARN	M	Log level for helm test pod.
`test.config.timeout`	integer	Min-0, Max:65535 Unit: seconds	240	M	Option timeout is the total time required for deployment of OCSCP and helm test to take place for checking the readiness probe of OCSCP pods.
`podResources.limits`	integer	NA	cpu: 1.1 memory: 1Gi	M	Populates limit for nf-test.
`podResources.requests`	integer	NA	cpu: 1.1 memory: 1Gi	M	Populates requests for nf-test.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`test.resources`	string	NA	- horizontalpodautoscalers/v1 - deployments/v1 - configmaps/v1 - serviceaccounts/v1 - roles/v1 - services/v1 - rolebindings/v1	M	Helm resources to be tested.
`test.complianceEnable`	boolean	NA	true	M	Performs compliance check for each Kubernetes resource.
`customExtension.allResources.lables`	string	Kubernetes label object syntax	{}	O	Option to configure custom labels for the entire deployment applicable to all resource types. Format is: `<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value> .....`

`customExtension.allResources.annotations`	string	Kubernetes annotation object syntax	{}	O	Option to configure custom annotations for the entire deployment applicable to all resource types. Format is:
					`<string_annotation_1_key>:`
					`<string_annotation_1_value>`
					`<string_annotation_2_key>:`
					`<string_annotation_2_value>`
					`.....`
					
					Note: The following are the mandatory annotations if you are deploying SCP in Aspen Service Mesh:
					`sidecar.istio.io/inject: "false"`

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
customExtension.hooks.labels	string	K8s label object syntax	{}	O	Option to configure custom labels for Helm hook resources (pre/post install/upgrade/rollback hooks). Provide sidecar related labels for hooks. This section can be utilized for sidecar resources of hooks under annotations. hooks: labels: <string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>
customExtension.hooks.annotations	string	K8s annotation object syntax	{}	O	Option to configure custom annotations for Helm hook resources (pre/post install/upgrade/rollback hooks). Provide sidecar related annotation for hooks. This section can be utilized for sidecar resources of hooks under annotations. annotations: <string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>
customExtension.serviceaccount.labels	string	K8s label object syntax	{}	O	Option to configure custom labels for ServiceAccount. labels: <string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
customExtension.serviceaccount.annotations	string	K8s annotation object syntax	{}	O	Option to configure custom annotations for ServiceAccount. annotations: <string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>
customExtension.lbServices.labels	string	Kubernetes label object syntax	{}	O	Option to configure custom labels for the LoadBalancer pods of the deployment applicable to "Service" resource type. Format is: <string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value> .....

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description

`customExtension.lbServices.annotations`	string	Kubernetes annotation object syntax	{}	O	Option to configure custom annotations for the LoadBalancer pods of the deployment applicable to "Service" resource type. Format is:
					
					`<string_annotation_1_key>:`
					
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					
					`<string_annotation_2_value>`
					`.....`
					
					Note: Following is the mandatory annotations if you are deploying SCP in Aspen Service Mesh:
					
					`sidecar.istio.io/inject: "true"`
					
					If SCP is integrated with OSO 1.6 (with ASM), use the following annotations: `oracle.com/cnc: "true"`

`customExtension.lbDeployments.labels`	string	Kubernetes label object syntax	{}	O	Option to configure custom labels for the LoadBalancer pods of the deployment applicable to "Deployment" resource type. Format is:
					
					`<string_label_1_key>:`
					`<string_label_1_value>`
					`<string_label_2_key>:`
					`<string_label_2_value>`
					`......`

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
customExtension.lbDeployments.annotations	string	Kubernetes annotation object syntax	{}	O	Option to configure custom annotations for the LoadBalancer pods of the deployment applicable to "Deployment" resource type. Format is: <string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value> .....
customExtension.nonlbServices.labels	string	Kubernetes label object syntax	{}	O	Option to configure custom labels for the Non LoadBalancer pods of the deployment applicable to "Service" resource type. Format is: <string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value> .....
customExtension.nonlbServices.annotations	string	Kubernetes annotation object syntax	{}	O	Option to configure custom annotations for the Non LoadBalancer pods of the deployment applicable to "Service" resource type. Format is: <string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value> .....

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`customExtension.nonlbDeployments.labels`	string	Kubernetes label object syntax	{}	O	Option to configure custom labels for the Non LoadBalancer pods of the deployment applicable to "Deployment" resource type. Format is: `<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value> ......`

`customExtension.nonlbDeployments.annotations`	string	Kubernetes annotation object syntax	{}	O	Option to configure custom annotations for the Non LoadBalancer pods of the deployment applicable to "Deployment" resource type. Format is:
					
					`<string_annotation_1_key>:`
					
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					
					`<string_annotation_2_value>` `.....`
					
					Note: Following is the mandatory annotations if you are deploying SCP in Aspen Service Mesh:
					
					`sidecar.istio.io/inject: "true"`
					
					If SCP is integrated with OSO 1.6 (with ASM), use the following annotations: `oracle.com/cnc: "true"`

`k8sResource.container.prefix`	string	NA	{}	O	Option to add prefix to container names.
`k8sResource.container.suffix`	string	NA	{}	O	Option to add suffix to container names.
`hookJob.resources.limits.cpu`	integer	N/A	3	M	Maximum limit of CPU for hook job.
`hookJob.resources.limits.memory`	integer	N/A	3Gi	M	Maximum limit of memory for hook job in Giga Bytes.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`hookJob.resources.requests.cpu`	integer	N/A	3	M	Maximum allocated vCPU for hook job.
`hookJob.resources.requests.memory`	integer	N/A	3Gi	M	Requested memory (RAM) for hook job in Giga Bytes.
`hookAlerts.prometheus.fqdn`	string	N/A	occne-prometheus-server.occne-infra.svc.cluster.local	M	Fully Qualified Domain Name of Prometheus. **Note**: This configuration is required to ensure that alerts are raised when rollback to this release is performed.
`hookAlerts.prometheus.port`	integer	Valid port value	80	M	Port of Prometheus. **Note**: This configuration is required to ensure that alerts are raised when rollback to this release is performed.
`hookAlerts.prometheus.pathToFetchAlertManagerEndPoint`	string	N/A	"/prometheus/api/v1/alertmanagers"	M	Path to obtain Alertmanager endpoint. **Note**: This configuration is required to ensure that alerts are raised when rollback to this release is performed.
`hookAlerts.alertManagerContainerPort`	integer	Valid port value	9093	M	Alertmanager container port. **Note**: This configuration is required to ensure that alerts are raised when rollback to this release is performed.
`hookAlerts.customAlertExpiryEnabled`	boolean	true/false	false	M	This variable indicates that alert expiry occurs according to the `resolve_timeout` value of Alertmanager and upgrade or rollback hooks clear the alerts as applicable. If it is set to `true`, auto alert clear occurs after the `customAlertExpiryDuration` value and upgrade or rollback hooks may not clear the alerts. **Note**: This configuration is required to ensure that alerts are raised when rollback to this release is performed.
`hookAlerts.customAlertExpiryDuration`	integer		60	M	The custom duration (in minutes) post which alerts are automatically cleared. It is applicable only when `customAlertExpiryEnabled` is set to `true`. **Note**: This configuration is required to ensure that alerts are raised when rollback to this release is performed.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
database.dbHost	string	Valid IPv4 address as per RFC 791 or Valid FQDN	N/A	M	Hostname or IP address of DB connection service.
database.dbPort	string	Valid port value	N/A	M	Port for MySQL Database connection service.
database.dbAppUserSecretName	string	N/A	N/A	M	Name of the Kubernetes secret object containing the Database username and password.
database.dbPrivilegedUserSecretName	string	N/A	N/A	M	Name of the Kubernetes secret object containing the Database username and password for an admin user.
database.createUser	boolean	true/false	true	M	This parameter can enable or disable the automatic database and application user creation.
coherence.clusterName	string	N/A	scp-coherence-cluster	M	This is the name of the cluster that is created by Coherence. It must not exceed 66 characters.
coherence.federation.remoteScpOne.fqdnOrIp	string	NA	ocscp-scp-cache.fedsvc.svc.cluster.local	M	Indicates the remote SCP Federation Service FQDN or IP.
coherence.federation.remoteScpOne.port	integer	valid port range	30001	M	Indicates the remote SCP Federation Container and Service Port.
coherence.federation.remoteScpOne.clusterName	string	NA	ocscp-scp-coherence-cluster-fedsvc	M	Indicates the name of the cluster that is created by Coherence. It must not exceed 66 characters. **Note**: The only reason to keep it outside, if two different SCP cluster names become identical, this field must be changed.
coherence.federation.remoteScpOne.nfInstanceId	string	NA	6faf1bbc-6e4a-4454-a507-a14ef8e1bc5f	M	Indicated the NFInstanceId of the remote SCP.
coherence.federation.remoteScpTwo.fqdnOrIp	string	NA	ocscp-scp-cache.fed2svc.svc.cluster.local	M	Indicates the remote SCP Federation Service FQDN or IP.
coherence.federation.remoteScpTwo.port	integer	valid port range	30001	M	Indicates the remote SCP Federation Container and Service Port.
coherence.federation.remoteScpTwo.clusterName	string	NA	ocscp-scp-coherence-cluster-fed2svc	M	Indicates the name of the cluster that is created by Coherence. It must not exceed 66 characters. **Note**: The only reason to keep it outside, if two different SCP cluster names become identical, this field must be changed.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
coherence.federation.remoteScpTwo.nfInstanceId	string	NA	6faf1bbc-6e4a-4454-a507-a14ef8e1bc5d	M	Indicated the NFInstanceId of the remote SCP.
scpProfileInfo.fqdn	string	Labels can be alphanumeric and can also include hyphen (-). Hyphen cannot be the first character. Label combined with dot (.) forms domain.	N/A	M	Fully Qualified Domain Name of SCP. You can define the SCP FQDN value.
scpProfileInfo.nfType	string	CUSTOM_ORACLE_SCP, SCP	SCP	M	Indicates the NF type.
scpProfileInfo.locality	string	location of SCP.	NA	M	Locality of the SCP Instance, for example, geographic location and data center. Same locality must be present in ServingLocalities. **Note**: This value is case-sensitive.
scpProfileInfo.priority	integer	0 to 65535	1	O	Mention the priority of SCP. **Note**: The priority is considered within an SCP set.
scpProfileInfo.capacity	integer	0 to 65535	65535	O	Mention the capacity of SCP. **Note**: The capacity is considered within an SCP set.
scpProfileInfo.load	integer	0 to 100	0	O	Mention the load of SCP.
scpProfileInfo	array(ExtSnssai)	NA	NA	O	Specifies the list of Single Network Slice Selection Assistance Information (S-NSSAIs) supported by SCP. Each S-NSSAI consists of a mandatory Slice/Service Type (SST) and an optional Slice Differentiator (SD) used to differentiate slices with the same SST.
scpProfileInfo.plmnList.mcc	string	Must be of three digits ranging from 0 to 9	"410"	O	Indicates the mobile country code required for PLMN IDs supported by SCP. This PLMN List is managed by the SCP and is utilized in roaming scenarios to route requests to the SCP if it supports the specified PLMN.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`scpProfileInfo.plmnList.mnc`	string	Can be of two or three digits ranging from 0 to 9	"213"	O	Indicates the mobile network code required for PLMN IDs supported by SCP. This PLMN List is managed by the SCP and is utilized in roaming scenarios to route requests to the SCP if it supports the specified PLMN.
`scpProfileInfo.customInfo.mateScpInfo.capacity`	integer	Min = 0, Max = 65535	500	M	Static capacity information in the range of 0-65535 expressed as a weight relative to other SCP instances of the same type. **Note**: The `mateScpInfo` object is not applicable for SCP Release 16 deployment, so comment this parameter and populate the mate (alternate) SCP instance information in the `mateScpInfoList` object.
`scpProfileInfo.customInfo.mateScpInfo.priority`	integer	Priority: Min = 0, Max = 65535.	5	M	Priority, relative to other mate SCP instance, in the range of 0-65535. **Note**: The `mateScpInfo` object is not applicable for SCP Release 16 deployment, so comment this parameter and populate the mate (alternate) SCP instance information in the `mateScpInfoList` object.
`scpProfileInfo.customInfo.mateScpInfo.mateSCPLocalities`	string	Localities: As per 3GPP TS 29.510 spec	mateSCPLocalities: - Loc10	M	List of mated localities of SCP. **Note**: The `mateScpInfo` object is not applicable for SCP Release 16 deployment, so comment this parameter and populate the mate (alternate) SCP instance information in the `mateScpInfoList` object.
`scpProfileInfo.customInfo.mateScpInfo.scpFqdn`	string	Labels can be letter a-z, number 0-9, hyphen (-). Hyphen cannot be first character. Label combined with dot (.) forms domain	N/A	M	Fully Qualified Domain Name of SCP Format: <releaseName>-scpworker.< Namespace>.<domain> **Note**: The `mateScpInfo` object is not applicable for SCP Release 16 deployment, so comment this parameter and populate the mate (alternate) SCP instance information in the `mateScpInfoList` object.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
scpProfileInfo.customInfo.mateScpInfo.scpInstanceId	string	String uniquely identifying SCP service instance. The format of the SCP Service Instance ID is Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [15].	N/A	O	Instance ID of the SCP service. **Note**: The mateScpInfo object is not applicable for SCP Release 16 deployment, so comment this parameter and populate the mate (alternate) SCP instance information in the mateScpInfoList object.
scpProfileInfo.customInfo.mateScpInfoList[].capacity	integer	Min = 0, Max = 65535	500	M	Static capacity information in the range of 0-65535, expressed as a weight relative to other mate SCP instance. **Note**: This parameter is applicable only for Release 16 SCP deployment.
scpProfileInfo.customInfo.mateScpInfoList[].priority	integer	Priority: Min = 0, Max = 65535.	5	M	priority: (relative to other SCPs) in the range of 0-65535 to be used for NF selection; lower values indicate a higher priority. **Note**: This parameter is applicable only for Release 16 SCP deployment.
scpProfileInfo.customInfo.mateScpInfoList[].scpFqdn	string	Labels can be letter a-z, number 0-9, hyphen (-). Hyphen cannot be first character. Label combined with dot (.) forms domain	N/A	M	Fully Qualified Domain Name of the mated SCP Format: <releaseName>- scpworker.<Namespace>.<do main> **Note**: This parameter is applicable only for Release 16 SCP deployment.
scpProfileInfo.customInfo.mateScpInfoList[].scpInstanceId	string	String uniquely identifying SCP service instance. The format of the SCP Service Instance ID is Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [15].	N/A	O	Mated SCP instance ID. **Note**: This parameter is applicable only for Release 16 SCP deployment.
scpProfileInfo.customInfo.mateScpInfoList[].mateSCPLocalities	string	Localities: As per 3GPP TS 29.510 spec	mateSCPLocalities: - Loc10	M	List of mated SCP localities. **Note**: This parameter is applicable only for Release 16 SCP deployment.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
scpProfileInfo.customInfo.servingLocalities	string	NA	servingScope: Loc7, Loc8, Loc9, USEast	M	List of serving localities of SCP apart from the locality present in the "locality" attribute. **Note**: This value is case-sensitive.
scpProfileInfo.customInfo.mateSiteInfo	map	NA	mateSiteInfo: mateSite1: mateSiteLocalities: - Loc21 - Loc22 mateSite2: mateSiteLocalities: - Loc31 - Loc32	O	Indicates the map of 5G NFs localities in each mate site. The key of the map is a string type that represents the unique name of the mate site. The value is MateSiteLocalities with 5G NFs localities in the mate site.
scpProfileInfo.customInfo.mateSiteInfo.mateSiteLocalities	array	NA	NA	O	Indicates the list of 5G NFs localities in each mate site.
scpProfileInfo.customInfo.supportedNRFRegionOrSetIdList	string	NA	scpToRegisterWithNrfRegions ["setnrfl1.nrfset.5gc.mnc012.mcc345", "setnrfr1.nrfset.5gc.mnc012.mcc345"]	M	List of supported NRF SetIds in Release 16.
scpProfileInfo.nfInstanceId	string	String uniquely identifying a NF instance. The format of the NF Instance ID shall be a Universally Unique Identifier (UUID) version 4 as described in IETF RFC 4122 [15].	N/A	M	String uniquely identifying the SCP instance. The format of the Instance ID is a Universally Unique Identifier (UUID) version 4 as described in IETF RFC 4122.
scpProfileInfo.servingScope	string	NA	NA	C	5G NFs localities to be served by the SCP instance.
scpProfileInfo.nfSetIdList	string	NA	NA	C	NF Set ID to which SCP belongs to.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
scpProfileInfo.scpInfo.scpPrefix	string	NA	NA	O	This is an optional deployment specific string to construct the apiRoot of the next hop SCP. For more information, see Clause 6.10 of 3GPP TS 29.500. If the provided scpPrefix matches apiPrefix present in the received request URI (for both notification and service requests), it will be removed. Therefore, it is recommended to keep scpPrefix unique, to ensure that it does not match with any other apiPrefix and result in routing failure.
scpProfileInfo.scpInfo.scpPorts.https	integer	Min - 0, Max - 65535	9443	C	SCP port number for HTTPS. Example: https: 9443 **Note:** With https port being uncommented, http cannot be commented as it is required for internal communication by SCP.
scpProfileInfo.scpInfo.scpPorts.http	integer	Min- 0, Max-65535	8000	M	SCP port number for HTTP. This port cannot be commented as it is required by SCP for internal communication. Example: http: 8000
nrfProfiles.nfServices.capacity	integer	0 to 65535	5000	O	Capacity of the NRF among the NRF list. It is used for load balancing between the NRFs.
nrfProfiles.nfServices.apiPrefix	string	Can be combination of letters from a-z and A-Z	NA	O	Location of NRF.
nrfProfiles.nfServices.fqdn	string	fqdn: Labels can be letter a-z, number 0-9, hyphen(-). Hyphen cannot be first character. Label combined with dot(.) forms domain.	NA	O	FQDN of NRF.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
nrfProfiles.nfServices.ipEndPoints	list of IP address and port	[{"ipv4Address": <IpV4 Address>, "port": <integer>}] or [{"ipv6Address": <IpV6 Address>, "port": <integer>}] or [{"ipv4Address": <IpV4 Address>, "port": <integer>}, {"ipv6Address": <IpV6 Address>, "port": <integer>}]	NA	O	List of IPv4 Address or IPv6 Address, or both IPv4 and IPv6 Addresses transport and port combination of the given NRF.
nrfProfiles.nfServices.load	integer	0 to 100	0	O	Mention the load of the service.
nrfProfiles.nfServices.nfServiceStatus	string	REGISTERED or SUSPENDED (TS 29.510)	REGISTERED	O	Status of service. It is not used by SCP but must be present in the NF profile format with all mandatory fields.
nrfProfiles.nfServices.scheme	string	NA	http	O	HTTP scheme.
nrfProfiles.nfServices.serviceInstanceId	string	String uniquely identifying a NF service instance. The format of the NF Service Instance ID is Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [15].	f86b54b7-aef9-4c78-b346-3bfb7f380812	O	Instance ID of the SCP service. **Note**: • If you want to configure any services, you must provide the configuration while deploying it through Helm using the custom `ocscp_values.yaml` file. • When SCP is deployed with Release 16 and the NF type is SCP, comment all the parameters under the `nfServices` category.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
nrfProfiles.nfServices.serviceName	string	NA	nnrf-nfm	O	Supported values for serviceName: • nscp-5g-sbi-proxy (Proxy Service) • nmediation-http (Mediation service) • nscp-5g-sbi-proxy is a mandatory service. However, when nftype is SCP, this service is not mandatory. The other two services are optional. If these services are provided with nfServiceStatus REGISTERED, they register with NRF. If nfServiceStatus is SUSPENDED or UNDISCOVERABLE, then there is no registration with NRF for the corresponding service. If provided irrespective of nfServiceStatus, they are used in virtual service creation. **Note**: nmediation-http service is optional. If you want to configure any of these services, then the user must provide this configuration while deploying it through helm using the custom ocscp_values.yaml file.
nrfProfiles.nfServices.priority	integer	0 to 65535	0	O	Priority of NRF among the NRF list. It is used for load balancing between the NRFs.
nrfProfiles.nfServices.versions.apiFullVersion	string	NA	1.0.0	O	Version of API.
nrfProfiles.nfServices.versions.apiVersionInUri	string	NA	v1	O	URI of API.
nrfProfiles.nfServices.capacity	integer	0 to 65535	5000	O	Capacity of the NRF among the NRF list. It is used for load balancing between the NRFs.
nrfProfiles.nfServices.apiPrefix	string	Can be combination of letters from a-z and A-Z	NA	O	Location of NRF.
nrfProfiles.nfServices.fqdn	string	fqdn: Labels can be letter a-z, number 0-9, hyphen(-). Hyphen cannot be first character. Label combined with dot(.) forms domain.	NA	O	FQDN of NRF.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`nrfProfiles.nfServices.ipEndPoints`	list of IP address and port	[{"ipv4Address": <IpV4 Address>, "port": <integer>}] or [{"ipv6Address": <IpV6 Address>, "port": <integer>}] or [{"ipv4Address": <IpV4 Address>, "port": <integer>}, {"ipv6Address": <IpV6 Address>, "port": <integer>}]	NA	O	List of IPv4 Address or IPv6 Address, or both IPv4 and IPv6 Addresses transport and port combination of the given NRF.
`nrfProfiles.nfServices.load`	integer	0 to 100	0	O	Mention the load of the service.
`nrfProfiles.nfServices.nfServiceStatus`	string	REGISTERED or SUSPENDED (TS 29.510)	REGISTERED	O	Status of service. It is not used by SCP but must be present in the NF profile format with all mandatory fields.
`nrfProfiles.nfServices.scheme`	string	NA	http	O	HTTP scheme.
`nrfProfiles.nfServices.serviceInstanceId`	string	String uniquely identifying a NF service instance. The format of the NF Service Instance ID is Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [15].	f86b54b7-aef9-4c78-b346-3bfb7f380812	O	Instance ID of the SCP service. **Note**: • If you want to configure any services, you must provide the configuration while deploying it through Helm using the custom `ocscp_values.yaml` file. • When SCP is deployed with Release 16 and the NF type is SCP, comment all the parameters under the `nfServices` category.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`nrfProfiles.nfServices.serviceName`	string	NA	nnrf-disc	O	Supported values for serviceName: • nscp-5g-sbi-proxy (Proxy Service) • nmediation-http (Mediation service) • nscp-5g-sbi-proxy is a mandatory service. However, when nftype is SCP, this service is not mandatory. The other two services are optional. If these services are provided with nfServiceStatus REGISTERED, they register with NRF. If nfServiceStatus is SUSPENDED or UNDISCOVERABLE, then there is no registration with NRF for the corresponding service. If provided irrespective of nfServiceStatus, they are used in virtual service creation. **Note**: nmediation-http service is optional. If you want to configure any of these services, then the user must provide this configuration while deploying it through helm using the custom `ocscp_values.yaml` file.
`nrfProfiles.nfServices.priority`	integer	0 to 65535	0	O	Priority of NRF among the NRF list. It is used for load balancing between the NRFs.
`nrfProfiles.nfServices.versions.apiFullVersion`	string	NA	1.0.0	O	Version of API.
`nrfProfiles.nfServices.versions.apiVersionInUri`	string	NA	v1	O	URI of API.
`scplocalityconfig.mapping_param`	string	LOCALITY, NFINSTANCEID, FQDN	LOCALITY	M	Mapping parameter or the key to look for is used to query the corresponding field in NF profile received in response to NF discovery. This configuration is used to update the Discovery response based on the match criteria (id_value) with SCP IP/Port/FQDN in NF Profile received. It is used to handle AMF discovery from any consumer so that consumer can send requests back to SCP and not directly to AMF after discovering it. For this functionality, consumers must send AMF discovery requests to SCP.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
scplocalityconfig.mapping_info.id_value	string	NA	N/A	M	Used to match value against the value obtained from the mapping parameter.
scplocalityconfig.mapping_info.ip_v4_address	string	Valid IPV4 address as per RFC 791	NA	M	The IP address to be used while updating ipv4Address and callback URI in NF discovery response.
scplocalityconfig.mapping_info.fqdn	string	Labels can be letter a-z, number 0-9, hyphen (-). Hyphen cannot be first character. Label combined with dot (.) forms domain.	NA	M	The FQDN to be used while updating FQDN in the NF discovery response.
scplocalityconfig.mapping_info.port	integer	0 to 65535	NA	M	The port to be used while updating port in NF discovery response.
PROBING_LISTENER_PORT	integer	Min- 0, Max-65535	8002	M	This port is used by scp-worker listening for probing.
SIGNALLING_LISTENER_PORT	integer	Min- 0, Max-65535	8080	M	The signaling listener port used by scp-worker.
SIGNALLING_LISTENER_PORT_HTTPS	integer	Min- 0, Max-65535	9443	O	This port will be used for scp-worker listening for signaling of HTTPS connections. **Note**: This parameter is mandatory when HTTPS is enabled.
scpServiceAccountName	string	NA	&scpServiceAccountName ""	O	Indicates the service account used by SCP pods. You may provide SCP service account but if it is left blank or removed, a default service account is created by SCP for its use. Default is empty. The following rules are required by SCP: rules: `- apiGroups: [""] resources: - pods - services - configmaps verbs: ["get", "list", "watch"] - apiGroups: - "" # "" indicates the core API group resources: - secrets - endpoints verbs: ["get", "list", "watch"]` For information about defining permissions using roles for SCP, see Manually Creating Service Account, Role, and Rolebinding.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`autoCreateResources.enabled`	boolean	true or false	false	M	Controls the automated creation of Kubernetes resources such as service accounts using Helm charts.
`serviceAccounts.create`	boolean	true or false	true	M	Controls automatic creation of service accounts. This parameter is valid if `autoCreateResources` is enabled.
`serviceAccounts.accounts.scpServiceAccountName`	string	NA	*scpServiceAccountName	M	Takes the service account name as configured for `scpServiceAccountName`.
`serviceAccounts.accounts.type`	string	SCP	SCP	M	Specifies the type of service account. The type determines the predefined Role-Based Access Control (RBAC) rules applied during Helm installation and upgrade.
`securityContext.runAsUser`	Integer	-	1002	O	A security context defines privilege and access control settings for a pod or container. The default values is picked in case no parameter is provided for security context as mentioned in the following example: `securityContext: {}`
`securityContext.runAsGroup`	Integer	-	1002	O	Contains the primary group ID of the processes within any container of the pod.
`securityContext.fsGroup`	Integer	-	1002	O	Contains the supplemental group applied to some volumes. If the `fsGroup` field is specified, all process of container are also a part of the supplementary group for the given value.
`enableContainerSecurityContext`	Boolean	true or false	true	O	Enables security context for containers.
`containerSecurityContext`	allowPrivilegeEscalation: Boolean	true or false	false	M	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.
`containerSecurityContext.runAsNonRoot`	Boolean	true or false	true	M	Prevents containers from starting as root user.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
containerSecurityContext.readOnlyRootFilesystem	Boolean	true or false	false	M	Mounts the container's root filesystem as read-only.
containerSecurityContext.privileged	Boolean	true or false	false	M	Provides containers' access to the host's resources and kernel capabilities.
containerSecurityContext.runAsUser	Integer	Valid IDs for security context for user	10000	M	Specifies that for any container in the pod, all processes must run with the provided user ID.
containerSecurityContext.capabilities.add	List of Strings	Valid Linux capabilities	drop: -all	M	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.
containerSecurityContext.capabilities.drop	List of Strings	Valid Linux capabilities	drop: -all	M	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.
nrfProfiles.nfType	string		NRF	M	nfType must be NRF.
nrfProfiles.nfSetIdList	string	SetIds that NRF belongs to.	["setscpl1.scpset.5gc.mnc012.mcc345"]	C	Indicates NFSet IDs to which NRF belongs.
nrfProfiles.capacity	integer	0 to 65535	10000	O	This field specifies the capacity of NRF. This parameter is considered within a set of NRF instances or NRF service instances.
nrfProfiles.locality	string	This is operator defined information about the location of NRF.	N/A	M	This field is used to denote whether the NRF is local for SCP or unknown for SCP. If NRF Locality is within the Serving or Mate Locality of SCP, it is considered as local. Otherwise, it is considered as unknown. Producer NF profiles learnt from local NRF has all existing routing support. NF profiles learnt from unknown NRF only supports routing through another unknown SCP when the "3gpp-sbi-target-apiroot" header is present, which is called as interSCP routing or default routing. **Note**: This value is case-sensitive.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
nrfProfiles.nfInstanceId	string	String uniquely identifying a NF instance. The format of the NF Instance ID shall be a Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [15].	N/A	M	String uniquely identifying the NRF instance. The format of the instance ID is a Universally Unique Identifier (UUID) version 4 as described in IETF RFC 4122. Example: 6faf1bbc-6e4a-2828-a507-a14ef8e1bc5a
nrfProfiles.priority	integer	0 to 65535	0	O	This field specifies the priority of NRF. Lower value means higher priority. For example, primary NRF can be indicated as priority = 0 and secondary NRF as priority = 1. Similarly, further levels of NRF priority can be indicated. This parameter is considered within a set of NRF instances or NRF service instances.
nrfProfiles.interPlmnFqdn	string	NA	nrf.5gc.mnc<MNC>.mcc<MCC>.3gppnetwork.org	O	SCP selects NRF that matches the "3gpp-Sbi-target-apiRoot" header in the received Discovery Request from V-PLMN in roaming scenarios.
nrfProfiles.plmnList.mcc	string	Must be of three digits ranging from 0 to 9	"213"	O	Indicates the mobile country code required for PLMN IDs supported by NRF. This is the PLMN list served by the NRF. It is used in roaming scenarios to forward NRF-oriented requests to the NRF that supports the PLMN list.
nrfProfiles.plmnList.mnc	string	Can be of two or three digits ranging from 0 to 9	"313"	O	Indicates the mobile network code required for PLMN IDs supported by NRF. This is the PLMN list served by the NRF. It is used in roaming scenarios to forward NRF-oriented requests to the NRF that supports the PLMN list.
nrfProfiles.snpnList.mcc	string	Must be of three digits ranging from 0 to 9	"345"	O	Indicates the mobile country code required for Standalone Non Public Network (SNPN) supported by NRF.
nrfProfiles.snpnList.mnc	string	Can be of two or three digits ranging from 0 to 9	"445"	O	Indicates the mobile network code required for Standalone Non Public Network (SNPN) supported by NRF.
nrfProfiles.snpnList.nid	string	NA	000007ed9d5	O	Indicates the network identifier required for Standalone Non Public Network (SNPN) supported by NRF.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
nrfProfiles.customInfo.preferredNrfForOnDemandDiscovery	boolean	true or false	true	M	Specifies the NRF preferred by scp-nrfproxy for delegated discovery. **Note**: This parameter must be set only for one NRF instance.
nrfProfiles.customInfo.preferredNrfForOauth	boolean	true or false	true	M	Indicates the NRF to be used for NRF oAuth2 requests. This parameter can be present only in one of the NRF profiles. It is used to populate the NRF configuration table for nnrf-oauth using the NRF profile containing this parameter from the deployment file.
nrfProfiles.nfServices.serviceName	string	NA	NA	O	Supported values for serviceName: nnrf-nfm and nnrf-disc
nrfProfiles.nfServices.fqdn	string	fqdn: Labels can be letter a-z, number 0-9, hyphen(-). Hyphen cannot be first character. Label combined with dot(.) forms domain.	NA	O	FQDN of the NRF service mentioned in nrfProfiles.nfServices.serviceName.
nrfProfiles.nfServices.port	integer	port: 0 to 65535	80	O	Port number of the NF service.
nrfProfiles.nfServices.apiPrefix	string	apiPrefix: Can be combination of letters from a-z and A-Z	NA	O	Can be a combination of letters from a-z and A-Z
nrfProfiles.nfServices.scheme	string	http or https	http	O	HTTP scheme used by SCP to interact with NRF. **Note**: This value is case-sensitive.
nrfProfiles.nfServices.priority	integer	0 to 65535	0	O	Mention the priority of the service.
nrfProfiles.nfServices.capacity	integer	0 to 65535	100	O	Mention the capacity of the service.
nrfProfiles.nfServices.load	integer	0 to 100	0	O	Mention the load of the service.
nrfProfiles.nfServices.nfServiceStatus	string	REGISTERED or SUSPENDED (TS 29.510)	REGISTERED	O	Mention the status of the NRF service.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`nrfProfiles.nfServices.ipEndPoints`	list of IP address and port	[{"ipv4Address": <IpV4 Address>, "port": <integer>}] or [{"ipv6Address": <IpV6 Address>, "port": <integer>}] or [{"ipv4Address": <IpV4 Address>, "port": <integer>}, {"ipv6Address": <IpV6 Address>, "port": <integer>}]	NA	O	List of IPv4 Address or IPv6 Address, or both IPv4 and IPv6 Addresses transport and port combination of the given NRF.
`nrfProfiles.nfServices.apiPrefix`	integer	Can be combination of letters from a-z and A-Z	NA	O	API Prefix.
`nrfProfiles.nfServices.versions.apiFullVersion`	string	NA	NA	O	API Prefix of the NRF Service identified by nrfProfiles.nfServices.serviceName.
`nrfProfiles.nfServices.versions.apiVersionInUri`	string	NA	NA	O	API version of the URI of the NRF Service identified by nrfProfiles.nfServices.serviceName.
`nrfProfiles.nfServices.serviceInstanceId`	string	String uniquely identifying a NF service instance. The format of the NF Service Instance ID is Universally Unique Identifier (UUID) version 4, as described in IETF RFC 4122 [15].	f86b54b7-aef9-4c78-b346-3bfb7f380812	O	This is service InstanceID of the NRF service referred by nrfProfiles.nfServices.serviceName. **Note**: • nfServices are completely optional. One or all services can be removed. For removing all services, you must remove the nfServices key. • The nfServices block from `ocscp_values.yaml` can be removed if you want to configure any of these services. You must provide this configuration while deploying it through Helm using the `custom ocscp_values.yaml` file.
`tracingEnable`	&scpworkerTracingEnabled true	true or false	true	O	Option to enable or disable Jaeger tracing. The reference variable `&scpworkerTracingEnabled` should not be changed, however, the value `true/false` can be changed.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`enableTraceBody`	&scpworkerJaegerBodyEnabled false	true or false	false	O	Option to enable or disable tracing for full body of all Request or Response messages. The configuration is added only if tracingenable is configured as `true`. The reference variable `&scpworkerJaegerBodyEnabled` should not be changed, however, the value `true/false` can be changed.
`releaseVersion`	list	rel16	rel16	M	Enables Release 16 while deploying SCP. For information about Release 16, see 3GPP TS 23.501.
`scpMetricVersion`	string	-	• Default value for CNE: v1 • Default value for OCI: v2	M	This parameter defines the metric version. If v2 is used, some of the dimensions are clubbed together to keep the dimension count below 20. This must be used for OCI deployments. If v1 is used, no change in metric dimension from prior releases and the dimension count can go beyond 20 dimensions. This is used for CNE deployments.
`dnsSRVAlternateRouting`	boolean	true or false	false	M	Enables or disables the Alternate Routing based on the DNS SRV Records feature. **Note**: You must perform the Helm install while enabling or disabling this feature.
`nrfProxyService`	boolean	true or false	false	M	Enables or disables the scp-nrfproxy microservice. **Note**: This parameter is applicable only for SCP Release 16 deployment.
`mediationService`	boolean	true or false	false	M	Enables or disables Mediation.
`nrfProxyOauthService`	boolean	true or false	false	M	Enables or disables the nrfproxy-oauth service.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`userNamespacesEnabled`	boolean	true or false	false	O	Enables or disables the Kubernetes User Namespaces feature. When this parameter is enabled, it sets `spec.hostUsers: false` for pods and maps container user and group IDs (UIDs or GIDs) to distinct and unprivileged IDs on the host to improve isolation. Use this configuration if the following prerequisites are met: • Kubernetes version 1.33 or later • Container runtime version 2.0 or later • CRI-O version 1.25 or later **Note**: The CNE Kernel version must be 5.19 or later. For more information about the Kubernetes User Namespaces feature and `spec.hostUsers`, see https://kubernetes.io/docs/home/.
`dnsSrvSchemeConfig.defaultScheme`	string	https or http	https	O	This is the default scheme to be used to create Domain Name System (DNS) Service (SRV) Service Proto Name (SPN) for NF profile level FQDN. The same configuration is used to derive the scheme to perform DNS SRV alternate route of notification messages when NFService is unknown and nativeEgressHttpsSupport is set to true.
`dnsSrvSchemeConfig.exceptionList`	List<String>	Valid NF Types	""	O	The list of NF types that must use non-default scheme for SPN creation. For example, if the default scheme is HTTPS, then the non-default will be HTTP, and vice versa.
`serviceIpFamilyPolicy.scpcAudit`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpcAudit service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpcConfiguration`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpcConfiguration service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`serviceIpFamilyPolicy.scpcSubscription`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpcSubscription service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpcNotification`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpcNotification service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpcAlternateResolution`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpcAlternateResolution service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpCache`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpCache service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpNrfProxyOauth`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpNrfProxyOauth service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpNrfproxy`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpNrfproxy service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpWorker`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpWorker service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpMediation`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpMediation service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`serviceIpFamilyPolicy.scpMediationTest`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpMediationTest service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilyPolicy.scpcLoadManager`	<string>	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	M	ipFamilyPolicy to be allocated to scpcLoadManager service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilies.scpcAudit`	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpcAudit service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilies.scpcConfiguration`	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpcConfiguration service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilies.scpcSubscription`	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpcSubscription service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilies.scpcNotification`	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpcNotification service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilies.scpcAlternateResolution`	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpcAlternateResolution service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.
`serviceIpFamilies.scpCache`	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpCache service. For supported combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy`, see Table 3-2.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
serviceIpFamilies.scpNrfProxyOauth	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpNrfProxyOauth service. For supported combinations of serviceIpFamilies and serviceIpFamilyPolicy, see Table 3-2.
serviceIpFamilies.scpNrfproxy	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpNrfproxy service. For supported combinations of serviceIpFamilies and serviceIpFamilyPolicy, see Table 3-2.
serviceIpFamilies.scpWorker	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpWorker service. For supported combinations of serviceIpFamilies and serviceIpFamilyPolicy, see Table 3-2.
serviceIpFamilies.scpMediation	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpMediation service. For supported combinations of serviceIpFamilies and serviceIpFamilyPolicy, see Table 3-2.
serviceIpFamilies.scpMediationTest	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpMediationTest service. For supported combinations of serviceIpFamilies and serviceIpFamilyPolicy, see Table 3-2.
serviceIpFamilies.scpcLoadManager	List<String>	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	M	ipFamilies to be allocated to scpcLoadManager service. For supported combinations of serviceIpFamilies and serviceIpFamilyPolicy, see Table 3-2.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
scpPreferEgressTrafficOnIPv6	Boolean	true or false	false	C	This parameter is used to prefer IPv6 for egress connections when both IPv4 and IPv6 addresses are available. This value is set to true when: • ipFamilyPolicy is PreferDualStack or RequireDualStack. • SCP uses IPv6 address for egress traffic. **Note:** • In the absence of IPv6, routing occurs through IPv4. • The above mentioned configuration is not applicable for egress connections where IP address is obtained from NF Profile.
scpPreferInternalTrafficOnIPv6	<boolean>	true or false	false	C	This parameter is used to prefer IPv6 communication within internal SCP services when both IPv4 and IPv6 addresses are available. The value should be set to true in the following conditions: • when ipFamilyPolicy is PreferDualStack or RequireDualStack. • when you want SCP to use IPv6 address for egress traffic. **Note:** In the absence of IPv6 address, IPv4 routing happens.
containerPortNames.scp-worker.http	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	http2-5gsig	O	Defines the containerPort name of the SCP-Worker pod for HTTP communication. The same container port name should be used in backendPortName of annotations defined for Cloud Native Load Balancer (CNLB) enabled deployment on SCP-Worker.
containerPortNames.scp-worker.https	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	https-5gsig	O	Defines the containerPort name of the SCP-Worker pod for HTTPs communication. The same container port name should be used in backendPortName of annotations defined for CNLB enabled deployment on SCP-Worker.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
containerPortNames.scp-cache.coherence	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	coherence-fed	O	Defines the containerPort name of the SCP-Cache pod for coherence communication. The same container port name should be used in backendPortName of annotations defined for CNLB enabled deployment on SCP-Cache.
containerPortNames.scp-config.http	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	http2-config	O	Defines the containerPort name of the SCPC-Configuration pod for establishing communication with the CNC Console. The same container port name should be used in backendPortName of annotations defined for CNLB enabled deployment on SCPC-Configuration.
cnlbInfo.cnlbEnable	boolean	true or false	false	C	Enables or disables the CNLB feature if SCP is deployed on CNE that has the CNLB feature enabled. **Note:** For the changes to take effect in SCP after updating the value of this parameter, you must do a Helm upgrade to the currently deployed release. It restarts SCPC-Configuration.
cnlbInfo.cnlbIPv4	List of <IPv4 Address>	Valid IPv4 address	NA	C	Provides the list of IPv4 addresses through which SCP can be discovered by other NFs in the network. CNLB exposes its IPv4 addresses to consumer NFs to establish communication. **Note:** For the changes to take effect in SCP after updating the value of this parameter, you must do a Helm upgrade to the currently deployed release. It restarts SCPC-Configuration.
cnlbInfo.cnlbIPv6	List of <IPv6 Address>	Valid IPv6 address	NA	C	Provides the list of IPv6 addresses through which SCP can be discovered by other NFs in the network. CNLB exposes its IPv6 addresses to consumer NFs to establish communication. **Note:** For the changes to take effect in SCP after updating the value of this parameter, you must do a Helm upgrade to the currently deployed release. It restarts SCPC-Configuration.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`xfccHeaderDecode.certExtractIndex`	integer	0//right most,-1// left most, 2-3rd from right most	0	M	Parameters that control XFCC header extraction by specifying indexes and field names. If there are no additional hops adding XFCC header between consumer and SCP Worker, the default extraction index value of 0 is used for both certificate and field. In case there are additional hops adding XFCC header between consumer and SCP Worker, extraction index value of -1 is used for both certificate and field. Indicates certificate extraction index. **Note:** From SCP 22.3.0, the xfccHeaderDecode block, which is used for configuring decoding of the xfcc header, cannot be used from the deployment file. You can use the new SCP Consumer NF Info Configuration REST API parameter to configure this information. For more information about this parameter, see *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*. This block will be removed in the next release.
`xfccHeaderDecode.extractField`	string		DNS	M	Parameters that control XFCC header extraction by specifying indexes and field names. Indicates the field name to extract. **Note:** From SCP 22.3.0, the xfccHeaderDecode block, which is used for configuring decoding of the xfcc header, cannot be used from the deployment file. You can use the new SCP Consumer NF Info Configuration REST API parameter to configure this information. For more information about this parameter, see *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*. This block will be removed in the next release.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`xfccHeaderDecode.extractIndex`	integer	0//right most,-1// left most, 2-3rd from right most	0	M	Parameters that control XFCC header extraction by specifying indexes and field names. Indicates the index from which the field is extracted. **Note:** From SCP 22.3.0, the xfccHeaderDecode block, which is used for configuring decoding of the xfcc header, cannot be used from the deployment file. You can use the new SCP Consumer NF Info Configuration REST API parameter to configure this information. For more information about this parameter, see *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*. This block will be removed in the next release.
`istioSidecarQuitUrl`	&sidecarQuitUrl "http://127.0.0.1:15000/quitquitquit"		"http://127.0.0.1:15000/quitquitquit"	M	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://127.0.0.1:15000/quitquitquit"` can be changed. Applicable only when `serviceMeshEnabled` is set to `true`.
`istioSidecarReadyUrl`	&sidecarReadyUrl "http://127.0.0.1:15000/ready"		"http://127.0.0.1:15000/ready"	M	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://127.0.0.1:15000/ready"` can be changed. Applicable only when `serviceMeshEnabled` is set to `true`.
`serviceSpecifications.port.coherenceMgmtSvcPort`	integer	Min-1024, Max-65535	9000	M	The service port to access the Coherence cluster status using the rest based URI.
`serviceSpecifications.port.coherenceMsgPort1`	integer	Min- 1024, Max-65535	8095	M	The Coherence communication port start range.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
serviceSpecifications.port.coherenceMsgPort2	integer	Min- 1024, Max-65535	8096	M	The Coherence communication port end range.
serviceSpecifications.port.publicSignalingPort	integer	Min- 0, Max-65535	8000	M	An option to configure signaling ports.
serviceSpecifications.port.publicSignalingPortHttps	integer	Min- 0, Max-65535	443	O	Signaling port to be used for HTTPS connections. To be enabled if user wants to use HTTPS. If enabled, security certificates must be configured in the appropriate sections to enable communication over HTTPS.
serviceSpecifications.workerServices.name	string	NA	scp-worker	M	The name of the scp-worker service. **Note**: The default service name, scp-worker, cannot be modified. However, you can edit or modify only the newly added service names.
serviceSpecifications.workerServices.networkNameEnabled	boolean	true/false	false	O	An option to enable or disable metalLB IP allocation from the pool for Signaling interfaces.
serviceSpecifications.workerServices.networkName	boolean	true/false	false	C	An annotation that notifies metalLB to allocate an IP address for the Signaling interface of SCP. The annotation is added when `networkNameEnabled` is set to `true`.
serviceSpecifications.workerServices.publicSignalingIPSpecified	boolean	true/false	false	M	Regulates the value of `serviceSpecifications.workerServices.publicConfigIP`. If this parameter is set to `true`, then the value provided for `serviceSpecifications.workerServices.publicConfigIP` is considered. **Note:** This configuration is applicable for SERVICE 2.
serviceSpecifications.workerServices.publicSignalingIP	string	valid IP address	NA	O	Public configured IP address of the scp-worker service. **Note:** This configuration is applicable for SERVICE 2.
serviceSpecifications.workerServices.publicSignalingIPv6Specified	<boolean>	true or false	false	O	Enables or disables Loadbalancer IPv6 configuration statically for Signaling interfaces. **Note:** This configuration is applicable for SERVICE 2.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`serviceSpecifications.workerServices.publicSignalingIPv6`	<IPv6 Address>	Valid IPv6 address	NA	C	Configures static signaling Loadbalancer IP. The configured value is used if publicSignalingIPv6Specified is configured as true. **Note:** This configuration is applicable for SERVICE 2.
`serviceSpecifications.workerServices.ipFamilyPolicy`	*workerIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	SingleStack	C	ipFamilyPolicy to be allocated to scpWorker service. This value depends on global.serviceIpFamilyPolicy.scpWorker. **Note:** This configuration is applicable for SERVICE 2.
`serviceSpecifications.workerServices.ipFamilies`	*workerIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	[IPv4]	C	ipFamilies to be allocated to scpWorker service. This value depends on global.serviceIpFamilies.scpWorker. **Note:** This configuration is applicable for SERVICE 2.
`serviceSpecifications.workerServices.port.staticNodePortEnabled`	boolean	true/false	false	M	Regulates the value of `serviceSpecifications.workerServices.port.nodePort`. If this parameter is set to `true`, then the value provided for `serviceSpecifications.workerServices.port.nodePort` is considered.
`serviceSpecifications.workerServices.port.nodePort`	string	30000-32768	NA	O	The static node port of the scp-worker service.

`serviceSpecifications.workerServices.customExtension.labels`	string	K8s label object syntax	customExtension: labels: {} annotations: {}	O	An optional field to configure service specific labels applicable to the "Service" resource type.
					Format is:
					
					`<string_label_1_key>: <string_label_1_value>`
					`<string_label_2_key>: <string_label_2_value>`

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description

`serviceSpecifications.workerServices.customExtension.annotations`	string	K8s annotations object syntax	customExtension: labels: {} annotations: {}	O	An optional field to configure service specific annotations applicable to the "Service" resource type.
					Format is:
					
					`<string_annotation_1_key>:`
					
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					
					`<string_annotation_2_value>`

`serviceSpecifications.scpSubscriptionInfo.ip`	string	Valid IP address obtained from the metalLB pool	NA	O	Used for constructing callbackUri for NF profile notification from NRF. metallb or primaryIp, this ip is obtained from metallb pool. You can provide either IPv4 or IPv6 address. **Note**: If a specific IP of SCP is required to be conveyed as part of the subscription payload in the SCP's subscription request to NRF, NRF will route the NF profile notifications to this specified IP. Ensure that the same IP is configured as `publicSignalingIP` with the corresponding `publicSignalingIPSpecified` or `publicSignalingIPv6Specified` parameter set to true. If this configuration is not done, then SCP will not process the NF profile notifications from NRF and result in a 508 loop detection error.
`serviceSpecifications.scpSubscriptionInfo.scheme`	string	http	http	O	The preferable scp-worker scheme for callback notifications.
`serviceSpecifications.scpSubscriptionInfo.fqdn`	string	NA	<scprel>-scp-worker.scpsvc.svc.cluster.local	O	An option to configure FQDN for callback URI creation.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
scpSoothsayerConfig.systemOptions.trafficPolicy.connectionPool.http.idleTimeout	integer	NA	600s	O	HTTP idle timeout for upstream connections. Only HTTP IdleTimeout is configured. idleTimeout must be set to a value that is less than kube-proxy timeout value so that before kube-proxy silently discards connection, the connection gets terminated gracefully by HTTP.
scpSoothsayerConfig.systemOptions.trafficPolicy.connectionPool.tcp.connectTimeout	integer	NA	250ms	O	TCP keep alive settings for upstream connections.
scpSoothsayerConfig.systemOptions.trafficPolicy.connectionPool.tcp.tcpKeepalive.probes	integer	Maximum number of keepalive probes to send without response before deciding the connection is dead.Min value: 1, Max value: 16 minutes	9 minutes	O	Sets the `tcpKeepalive` parameter to enable TCP Keepalives. `tcpKeepalive.probes` - Maximum number of keepalive probes to send without response before deciding the connection is dead.
scpSoothsayerConfig.systemOptions.trafficPolicy.connectionPool.tcp.tcpKeepalive.time	integer	The time duration that a connection must be idle before keep-alive probes start being sent. Min value: 1 sec, Max value: 7200 sec	180s	O	The time duration that a connection must be idle before keep-alive probes start is sent.
scpSoothsayerConfig.systemOptions.trafficPolicy.connectionPool.tcp.tcpKeepalive.interval	integer	The time duration between keep-alive probes. Min value: 1 sec, Max value: 120 sec	1s	O	The time duration between keep-alive probes.
scpSoothsayerConfig.nrfServiceForAudit	string	nnrf-nfm/nnrf-disc	nnrf-nfm	O	Configures the NRF Service type service to retrieve profiles from NRF. Possible values are: • nnrf-nfm • nnrf-disc You must configure one of the above mentioned values, which is used by Audit to query to NRF for fetching profiles.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
scpSoothsayerConfig.reverseProxyEnabled	boolean	true/false	true	M	If it is enabled, then all the NFs, which support reverseProxy, Reverse proxy (reverseProxySupport = true), get enabled by default. In case you want to disable after deployment, then use the APIs provided to reconfigure the reverseProxySupport option. **Note**: This parameter is not supported and will be removed in the future release.
ddSslConfiguration	string	NA	NA	O	This parameter is used to configure SSL or TLS certificate for the Traffic Feed feature. Certification Authority (CA) and Truststore password information is required to generate TrustStore to connect to Oracle Communications Network Analytics Data Director (OCNADD). For more information about OCNADD, see *Oracle Communications Network Analytics Data Director User Guide*. You must create secret with CA and TrustStore password files and provide these details in the deployment file. The storeType field indicates the type of truststore (jks and p12 supported).
ddSslConfiguration.sslEnabledProtocol	string	TLSv1.3, TLSv1.2	TLSv1.3	O	Indicates the TLS version to be used for SSL connection.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
ddSslConfiguration.cipherSuitesTlsV1_2	string	• 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_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	• 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_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	O	Indicates the cipher suites available for TLSv1.2 connections.
ddSslConfiguration.cipherSuitesTlsV1_3	string	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256	O	Indicates the cipher suites available for TLSv1.3 connections.
ddSslConfiguration.k8NameSpace	string	NA	scpsvc	O	Indicates the namespace of the Kubernetes secret.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`ddSslConfiguration.primary.k8SecretName`	string	NA	primary-ocscpdd-secret	O	Secret must be created for truststore password, certificate, privateKey, and keystore password which is required for TrafficFeed SSL connection and details to be provided: • Name of secret that contains truststore password information **Note**: A valid Truststore password file name and secret should be provided to establish TrafficFeed SSL connection
`ddSslConfiguration.primary.trustStorePassword.fileName`	string	NA	ddtrust.txt	O	Secret must be created for truststore password, certificate, privateKey, and keystore password which is required for TrafficFeed SSL connection and details to be provided: • File name that has password for truststore **Note**: A valid Truststore password file name and secret should be provided to establish TrafficFeed SSL connection
`ddSslConfiguration.primary.caBundle.k8SecretName`	string	NA	primary-ocscpdd-secret	O	Secret must be created for caBundle, which is used to generate the truststore required for the SSL connection with TrafficFeed, and details to be provided: • Name of secret that contains caBundle data **Note**: A valid caBundle file name and secret should be provided to establish TrafficFeed SSL connection.
`ddSslConfiguration.primary.caBundle.fileName`	string	NA	certificate.crt	O	Secret must be created for caBundle, which is used to generate the truststore required for the SSL connection with TrafficFeed, and details to be provided: • File name of caBundle **Note**: A valid caBundle file name and secret should be provided to establish TrafficFeed SSL connection.
`ddSslConfiguration.primary.trustStoreType`	string	NA	p12	O	This parameter indicates the TrustStore type, JKS or PKCS12.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
ddSslConfiguration.primary.certificate.rsa	string	NA	dd_certificate.cer	O	Primary TLS certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • rsa certificate file name **Note**: A valid certificate file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.primary.certificate.ecdsa	string	NA	dd_ssl_ecdsa_certificate.crt	O	Primary TLS certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • ecdsa certificate file name **Note**: A valid certificate file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.primary.certificate.ecdsa	string	NA	dd_rsa_private_key_pkcs1.pem	O	Primary PrivateKey should be created for certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • rsa private key file name **Note**: A valid privateKey file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.primary.privateKey.ecdsa	string	NA	dd_ssl_ecdsa_private_key.pem	O	Primary PrivateKey should be created for certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • ecdsa private key file name **Note**: A valid privateKey file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.primary.keyStorePassword.fileName	string	NA	ddkey.txt	O	Primary keyStore password required for TrafficFeed SSL connection and details should be provided: • File name that has password for keystore **Note**: A valid keystore password file name and secret must be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.primary.keyStoreType	string	NA	p12	O	This parameter indicates the Keystore type, JKS or PKCS12.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
ddSslConfiguration.secondary.k8SecretName	string	NA	secondary-ocscpdd-secret	O	Secret must be created for truststore password, certificate, privateKey, and keystore password which is required for TrafficFeed SSL connection and details to be provided: • Name of secret that contains truststore password information **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid Truststore password file name and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.secondary.trustStorePassword.fileName	string	NA	ddtrust.txt	O	Secret must be created for truststore password, certificate, privateKey, and keystore password which is required for TrafficFeed SSL connection and details to be provided: • File name that has password for truststore **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid Truststore password file name and secret should be provided to establish TrafficFeed SSL connection
ddSslConfiguration.secondary.caBundle.k8SecretName	string	NA	secondary-ocscpdd-secret	O	Secret must be created for caBundle, which is used to generate the truststore required for the SSL connection with TrafficFeed, and details to be provided: • Name of secret that contains caBundle data **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid caBundle file name and secret should be provided to establish TrafficFeed SSL connection.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
ddSslConfiguration.secondary.caBundle.fileName	string	NA	certificate.crt	O	Secret must be created for caBundle, which is used to generate the truststore required for the SSL connection with TrafficFeed, and details to be provided: • File name of caBundle **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid caBundle file name and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.secondary.trustStoreType	string	NA	p12	O	This parameter indicates the TrustStore type, JKS or PKCS12. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates.
ddSslConfiguration.secondary.certificate.rsa	string	NA	dd_certificate.cer	O	Secondary TLS certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • rsa certificate file name **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid certificate file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.secondary.certificate.ecdsa	string	NA	dd_ssl_ecdsa_certificate.crt	O	Secondary TLS certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • ecdsa certificate file name **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid certificate file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
ddSslConfiguration.secondary.privateKey.rsa	string	NA	dd_rsa_private_key_pkcs1.pem	O	Secondary PrivateKey should be created for certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • rsa private key file name **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid privateKey file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.secondary.privateKey.ecdsa	string	NA	dd_ssl_ecdsa_private_key.pem	O	Secondary PrivateKey should be created for certificate used for keyStore required for TrafficFeed SSL connection and details should be provided: • ecdsa private key file name **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid privateKey file name for RSA or ECDSA and secret should be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.secondary.keyStorePassword.fileName	string	NA	ddkey.txt	O	Secondary keyStore password required for TrafficFeed SSL connection and details should be provided: • File name that has password for keystore **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid keystore password file name and secret must be provided to establish TrafficFeed SSL connection.
ddSslConfiguration.secondary.keyStoreType	string	NA	p12	O	This parameter indicates the Keystore type, JKS or PKCS12. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates.
ddSslConfiguration.initialAlgorithm	string	NA	RS256	O	This parameter indicates the SSL Algorithm.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
ddSaslConfiguration.userName.fileName	string	NA	userName.txt	O	This parameter is used to configure SSL for TrafficFeed feature. Password information is used by SCP to connect to OCNADD with SASL as security mechanism. You must create secret with userName files and provide details in deployment file. **Note:** A valid username and password file name and secret must be provided to establish TrafficFeed SASL connection.
ddSaslConfiguration.userName.k8SecretName	string	NA	ocscpddsasl-secret	O	This parameter is used to configure SSL for TrafficFeed feature. UserName information is used by SCP to connect to OCNADD with SASL as security mechanism. You must create secret with userName files and provide details in deployment file. **Note**: A valid username and password file name and secret must be provided to establish TrafficFeed SASL connection.
ddSaslConfiguration.password.fileName	string	NA	password.txt	O	This parameter is used to configure SSL for TrafficFeed feature. Password information is used by SCP to connect to OCNADD with SASL as security mechanism. You must create secret with password files and provide details in deployment file. **Note**: A valid username and password file name and secret must be provided to establish TrafficFeed SASL connection.
ddSaslConfiguration.password.k8SecretName	string	NA	ocscpddsasl-secret	O	This parameter is used to configure SSL for TrafficFeed feature. Password information is used by SCP to connect to OCNADD with SASL as security mechanism. You must create secret with password files and provide details in deployment file. **Note**: A valid username and password file name and secret must be provided to establish TrafficFeed SASL connection.
sbiProxySslConfigurations.server.tlsVersion	string	The allowed values are: • TLSv1.3,TLSv1.2 • TLSv1.3 • TLSv1.2	TLSv1.3,TLSv1.2	O	Indicates the version of Transport Layer Security (TLS).

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.k8NameSpace	string	NA	scpsvc	O	Indicates Kubernetes namespace.
sbiProxySslConfigurations.server.cipherSuitesTlsV1_2	string	• 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_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	• 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_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	O	Indicates the cipher suites available for TLSv1.2 connections.
sbiProxySslConfigurations.server.cipherSuitesTlsV1_3	string	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256	O	Indicates the cipher suites available for TLSv1.3 connections.
sbiProxySslConfigurations.server.primary.secretName	string	NA	server-primary-ocscp-secret	O	Indicates the name of Kubernetes secret. **Note**: A valid Truststore password file name and secret should be provided to establish server side SSL connection.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
`sbiProxySslConfigurations.server.primary.privateKey.rsa`	string	NA	server_rsa_private_key_pkcs1.pem	O	Indicates the RSA private key file name. **Note**: A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.
`sbiProxySslConfigurations.server.primary.privateKey.ecdsa`	string	NA	ssl_ecdsa_private_key.pem	O	Indicates the ecdsa private key file name. **Note**: A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.
`sbiProxySslConfigurations.server.primary.certificate.rsa`	string	NA	server_ocscp.cer	O	Indicates the RSA certificate file name. **Note**: A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.
`sbiProxySslConfigurations.server.primary.certificate.ecdsa`	string	NA	ssl_ecdsa_certificate.crt	O	Indicates the ecdsa certificate file name. **Note**: A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.
`sbiProxySslConfigurations.server.primary.caBundle.k8SecretName`	string	NA	server-primary-ocscp-secret	O	Indicates the name of Kubernetes secret that contains caBundle data. **Note**: A valid caBundle file name and secret should be provided to establish server side SSL connection.
`sbiProxySslConfigurations.server.primary.caBundle.fileName`	string	NA	server_caroot.cer	O	Indicates the file name of caBundle. **Note**: • A valid caBundle file name and secret should be provided to establish server side SSL connection. • For HTTPS communication, you can use multiple intermediate and root CA certificates by combining them into a single CA bundle file. This combined CA bundle can be configured under the `sbiProxySslConfigurations` Helm parameter.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.server.primary.keyStorePassword.fileName	string	NA	key.txt	O	Indicates the file name that has password for keystore. **Note**: A valid keyStore password file name and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.primary.trustStorePassword.fileName	string	NA	trust.txt	O	Indicates the file name that has password for truststore. **Note**: A valid Truststore password file name and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.secondary.secretName	string	NA	server-secondary-ocscp-secret	O	Indicates the name of Kubernetes secret. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid Truststore password file name and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.secondary.privateKey.rsa	string	NA	2nd_server_rsa_private_key_pkcs1.pem	O	Indicates the RSA private key file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.secondary.privateKey.ecdsa	string	NA	ssl_ecdsa_private_key.pem	O	Indicates the ecdsa private key file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.server.secondary.certificate.rsa	string	NA	2nd_server_ocscp.cer	O	Indicates the RSA certificate file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.secondary.certificate.ecdsatlsVersion	string	NA	ssl_ecdsa_certificate.crt	O	Indicates the ecdsa certificate file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.secondary.caBundle.k8SecretName	string	NA	server-secondary-ocscp-secret	O	Indicates the name of Kubernetes secret that contains caBundle data. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid caBundle file name and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.secondary.caBundle.fileName	string	NA	server_caroot.cer	O	Indicates the file name of caBundle. **Note**: • You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid caBundle file name and secret should be provided to establish server side SSL connection. • For HTTPS communication, you can use multiple intermediate and root CA certificates by combining them into a single CA bundle file. This combined CA bundle can be configured under the sbiProxySslConfigurations Helm parameter.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.server.secondary.keyStorePassword.fileName	string	NA	key.txt	O	Indicates the file name that has password for keystore. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid keyStore password file name and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.server.secondary.trustStorePassword.fileName	string	NA	trust.txt	O	Indicates the file name that has password for truststore. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid Truststore password file name and secret should be provided to establish server side SSL connection.
sbiProxySslConfigurations.terminateTLSConnsOnCertExpiry.client	boolean	true or false	false	O	Helm configuration for Egress (client) connections to determine whether to terminate or maintain existing HTTPS connections when the configured TLS certificate is updated or renewed. When the TLS certificate expires, SCP: • Maintains the existing HTTPS connections that were using the expired certificates. • Creates new HTTPS connections that use the updated or renewed TLS certificate.
sbiProxySslConfigurations.client.primary.nfType	string	NA	default	O	Indicates the client NF type.
sbiProxySslConfigurations.client[0].tlsVersion	string	The allowed values are: • TLSv1.3,TLSv1.2 • TLSv1.3 • TLSv1.2	TLSv1.3,TLSv1.2	O	Indicates the TLS version to be used by the client.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.client[0].cipherSuitesTlsV1_2	string	• 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_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	• 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_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	O	Indicates the cipher suites that can be used for TLSv1.2 connections.
sbiProxySslConfigurations.client[0].cipherSuitesTlsV1_3	string	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256	O	Indicates the cipher suites that can be used for TLSv1.3 connections.
sbiProxySslConfigurations.client.primary.secretName	string	NA	default-primary-ocscp-secret	O	Indicates the name of Kubernetes secret. **Note**: A valid Truststore password file name and secret should be provided to establish client side SSL connection.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.client.primary.privateKey.rsa	string	NA	client_rsa_private_key_pkcs1.pem	O	Indicates the RSA private key file name. **Note**: A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.primary.privateKey.ecdsa	string	NA	ssl_ecdsa_private_key.pem	O	Indicates the ecdsa private key file name. **Note**: A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.primary.certificate.rsa	string	NA	client_ocscp.cer	O	Indicates the RSA certificate file name. **Note**: A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.primary.certificate.ecdsa	string	NA	ssl_ecdsa_certificate.crt	O	Indicates the ecdsa certificate file name. **Note**: A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.primary.caBundle.k8SecretName	string	NA	default-primary-ocscp-secret	O	Indicates the name of Kubernetes secret that contains caBundle data. **Note**: A valid caBundle file name and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.primary.caBundle.fileName	string	NA	server_caroot.cer	O	Indicates the file name of caBundle. **Note**: • A valid caBundle file name and secret should be provided to establish client side SSL connection. • For HTTPS communication, you can use multiple intermediate and root CA certificates by combining them into a single CA bundle file. This combined CA bundle can be configured under the sbiProxySslConfigurations Helm parameter.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.client.primary.keyStorePassword.fileName	string	NA	key.txt	O	Indicates the file name that has password for keystore. **Note**: A valid keyStore password file name and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.primary.trustStorePassword.fileName	string	NA	trust.txt	O	Indicates the file name that has password for truststore. **Note**: A valid Truststore password file name and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.secondary.secretName	string	NA	default-secondary-ocscp-secret	O	Indicates the name of Kubernetes secret. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid Truststore password file name and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.secondary.privateKey.rsa	string	NA	2nd_client_rsa_private_key_pkcs1.pem	O	Indicates the RSA private key file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.secondary.privateKey.ecdsa	string	NA	ssl_ecdsa_private_key.pem	O	Indicates the ecdsa private key file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid privateKey file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.client.secondary.certificate.rsa	string	NA	2nd_client_ocscp.cer	O	Indicates the RSA certificate file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.secondary.certificate.ecdsa	string	NA	ssl_ecdsa_certificate.crt	O	Indicates the ecdsa certificate file name. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid certificate file name whether for RSA or ECDSA and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.secondary.caBundle.k8SecretName	string	NA	default-secondary-ocscp-secret	O	Indicates the name of Kubernetes secret that contains caBundle data. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid caBundle file name and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.secondary.caBundle.fileName	string	NA	caroot.cer	O	Indicates the file name of caBundle. **Note**: • You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid caBundle file name and secret should be provided to establish client side SSL connection. • For HTTPS communication, you can use multiple intermediate and root CA certificates by combining them into a single CA bundle file. This combined CA bundle can be configured under the sbiProxySslConfigurations Helm parameter.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sbiProxySslConfigurations.client.secondary.keyStorePassword.fileName	string	NA	key.txt	O	Indicates the file name that has password for keystore. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid keyStore password file name and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.client.secondary.trustStorePassword.fileName	string	NA	trust.txt	O	Indicates the file name that has password for truststore. **Note**: You can configure this parameter only if you want to enable the secondary TLS certificate to support multiple TLS certificates. A valid Truststore password file name and secret should be provided to establish client side SSL connection.
sbiProxySslConfigurations.initialAlgorithm	string	ES256 and RS256	RS256	O	Indicates SSL or TLS algorithm. The supported algorithms are: ES256 and RS256.
sbiProxySslConfigurations.client[0].nfTypeExtensionSelfValidation	boolean	true, false	false	O	You can configure this parameter to enable or disable validation of the nfType extension value in the SCP's client TLS certificate. If enabled and the nfType extension is present in the TLS certificate, SCP will verify that the value is "SCP".
k8sApiClientConfiguration.k8sApiClientDefaultConfig	boolean	true, false	true	O	Determines whether to use the default Kubernetes client or a custom configured Kubernetes client.
k8sApiClientConfiguration.tlsVersion	string	'TLSv1.3', 'TLSv1.2', 'TLSv1.3, TLSv1.2'	TLSv1.3,TLSv1.2	O	Indicates the TLS version to be used by the Kubernetes client.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
k8sApiClientConfiguration.cipherSuitesTlsV1_2	string	• 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_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	List of strings containing specific ciphers	O	Indicates the cipher suites that can be used for TLS 1.2 connections.
k8sApiClientConfiguration.cipherSuitesTlsV1_3	string	• TLS_AES_128_GCM_SHA256 • TLS_AES_256_GCM_SHA384 • TLS_CHACHA20_POLY1305_SHA256	List of strings containing specific ciphers	O	Indicates the cipher suites that can be used for TLS 1.3 connections.
sslCertExpiryCriticalThreshold	integer	Should be less than sslCertExpiryMajorThreshold and sslCertExpiryMinorThreshold	30D **Note**: The allowed dimensions are D for days, H for hours, and M for minutes, and the default value is days (D).	M	Indicates the certificate expiry threshold values for triggering Minor, Major, and Critical alerts for TLS certificate expiration.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
sslCertExpiryMajorThreshold	integer	Should be less than sslCertExpiryMinorThreshold and higher than sslCertExpiryCriticalThreshold	90D **Note**: The allowed dimensions are D for days, H for hours, and M for minutes, and the default value is days (D).	M	Indicates the certificate expiry threshold values for triggering Minor, Major, and Critical alerts for TLS certificate expiration.
sslCertExpiryMinorThreshold	integer	Should be higher than sslCertExpiryMajorThreshold and sslCertExpiryCriticalThreshold	180D **Note**: The allowed dimensions are D for days, H for hours, and M for minutes, and the default value is days (D).	M	Indicates the certificate expiry threshold values for triggering Minor, Major, and Critical alerts for TLS certificate expiration.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
enableTlsExtensionsCompliance	boolean	true,false	true	M	You can configure this parameter to enable or disable the control of certain TLS extensions. This involves disabling specific TLS extensions and setting values for the signature_algorithms, signature_algorithms_cert, and supported_groups (Named Groups) extensions. The signature_algorithms and signature_algorithms_cert extensions correspond to Signature Schemes, while supported_groups is the same as Named Groups. These controls will apply to all TLS communication in the SCP worker. If disabled, the JDK system defaults will be used. If enabled, the following settings will apply: • Disabled Extensions: session_ticket, status_request, status_request_v2, psk_key_exchange_modes, pre_shared_key, early_data, certificate_authorities, ec_point_formats • Signature Schemes: ecdsa_secp521r1_sha512, ecdsa_secp384r1_sha384, ecdsa_secp256r1_sha256, ed448, ed25519, rsa_pss_rsae_sha512, rsa_pss_rsae_sha384, rsa_pss_rsae_sha256, rsa_pss_pss_sha512, rsa_pss_pss_sha384, rsa_pss_pss_sha256, rsa_pkcs1_sha512, rsa_pkcs1_sha384, rsa_pkcs1_sha256 • Named Groups: secp521r1, secp384r1, secp256r1, x448, x25519
tlsSessionResumptionDisabled	boolean	true,false	true	M	Disables TLS session resumption when the pre_shared_key extension is disabled. This variable must be set to true when the pre_shared_key extension is disabled, and conversely.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
clientDisabledExtensions	string	-	session_ticket, status_request, status_request_v2, psk_key_exchange_modes, pre_shared_key, early_data, certificate_authorities, ec_point_formats	C	Disables the extensions in HTTPS communication while interacting with client.
serverDisabledExtensions	string	-	session_ticket, status_request, status_request_v2, psk_key_exchange_modes, pre_shared_key, early_data, ec_point_formats	C	Disables the extensions in HTTPS communication while interacting with server.
clientAllowedSignatureSchemes	string	-	ecdsa_secp521r1_sha512, ecdsa_secp384r1_sha384, ecdsa_secp256r1_sha256, ed448, ed25519, rsa_pss_rsae_sha512, rsa_pss_rsae_sha384, sa_pss_rsae_sha256, rsa_pss_pss_sha512, rsa_pss_pss_sha384, rsa_pss_pss_sha256, rsa_pkcs1_sha512, rsa_pkcs1_sha384, rsa_pkcs1_sha256	C	Lists the signature schemes allowed for the client in HTTPS communication.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
serverAllowedSignatureSchemes	string	-	ecdsa_secp521r1_sha512, ecdsa_secp384r1_sha384, ecdsa_secp256r1_sha256, ed448, ed25519, rsa_pss_rsae_sha512, rsa_pss_rsae_sha384, rsa_pss_rsae_sha256, rsa_pss_pss_sha512, rsa_pss_pss_sha384, rsa_pss_pss_sha256, rsa_pkcs1_sha512, rsa_pkcs1_sha384, rsa_pkcs1_sha256	C	Lists the signature schemes allowed for the server in HTTPS communication.
allowedNamedGroups	string	-	secp521r1,secp384r1,secp256r1,x448,x25519	C	Lists the allowed name groups in HTTPS communication.
enableDnsBasedNrfBootStrapInfoFeature	boolean	true,false	false	O	Enables or disables the nrf_bootstrap_info feature in the SCP deployment.
deRegisterScpDuringMigration	boolean	true,false	false	O	Deregisters SCP with the old or static nrfset if both NRFs in the migration from static to DNS SRV are the same.
preferredDNSSRVNrfSetIdForOnDemandDiscovery	strings	NA	setnrfl1.nrfset.5gc.mnc012.mcc345	O	Preferred DNSSRV NrfSetId to be used for on demand discovery when the nrf_bootstrap_info feature is enabled during deployment.
nrfSrvConfiguration.nrfSrvFqdn	strings	NA	nrf1svc.scpsvc.svc.cluster.local	M	NRF SRV FQDN for the corresponding NRF SRV configuration.
nrfSrvConfiguration.nfSetIdList	strings	NA	"setnrfl1.nrfset.5gc.mnc012.mcc345"	M	SetId for this NRF SRV configuration. This setId must be unique for each NRF SRV configuration; this setId must not be present in other NRF SRV configurations.
nrfSrvConfiguration.performSubscription	boolean	true/false	false	O	Allow to decide whether NRF from this NRF SRV is used for subscription or not.

Table 3-1 (Cont.) Global Parameters

Parameter Name	Data Type	Range	Default Value	M/O/C	Description
nrfSrvConfiguration.plmnList.mcc	integer	Must be of three digits ranging from 0 to 9	330	O	Indicates the mobile country code required for PLMN IDs supported by NRF used in NRF DNS SRV. This is the PLMN list served by the NRF used in the NRF DNS SRV feature. It is employed in roaming scenarios to route NRF-related requests to the NRF that supports the PLMN list.
nrfSrvConfiguration.plmnList.mnc	integer	Can be of two or three digits ranging from 0 to 9	143	O	Indicates the mobile network code required for PLMN IDs supported by NRF used in NRF DNS SRV. This is the PLMN list served by the NRF used in the NRF DNS SRV feature. It is employed in roaming scenarios to route NRF-related requests to the NRF that supports the PLMN list.
nrfSrvConfiguration.performAudit	boolean	true,false	true	O	Allows to decide whether NRF from this NRF SRV should be used for a audit or not.
nrfSrvConfiguration.registerScp	boolean	true,false	true	O	Allows to decide whether to register SCP with the NRF from the NRF Set.
nrfSrvConfiguration.scheme	string	"http","https"	http	M	Used for the URI Scheme. The supported value is http/https.
nrfSrvConfiguration.apiPrefix	string	NA	USEast	O	Used for apiPrefix.
nrfSrvConfiguration.versions	string	• apiVersionInUri: <string> • apiFullVersion: <string>	• apiVersionInUri: v1 • apiFullVersion: 1.0.0	M	Lists the NFServiceVersion. Configuring multiple API versions is permissible, but at least one entry in the version list must have its apiVersionInUri set to "v1." This is because SCP currently utilizes "v1" for its self-generated requests towards NRF. .
nrfSrvConfiguration.serviceNames	string	• nnrf-nfm • nnrf-disc • nnrf-oauth2	• nnrf-nfm • nnrf-disc • nnrf-oauth2	M	This is the name of the service. The supported value is nnrf-nfm/nnrf-disc/nnrf-oauth2.
nrfSrvConfiguration.isInterPlmnFqdn	boolean	true,false	false	O	Allows you to decide if SCP has to support inter-PLMn alternate routes or not.

The following table describes various combinations of `serviceIpFamilies` and `serviceIpFamilyPolicy` for SCP microservices:

Table 3-2 serviceIpFamilies to serviceIpFamilyPolicy Mapping

serviceIpFamilies	serviceIpFamilyPolicy		
	SingleStack	PreferDualStack	RequireDualStack
IPv4	Y	Y (*)	Y (*)
IPv6	Y	Y (**)	Y (**)
IPv4, IPv6	N	Y	Y
IPv6, IPv4	N	Y	Y

- * indicates that services will also be assigned IPv6 addresses if the deployment environment has both IPv4 and IPv6 addresses. In this case, IpFamilies are exposed in the following order:
  - IPv4
  - IPv6
- ** indicates that services will also be assigned IPv4 addresses if the deployment environment has both IPv4 and IPv6 addresses. In this case, IpFamilies are exposed in the following order:
  - IPv6
  - IPv4

3.1.2 SCPC-Configuration Parameters

The following table lists the SCPC-Configuration parameters.

Table 3-3 SCPC-Configuration Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-configuration.imageDetails.image`	string	image: 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	scpc-configuration	M	Indicates Image Tag to be used for configuration container

Table 3-3 (Cont.) SCPC-Configuration Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-configuration.imageDetails.tag`	string	Tag: 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	SCP Images	M	Indicates the Tag name of SCP configuration image.
`scpc-configuration.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scpc-configuration.resources.requests.memory`	integer	NA	2Gi	M	Indicates the requested memory (RAM) for configuration microservice in Giga Bytes.
`scpc-configuration.resources.requests.cpu`	integer	NA	2	M	Indicates the maximum allocated vCPU for configuration microservice.
`scpc-configuration.resources.requests.ephemeral-storage`	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scpc-configuration.resources.limits.memory`	integer	NA	2Gi	M	Indicates the maximum limit of memory for configuration microservice.
`scpc-configuration.resources.limits.cpu`	integer	NA	2	M	Indicates the maximum limit of CPU for configuration microservice.

Table 3-3 (Cont.) SCPC-Configuration Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-configuration.resources.limits.ephemeral-storage	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scpc-configuration.log.level	string		*configLogLevelRef	O	Enables the required level of logging for the service. **Note**: Do not modify this reference variable.
scpc-configuration.defaultTopologySource	string	(NRF,LOCAL)	NRF	O	Sets Topology Source globally for all NFs .
scpc-configuration.initializationFailTimeout	integer	NA	160000	O	initializationFailTimeout in ms - Maximum lifetime in milliseconds of a connection in the pool after it is closed.
scpc-configuration.idleTimeout	integer	NA	10000	O	idleTimeout in ms - Maximum idle time for connection.
scpc-configuration.minimumIdle	integer	NA	1	O	Indicates the minimum number of idle connections maintained by HikariCP in a connection pool.
scpc-configuration.connectionTimeout	integer	NA	20000	O	connectionTimeout in ms - Maximum number of milliseconds that a client waits for a connection
scpc-configuration.maxPoolSize	integer	NA	10	O	Indicates the maximum pool size Hikari CP can create.
scpc-configuration.maxLifetime	integer	NA	240	O	Indicates the maximum lifetime in ms of a connection in the pool after it is closed.
scpc-configuration.service.type	string	ClusterIP, LoadBalancer, NodePort,ExternalName	LoadBalancer	O	When this value is enabled, it overrides the default derivation of service type. **Note**: If Oracle Communications Cloud Native Configuration Console (CNC Console) is used, it is recommended to use ClusterIP.

Table 3-3 (Cont.) SCPC-Configuration Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-configuration.service.publicConfigIPSpecified`	boolean	true or false	false	O	Option to enable or disable Loadbalancer IP configuration statically for the OAM interface.
`scpc-configuration.service.publicConfigIP`	<IPv4 Address>	Valid IPV4 address as per RFC 791	NA	C	Option to configure static Loadbalancer IP. Configured value is used only if oamloadbalanceripenabled is configured as `true`.
`scpc-configuration.service.staticnodeportenabled`	boolean	true or false	false	O	Option to enable or disable configuring static Node Port for the OAM interface.
`scpc-configuration.service.nodeport`	integer	30000 to 32767	31612	C	Option to configure static Node Port for OAM interface. Configured value will be used only if staticnodeportenabled is configured as `true`.
`scpc-configuration.service.configServiceNetworkNameEnabled`	boolean	true or false	false	O	Option to enable or disable metalLB IP allocation dynamically from the pool for the OAM interface.
`scpc-configuration.service.configServiceNetworkName`	string	NA	metallb.universe.tf/address-pool: oam	C	Indicates the metalLB network name.

`scpc-configuration.service.customExtension.labels`	`<string_label_1_key>:`
	`<string_label_1_value>`
	`<string_label_2_key>:`
	`<string_label_2_value>`
		Kubernetes label object syntax	`customExtension:`
			`  labels: {}`
			`annotations:`
			` {}`
				O	Optional field to configure service specific labels applicable to "Service" Resource Type.

Table 3-3 (Cont.) SCPC-Configuration Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scpc-configuration.service.customExtension.annotations`	`<string_annotation_1_key>: <string_annotation_1_value>`
	
	`<string_annotation_2_key>: <string_annotation_2_value>`
		Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	Optional field to configure service specific annotations applicable to "Service" Resource Type.

`scpc-configuration.service.ipFamilyPolicy`	*configIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpcConfiguration service. This value depends on the value of global.serviceIpFamilyPolicy.scpcConfiguration.
`scpc-configuration.service.ipFamilies`	*configIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpcConfiguration service. This value depends on the value of global.serviceIpFamilies.scpcConfiguration.
`scpc-configuration.deployment.containerPortName`	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	http2-config	O	Exposes the name of the container port. In CNLB annotation, the back-end port name aligns with the container port name.

Table 3-3 (Cont.) SCPC-Configuration Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-configuration.deployment.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	Kubernetes label object syntax	customExtension: labels: {} annotations: {}	O	Configures service specific labels applicable for "Service" resource type.
scpc-configuration.deployment.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	Kubernetes annotations object syntax	customExtension: labels: {} annotations: {}	O	Configures service specific annotations applicable to "Service" resource type.
scpc-configuration.nodeSelector.nodeKey	string	nodeSelector: Use this configuration to apply nodeSelector to Configuration service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Configuration service pods.

Table 3-3 (Cont.) SCPC-Configuration Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-configuration.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scpc-configuration	O	Value of the node label.
`scpc-configuration.istioSidecarQuitUrl`	string		*sidecarQuitUrl	C	Defines the URL for quitting service mesh sidecar. This URL is used to hook job when hook is completed and quits the sidecar. Applicable only in `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.
`scpc-configuration.istioSidecarReadyUrl`	string		*sidecarReadyUrl	C	Define the URL for checking service mesh sidecar status and start the application when the status is ready. Applicable only in `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.

3.1.3 SCPC-Subscription Parameters

The following table lists the SCPC-Subscription parameters.

Table 3-4 SCPC-Subscription Parameters

Parameter Name	Data Type	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-subscription.imageDetails.image`	string	image: 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	ocscp-subscription	M	NA
`scpc-subscription.imageDetails.tag`	string	Tag: 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	SCP Images	M	Indicates Image Tag to be used for the Configuration container.
`scpc-subscription.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scpc-subscription.resources.requests.memory`	integer	NA	2Gi	M	Indicates the requested memory (RAM) for configuration microservice in Giga Bytes.
`scpc-subscription.resources.requests.cpu`	integer	NA	2	M	Indicates the maximum allocated vCPU for configuration microservice.

Table 3-4 (Cont.) SCPC-Subscription Parameters

Parameter Name	Data Type	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-subscription.resources.requests.ephemeral-storage	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scpc-subscription.resources.limits.memory	integer	NA	2Gi	M	Indicates the maximum limit of memory for configuration microservice.
scpc-subscription.resources.limits.cpu	integer	NA	2	M	Indicates the maximum limit of CPU for configuration microservice.
scpc-subscription.resources.limits.ephemeral-storage	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scpc-subscription.guardTime	integer	Min: 5 Max: 180 (in seconds)	10	O	Configures guardTime in seconds. This is the advance time before validityTimerExpiry at which subscription is initiated.
scpc-subscription.subscriptionValidityPeriod	integer	Min: 1 Max: 168 (in hours)	168	O	Parameter used to set the period after which a subscription gets expired. NRF may or may not accept honor this. Defaulted to 7 days, that is, 168 hours.
scpc-subscription.log.level	string		*subsLogLevelRef	O	Enables the required level of logging for the service. **Note**: Do not modify this reference variable.
scpToRegisterWithNrfRegionOrSetIds	string	Valid Regions or SetIds to be registered with or empty for no registration	[]	M	Sets scpToRegisterWithNrfRegions with regions to register the high priority NRFs in specified regions. Example: scpToRegisterWithNrfRegionOrSetIds: ["reg1,reg2"]. Or, it can be set in the following format: Example: scpToRegisterWithNrfRegionOrSetIds: - reg1 - reg2

Table 3-4 (Cont.) SCPC-Subscription Parameters

Parameter Name	Data Type	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-subscription.initializationFailTimeout`	integer	NA	160000	O	initializationFailTimeout in ms - Maximum lifetime in milliseconds of a connection in the pool after it is closed.
`scpc-subscription.idleTimeout`	integer	NA	10000	O	idleTimeout in ms - Maximum idle time for connection.
`scpc-subscription.minimumIdle`	integer	NA	1	O	Indicates the minimum number of idle connections maintained by HikariCP in a connection pool.
`scpc-subscription.connectionTimeout`	integer	NA	20000	O	connectionTimeout in ms - Maximum number of milliseconds that a client will wait for a connection.
`scpc-subscription.maxPoolSize`	integer	NA	10	O	Indicates the maximum pool size Hikari CP can create.
`scpc-subscription.maxLifetime`	integer	NA	240	O	Indicates the maximum lifetime in ms of a connection in the pool after it is closed.
`scpc-subscription.service.type`	string	ClusterIP, LoadBalancer, NodePort	ClusterIP	O	When this value is enabled, it overrides the default derivation of Service Type.

`scpc-subscription.service.customExtension.labels`	`<string_label_1_key>:`
	
	`<string_label_1_value>`
	
	`<string_label_2_key>:`
	
	`<string_label_2_value>`
		K8s label object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	Optional field to configure service specific labels applicable to "Service" Resource Type.

Table 3-4 (Cont.) SCPC-Subscription Parameters

Parameter Name	Data Type	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-subscription.service.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	K8s annotations object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type.
scpc-subscription.service.ipFamilyPolicy	*subsIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpcSubscription service. This value depends on the value of global.serviceIpFamilyPolicy.scpcSubscription.
scpc-subscription.service.ipFamilies	*subsIpFamilyPolicy	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpcSubscription service. This value depends on the value of global.serviceIpFamilyPolicy.scpcSubscription.
scpc-subscription.deployment.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	K8s label object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.

Table 3-4 (Cont.) SCPC-Subscription Parameters

Parameter Name	Data Type	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scpc-subscription.deployment.customExtension.annotations`	`<string_annotation_1_key>: <string_annotation_1_value>`
	
	`<string_annotation_2_key>: <string_annotation_2_value>`
		K8s annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	Optional field to configure service specific annotations applicable to "Service" Resource Type.

`scpc-subscription.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Subscription service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Subscription service pods.
`scpc-subscription.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scpc-subscription	O	Value of the node label.
`scpc-subscription.istioSidecarQuitUrl`	string		*sidecarQuitUrl	C	Defines the URL to use for quitting service mesh sidecar. This URL will be used to hook job once hook is successfully completed and quits the sidecar. Only applicable in `serviceMeshEnabled` is set to "true" **Note**: Do not modify this reference variable.

Table 3-4 (Cont.) SCPC-Subscription Parameters

Parameter Name	Data Type	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-subscription.istioSidecarReadyUrl`	string		*sidecarReadyUrl	C	Defines the URL to use for checking service mesh sidecar status and starts application once status is ready. Only applicable in `serviceMeshEnabled` is set to "true" **Note**: Do not modify this reference variable.

3.1.4 SCPC-Notification Parameters

The following table lists the SCPC-Notification parameters.

Table 3-5 SCPC-Notification Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-notification.imageDetails.image`	string	image: 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.	ocscp-notification	M	Indicates the Image name of SCP notification.

Table 3-5 (Cont.) SCPC-Notification Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-notification.imageDetails.tag`	string	Tag: 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.	SCP Images	M	Indicates the Image Tag to be used for Configuration container.
`scpc-notification.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scpc-notification.resources.requests.memory`	integer	NA	8Gi	M	Indicates the requested memory (RAM) for configuration microservice in Giga Bytes.
`scpc-notification.resources.requests.cpu`	integer	NA	8	M	Indicates the maximum allocated vCPU for configuration microservice.
`scpc-notification.resources.requests.ephemeral-storage`	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scpc-notification.resources.limits.memory`	integer	NA	8Gi	M	Indicates the maximum limit of memory for configuration microservice.
`scpc-notification.resources.limits.cpu`	integer	NA	8	M	Indicates the maximum limit of CPU for configuration microservice.

Table 3-5 (Cont.) SCPC-Notification Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-notification.resources.limits.ephemeral-storage`	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scpc-notification.log.level`	string		*notifLogLevelRef	O	Enables the required level of logging for the service. **Note**: Do not modify this reference variable.
`scpc-notification.defaultLocalityToScp`	boolean	true/false	true	O	If set to `true`, registration notification for NF coming to SCP with no locality present gets considered in SCP's locality and that NF gets treated as within serving locality.
`scpc-notification.initializationFailTimeout`	integer	NA	160000	O	initializationFailTimeout in ms - Maximum lifetime in milliseconds of a connection in the pool after it is closed.
`scpc-notification.idleTimeout`	integer	NA	10000	O	idleTimeout in ms - Maximum idle time for connection.
`scpc-notification.minimumIdle`	integer	NA	1	O	Indicates the minimum number of idle connections maintained by HikariCP in a connection pool.
`scpc-notification.connectionTimeout`	integer	NA	20000	O	connectionTimeout in ms - Maximum number of milliseconds that a client will wait for a connection.
`scpc-notification.maxPoolSize`	integer	NA	100	O	Indicates the maximum pool size Hikari CP can create.
`scpc-notification.maxLifetime`	integer	NA	240	O	Indicates the maximum lifetime in ms of a connection in the pool after it is closed.
`scpc-notification.mergeNFServices.status`	boolean	true/false	false	M	Option to enable and disable merge NFServices within an NF Profile. **Note:** This parameter is supported only in the Release 15 deployment model, which is not supported from SCP 24.3.0.

Table 3-5 (Cont.) SCPC-Notification Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-notification.mergeNFServices.supportedNFServices`	List of strings. (example in description)	Valid 5G NF Services as per 3GPP TS 29.510. []i.e. Blank, which means consider all supported NF Services. If not provided, all supported NF Services are considered.	nudm-uecm, nudm-sdm	C	List of NFService's for which merge nf services within an NF Profile is triggered. Format Example: supportedNFServices: - nudm-uecm - nudm-sdm **Note**: This list is considered only if above status flag is enabled.
`scpc-notification.service.type`	string	ClusterIP, LoadBalancer , NodePort .	ClusterIP	O	When this value is enabled, it overrides the default derivation of Service Type.

`scpc-notification.service.customExtension.labels`	`<string_label_1_key>:`
	`<string_label_1_value>`
	`<string_label_2_key>:`
	`<string_label_2_value>`
		Kubernetes label object syntax.	`customExtension:`
			`  labels: {}`
			`annotations:`
			` {}`
				O	Optional field to configure service specific labels applicable to "Service" Resource Type.

Table 3-5 (Cont.) SCPC-Notification Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-notification.service.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	Kubernetes annotations object syntax.	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type.
scpc-notification.service.ipFamilyPolicy	*notifIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpcNotification service. This value depends on the value of global.serviceIpFamilyPolicy.scpcNotification.
scpc-notification.service.ipFamilies	*notifIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpcNotification service. This value depends on the value of global.serviceIpFamilies.scpcNotification.
scpc-notification.deployment.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	Kubernetes label object syntax.	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.

Table 3-5 (Cont.) SCPC-Notification Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-notification.deployment.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	Kubernetes annotations object syntax.	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type.
scpc-notification.nodeSelector.nodeKey	string	nodeSelector: Use this configuration to apply nodeSelector to Notification service pods nodeKey: Key of the node label.	ocscp	O	Enables node selector for Notification service pods.
scpc-notification.nodeSelector.nodeValue	string	nodeValue: Value of the node label.	scpc-notification	O	Indicates the value of the node label.
scpc-notification.istioSidecarReadyUrl	string		*sidecarReadyUrl	C	Defines the URL to use for checking service mesh sidecar status and starts application once status is ready. Applicable only in serviceMeshEnabled is set to "**true**". **Note**: Do not modify this reference variable.

3.1.5 SCPC-Audit Parameters

The following table lists the SCPC-Audit parameters.

Table 3-6 SCPC-Audit Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-audit.imageDetails.image`	string	image: 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.	ocscp-audit	M	Indicates the Image name of the SCP audit.
`scpc-audit.imageDetails.tag`	string	Tag: 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.	SCP Images	M	Indicates the Image Tag to be used for Configuration container.
`scpc-audit.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scpc-audit.resources.requests.memory`	integer	NA	4Gi	M	Indicates the requested memory (RAM) for configuration microservice in Giga Bytes.
`scpc-audit.resources.requests.cpu`	integer	NA	3	M	Indicates the maximum allocated vCPU for configuration microservice.

Table 3-6 (Cont.) SCPC-Audit Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-audit.resources.requests.ephemeral-storage`	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scpc-audit.resources.limits.memory`	integer	NA	4Gi	M	Indicates the maximum limit of memory for configuration microservice.
`scpc-audit.resources.limits.cpu`	integer	NA	3	M	Indicates the maximum limit of CPU for configuration microservice.
`scpc-audit.resources.limits.ephemeral-storage`	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scpc-audit.auditInterval`	integer	Min: 1, Max: 2147483647	600	M	Time interval in seconds that users want to configure.
`scpc-audit.auditInitialRetryInterval`	integer	Min: 1, Max: 2147483647	2	M	Retry interval in seconds for which audit keeps on retrying until successful response from NRF.
`scpc-audit.alternateResolutionAuditInterval`	integer	Min: 1, Max: 2147483647	300	M	Indicates the DNS SRV audit interval in seconds.
`scpc-audit.log.level`	string		*auditLogLevelRef	O	Enables desired level of logging for the service. **Note**: The value is the same as the `serviceLogLevels.scpcAudit` in the global section.
`scpc-audit.initializationFailTimeout`	integer	NA	160000	O	initializationFailTimeout in ms - Maximum lifetime in milliseconds of a connection in the pool after it is closed.
`scpc-audit.idleTimeout`	integer	NA	10000	O	idleTimeout in ms - Maximum idle time for connection.
`scpc-audit.minimumIdle`	integer	NA	1	O	Indicates the minimum number of idle connections maintained by HikariCP in a connection pool.

Table 3-6 (Cont.) SCPC-Audit Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-audit.connectionTimeout	integer	NA	20000	O	connectionTimeout in ms - Maximum number of milliseconds that a client will wait for a connection.
scpc-audit.maxPoolSize	integer	NA	10	O	Indicates the maximum pool size Hikari CP can create.
scpc-audit.maxLifetime	integer	NA	240	O	Indicates the maximum lifetime in ms of a connection in the pool after it is closed.
scpc-audit.service.type	string	ClusterIP, LoadBalancer, NodePort	ClusterIP	O	When this value is enabled, it overrides the default derivation of Service Type.
scpc-audit.service.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	Kubernetes label object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.
scpc-audit.service.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	Kubernetes annotations object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type

Table 3-6 (Cont.) SCPC-Audit Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-audit.service.ipFamilyPolicy	*auditIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpcAudit service. This value depends on the value of global.serviceIpFamilyPolicy.scpcAudit.
scpc-audit.service.ipFamilies	*auditIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpcAudit service. This value depends on the value of global.serviceIpFamilies.scpcAudit.
scpc-audit.deployment.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	Kubernetes label object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.
scpc-audit.deployment.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	Kubernetes annotations object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type.

Table 3-6 (Cont.) SCPC-Audit Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-audit.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Audit service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Audit service pods.
`scpc-audit.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scpc-audit	O	Indicates the value of the node label.
`scpc-audit.istioSidecarReadyUrl`	string		*sidecarReadyUrl	C	Defines the URL that is used for checking service mesh sidecar status and start the application when the status is ready. Applicable only when `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.

3.1.6 SCPC-Alternate-Resolution Parameters

The following table lists the SCPC-Alternate-Resolution parameters.

Table 3-7 SCPC-Alternate-Resolution Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-alternate-resolution.imageDetails.image`	string	image: 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.	ocscp-alternate-resolution	M	Indicates the Image name of scpc-alternate-resolution.
`scpc-alternate-resolution.imageDetails.tag`	string	Tag: 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.	SCP Images	M	Indicates the Image tag of scpc-alternate-resolution.
`scpc-alternate-resolution.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scpc-alternate-resolution.resources.requests.memory`	integer	NA	2Gi	M	Indicates the requested memory (RAM) for scpc-alternate-resolution in Giga Bytes.

Table 3-7 (Cont.) SCPC-Alternate-Resolution Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-alternate-resolution.resources.requests.cpu	integer	NA	2	M	Indicates the maximum allocated vCPU for scpc-alternate-resolution.
scpc-alternate-resolution.resources.requests.ephemeral-storage	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scpc-alternate-resolution.resources.limits.memory	integer	NA	2Gi	M	Indicates the maximum limit of memory for scpc-alternate-resolution.
scpc-alternate-resolution.resources.limits.cpu	integer	NA	2	M	Indicates the maximum limit of CPU scpc-alternate-resolution.
scpc-alternate-resolution.resources.limits.ephemeral-storage	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scpc-alternate-resolution.log.level	string		*alternateResolutionLogLevelRef	O	Enables desired level of logging for the service.
scpc-alternate-resolution.dnsSrvTTLAuditInterval	integer	Min: 1, Max: 2147483647	1000	M	Indicates the TTL based audit interval in milliseconds.

Table 3-7 (Cont.) SCPC-Alternate-Resolution Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scpc-alternate-resolution.istioSidecarReadyUrl`	string		*sidecarReadyUrl	C	Defines the URL that is used for checking service mesh sidecar status and start the application when the status is ready. Applicable only when `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.
`scpc-alternate-resolution.initializationFailTimeout`	integer	NA	160000	O	Indicates the maximum lifetime of a connection in the pool after it is closed. It is calculated in milliseconds.
`scpc-alternate-resolution.idleTimeout`	integer	NA	10000	O	Indicates the maximum idle time for a connection in milliseconds.
`scpc-alternate-resolution.minimumIdle`	integer	NA	1	O	Indicates the minimum number of idle connections maintained by HikariCP in a connection pool.
`scpc-alternate-resolution.connectionTimeout`	integer	NA	20000	O	Indicates the maximum number of milliseconds that a client can wait for a connection.
`scpc-alternate-resolution.maxPoolSize`	integer	NA	10	O	Indicates the maximum pool size HikariCP can create.
`scpc-alternate-resolution.maxLifetime`	integer	NA	240	O	Indicates the maximum lifetime of a connection in the pool after it is closed. It is calculated in milliseconds.
`scpc-alternate-resolution.service.type`	string	ClusterIP, LoadBalancer, NodePort	ClusterIP	O	Indicates the default service type used is ClusterIP.

Table 3-7 (Cont.) SCPC-Alternate-Resolution Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-alternate-resolution.service.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	K8s label object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.
scpc-alternate-resolution.service.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	K8s annotations object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type.
scpc-alternate-resolution.service.ipFamilyPolicy	*alternateResolutionIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpcAlternateResolution service. This value depends on the value of global.serviceIpFamilyPolicy.scpcAlternateResolution.
scpc-alternate-resolution.service.ipFamilies	*alternateResolutionIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpcAlternateResolution service. This value depends on the value of global.serviceIpFamilies.scpcAlternateResolution.
scpc-alternate-resolution.deployment.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	K8s label object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.

Table 3-7 (Cont.) SCPC-Alternate-Resolution Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scpc-alternate-resolution.deployment.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	K8s annotations object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type.
scpc-alternate-resolution.nodeSelector.nodeKey	string	nodeSelector: Use this configuration to apply nodeSelector to scpc-alternate-service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for scpc-alternate-service pods.
scpc-alternate-resolution.nodeSelector.nodeValue	string	nodeValue: Value of the node label	scpc-alternate-service	O	Value of the node label.

3.1.7 SCP-Worker Parameters

The following table lists the SCP-Worker parameters.

Table 3-8 SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-worker.imageDetails.image`	string	image: 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.	ocscp-worker	M	Indicates the Image name of SCP worker.
`scp-worker.imageDetails.tag`	string	Tag: 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.	SCP Images	M	Indicates the Image Tag to be used for SCP Worker container.
`scp-worker.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scp-worker.resources.requests.memory`	integer	8Gi or 16Gi	16 Gi	M	Indicates the requested memory (RAM) for scp-worker and scp-worker (large profile) microservice in Giga Bytes. **Note**: For smaller profile, change the memory as described in Resource Requirements.

Table 3-8 (Cont.) SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-worker.resources.requests.cpu`	integer	4 or 12	12	M	Indicates the maximum allocated vCPU for scp-worker and scp-worker (large profile) microservice. **Note**: For smaller profile, change the memory as described in Resource Requirements.
`scp-worker.resources.requests.ephemeral-storage`	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scp-worker.resources.limits.memory`	integer	8Gi or 16 Gi	16 Gi	M	Indicates the maximum limit of memory for scp-worker and scp-worker (large profile) microservice. **Note**: For smaller profile, change the memory as described in Resource Requirements.
`scp-worker.resources.limits.cpu`	integer	4 or 12	12	M	Indicates the maximum limit of CPU for scp-worker and scp-worker (large profile) microservice. **Note**: For smaller profile, change the memory as described in Resource Requirements.
`scp-worker.resources.limits.ephemeral-storage`	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scp-worker.tracingenable`	*scpworkerTracingEnabled	Reference Variable		O	Option to enable and disable Jaeger tracing. Default Value is False. **Note**: Do not modify this reference variable.
`scp-worker.enableTraceBody`	*scpworkerJaegerBodyEnabled	Reference Variable		O	Option to enable and disable tracing for full body of all Request or Response messages. The configuration is added only if tracingenable is configured as `true`.

Table 3-8 (Cont.) SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-worker.traceSampling`	integer	0.001 to 1	0.001	O	Option to set the sampling rate for Jaeger traces, that is, 0.01 means 1% of traffic passing through scp-worker will get traced.
`scp-worker.log.level`	string		*workerLogLevelRef	O	Enables the required level of logging for the service. **Note**: Do not modify this reference variable.
`scp-worker.service.ipFamilyPolicy`	*workerIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpWorker service. This value depends on the value of global.serviceIpFamilyPolicy.scpWorker.
`scp-worker.service.ipFamilies`	*workerIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpWorker service. This value depends on the value of global.serviceIpFamilies.scpWorker.
`scp-worker.deployment.containerPortName`	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	http2-5gsig	O	Exposes the name of the container port for HTTP traffic. In CNLB annotation, the back-end port name aligns with the container port name.
`scp-worker.deployment.containerPortNameHttps`	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	https-5gsig	O	Exposes the name of the container port for HTTPS traffic. In CNLB annotation, the back-end port name aligns with the container port name.

Table 3-8 (Cont.) SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-worker.deployment.customExtension.labels`	`<string_label_1_key>:`
	
	`<string_label_1_value>`
	
	`<string_label_2_key>:`
	
	`<string_label_2_value>`
		Kubernetes label object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	Optional field to configure service specific labels applicable to "Service" Resource Type.

`scp-worker.deployment.customExtension.annotations`	`<string_annotation_1_key>:`
	`<string_annotation_1_value>`
	
	`<string_annotation_2_key>:`
	`<string_annotation_2_value>`
		Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	Optional field to configure service specific annotations applicable to "Service" Resource Type.
					Note: Following is the mandatory annotation if you are deploying SCP in Aspen Service Mesh:
					
					`sidecar.istio.io/inject: "true"`
					
					If SCP is integrated with OSO 1.6 (with ASM), use the following annotations: `traffic.sidecar.istio.io/excludeInboundPorts: "8001"`

`scp-worker.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Worker service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Worker service pods.

Table 3-8 (Cont.) SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-worker.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scp-worker	O	Indicates the value of the node label.
`scp-worker.prometheus.scrape`	boolean	true/false	true	O	Option to enable or disable Prometheus metrics scraping.
`scp-worker.minreplicas`	integer	NA	2	M	Indicates the minimum replica count of scp-worker microservice.
`scp-worker.maxreplicas`	integer	Min: 2 Max: 32	32	M	Indicates the maximum replica count of scp-worker microservice.
`scp-worker.maxPdbUnavailable`	integer	NA	25%	M	Defines maximum unavailable value for Kubernetes pod disruption budget.
`scp-worker.downstream.idleTimeout`	integer	NA	600 (in seconds)	O	The idle timeout is defined as the period in which there are no active requests. When the idle timeout is reached the connection is closed. For more information, see the scenarios or recommendations mentioned in `systemOptions` under **scpSoothsayerConfig**. **Note**: The request based timeouts mean that HTTP/2 PINGs will not keep the connection alive.
`scp-worker.downstream.tcpKeepalive.probes`	integer	Min: 1 min Max: 16 minutes	9 min	*tcpKeepalive*- O *tcpKeepalive.probes*- M. if tcpKeepalive is set.	Sets the `tcpKeepalive` parameter to enable TCP Keepalives. `tcpKeepalive.probes` - Maximum number of keepalive probes to send without response before deciding the connection is dead.
`scp-worker.downstream.tcpKeepalive.time`	integer	Min: 1 Max: 7200 (in seconds)	180 (in seconds)	M. if *tcpKeepalive* is set.	The time duration that a connection must be idle before keep-alive probes start is sent.
`scp-worker.downstream.tcpKeepalive.interval`	integer	Min: 1 Max: 120 (in seconds)	1 second	M. if *tcpKeepalive* is set.	The time duration between keep-alive probes.

Table 3-8 (Cont.) SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-worker.istioSidecarReadyUrl`	string		*sidecarReadyUrl	C	Defines the URL that is used for checking service mesh sidecar status and start the application once status is ready. Only applicable when `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.
`scp-worker.maxUpstreamConnectionPerDestination`	integer	1 to 8	8	O	The maximum number of upstream connections per destination per worker pod.

Table 3-8 (Cont.) SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-worker.isStartupProbeEnabled`	boolean	true or false	true	O	Enables or disables startup probe.
					Note: To deploy SCP on CNE 1.8.4 and prior or on Kubernetes versions prior to 1.20.10. This parameter must be manually added in the scp-worker section of the `custom-values.yaml` file and set to false. In addition, add the following parameters:
					
					`readinessProbe`
					
					`initialDelaySeconds: 5`
					`livenessProbe:`
					
					`initialDelaySeconds: 180`
					
					Example:
					
					`scp-worker:`
					
					`isStartupProbeEnabled: false`
					`readinessProbe:`
					
					`initialDelaySeconds: 5`
					`livenessProbe:`
					
					`initialDelaySeconds: 180`

`scp-worker.scpAuthorityMetricLabelDisabled`	boolean	true or false	true	M	This parameter disables the scpAuthority dimension for worker metrics, if the `scpAuthorityMetricLabelDisabled` is set to `true`.

Table 3-8 (Cont.) SCP-Worker Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-worker.scpNFAndSvcInstanceIdMetricLabelDisabled`	boolean	true or false	false	M	This parameter disables the scpNFInstanceId and scpServiceInstanceId dimension for worker metrics, if the `scpNFAndSvcInstanceIdMetricLabelDisabled` is set to `true`.
`scp-worker.tracer.host`	fqdn	Labels can be letter a-z, number 0-9, hyphen (-). Hyphen cannot be first character. Label combined with dot (.) forms domain	NA	M	Configures trace collector FQDN such as Jaeger, APM agent, and so on. **Note**: Trace collector with OpenTelemetry port support should be configured, for example, jaeger-collector.
`scp-worker.tracer.port`	integer	Min: 0 Max: 65535	NA	M	Configures trace collector port such as Jaeger, APM agent, and so on. **Note**: Trace collector port with OpenTelemetry ports should be configured, for example, jaeger-collector ports 4317 or 4318.

3.1.8 SCP-Cache Parameters

The following table lists the SCP-Cache Parameters.

> **Note**
>
> The minimum and maximum vCPU values of SCP-Cache can be set to 2 vCPUs if the rate limiting feature is not required. If the rate limiting feature is required, SCP-Cache vCPU must be updated from 2 to 8 vCPUs.

Table 3-9 SCP-Cache Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-cache.imageDetails.image`	string	image: 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.	ocscp-cache	M	Indicates the Image name of ocscp-cache.
`scp-cache.imageDetails.tag`	string	Tag: 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.	SCP Images	M	Indicates the Image tag of ocscp-cache.
`scp-cache.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scp-cache.resources.requests.memory`	integer	NA	8Gi	M	Indicates the requested memory (RAM) for ocscp-cache in Giga Bytes.
`scp-cache.resources.requests.cpu`	integer	NA	8	M	Indicates the maximum allocated vCPU for ocscp-cache.

Table 3-9 (Cont.) SCP-Cache Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-cache.resources.requests.ephemeral-storage	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scp-cache.resources.limits.memory	integer	NA	2Gi	M	Indicates the maximum limit of memory for ocscp-cache.
scp-cache.resources.limits.cpu	integer	NA	8	M	Indicates the maximum limit of CPU ocscp-cache.
scp-cache.resources.limits.ephemeral-storage	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scp-cache.log.level	string		*cacheLogLevelRef	O	Enables desired level of logging for the service.
scp-cache.extraContainers	string	DISABLED, ENABLED, USE_GLOBAL_VALUE	USE_GLOBAL_VALUE	M	Spawns debug container along with application container in the pod. This debug container is used for debugging purposes. For more information about the debug tool, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.
scp-cache.minreplicas	integer	NA	3	M	Indicates the minimum replica count of the ocscp-cache microservice.
scp-cache.maxreplicas	integer	NA	3	M	Indicates the maximum replica count of the ocscp-cache microservice.
scp-cache.maxPdbUnavailable	integer	NA	1	M	Defines maximum unavailable value for Kubernetes pod disruption budget.

Table 3-9 (Cont.) SCP-Cache Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-cache.istioSidecarQuitUrl`	string	NA	*sidecarQuitUrl	M	Defines the URL that is used for quitting service mesh sidecar. This URL is used to quit the istio sidecar after the completion of hook job. The reference variable `&sidecarQuitUrl` should not be changed, however, the value `"http://127.0.0.1:15000/quitquitquit"` can be changed. It is applicable only when `serviceMeshEnabled` is set to `true`.
`scp-cache.istioSidecarReadyUrl`	string	NA	*sidecarReadyUrl	C	Defines the URL that is used for checking service mesh sidecar status and start the application once status is ready. It is applicable when `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.
`scp-cache.service.type`	string	ClusterIP, LoadBalancer, NodePort	LoadBalancer	O	When this value is enabled, it overrides the default derivation of service type.
`scp-cache.service.publicCacheSvcFedIPSpecified`	boolean	true or false	false	O	Enables or disables Loadbalancer IP configuration statically for a Signaling interface.
`scp-cache.service.publicCacheSvcFedIP`	ip address	IP Address format	10.75.212.88	O	Configures static Signaling Loadbalancer IP. The configured value is used only if publicCacheSvcFedIPSpecified is set to `true`.
`scp-cache.service.cacheServiceNetworkNameEnabled`	boolean	true or false	false	O	Enables or disables metalLB IP allocation dynamically from the pool for Signaling interface.

Table 3-9 (Cont.) SCP-Cache Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-cache.service.cacheServiceNetworkName`	string	alpha-numeric	"metallb.universe.tf/address-pool: signaling"	O	Annotation to notify metalLB to allocate an IP for Signaling interface for scp-cache service. The annotation is added only if cacheServiceNetworkNameEnabled is set to `true`.
`scp-cache.service.port.cohFederationPort`	integer	Min-1024, Max-65535	30001	M	Indicates the container or service Port where the Federation service is hosted.
`scp-cache.service.port.staticNodePortEnabled`	boolean	true or false	false	O	Enables or disables configuration of static Node Port for Signaling interface.
`scp-cache.service.port.nodePort`	integer	As per the Kubernetes cluster, by default it ranges from 30000 to 32767	30001	O	Configures static Node Port for Signaling interfaces. The configured value is used only if staticNodePortEnabled is set to `true`.
`scp-cache.service.port.coherenceMgmtSvcPort`	integer	Min-1024, Max-65535	9000	M	The service port to access the coherence cluster status using the rest based URI.
`scp-cache.service.port.coherenceMsgPort1`	integer	Min- 1024, Max-65535	8095	M	The coherence communication port start range.
`scp-cache.service.port.coherenceMsgPort2`	integer	Min- 1024, Max-65535	8096	M	The coherence communication port end range.

Table 3-9 (Cont.) SCP-Cache Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-cache.service.customExtension.labels`	string	Kubernetes label object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific labels applicable to the "Service" resource type.
					Format is:
					
					`<string_label_1_key>:`
					
					`<string_label_1_value>`
					
					`<string_label_2_key>:`
					
					`<string_label_2_value>`

`scp-cache.service.customExtension.annotations`	string	Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific annotations applicable to the "Service" resource type.
					Format is:
					
					`<string_annotation_1_key>:`
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					`<string_annotation_2_value>`

`scp-cache.service.ipFamilyPolicy`	*cacheIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpCache service. This value depends on the value of global.serviceIpFamilyPolicy.scpCache.
`scp-cache.service.ipFamilies`	*cacheIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpCache service. This value depends on the value of global.serviceIpFamilies.scpCache.

Table 3-9 (Cont.) SCP-Cache Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-cache.deployment.containerPortName`	string	Only alphanumeric characters (a-z, 0-9) and hyphen (-) are allowed. The length should be less than 15 characters.	coherence-fed	O	Exposes the name of the container port. In CNLB annotation, the back-end port name aligns with the container port name.

`scp-cache.deployment.customExtension.labels`	string	Kubernetes label object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific labels applicable to "Service" Resource Type.
					Format is:
					`<string_label_1_key>:`
					`<string_label_1_value>`
					
					`<string_label_2_key>:`
					`<string_label_2_value>`

Table 3-9 (Cont.) SCP-Cache Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-cache.deployment.customExtension.annotations`	string	Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific annotations applicable to "Service" Resource Type.
					Format is:
					`<string_annotation_1_key>:`
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					`<string_annotation_2_value>`
					
					Note: The following annotation is mandatory if you are deploying SCP in Aspen Service Mesh:
					
					`sidecar.istio.io/inject: "true"`
					
					If SCP is integrated with OSO 1.6 (with ASM), use the following annotation:
					`traffic.sidecar.istio.io/excludeInboundPorts: "8001"`

`scpc-cache.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Cache service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Cache service pods.
`scpc-cache.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scpc-cache	O	Value of the node label.

3.1.9 SCP-nrfProxy Parameters

The following table lists the SCP-nrfProxy parameters.

Table 3-10 SCP-nrfproxy Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-nrfproxy.imageDetails.image`	string	image: 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.	ocscp-nrfproxy	M	Indicates the Image name of ocscp-nrfproxy.
`scp-nrfproxy.imageDetails.tag`	string	Tag: 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.	SCP Images	M	Indicates the Image tag of ocscp-nrfproxy.
`scp-nrfproxy.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scp-nrfproxy.resources.requests.memory`	integer	NA	8Gi	M	Indicates the requested memory (RAM) for ocscp-nrfproxy in Giga Bytes.

Table 3-10 (Cont.) SCP-nrfproxy Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-nrfproxy.resources.requests.cpu	integer	NA	8	M	Indicates the maximum allocated vCPU for ocscp-nrfproxy.
scp-nrfproxy.resources.requests.ephemeral-storage	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scp-nrfproxy.resources.limits.memory	integer	NA	2Gi	M	Indicates the maximum limit of memory for ocscp-nrfproxy.
scp-nrfproxy.resources.limits.cpu	integer	NA	8	M	Indicates the maximum limit of CPU ocscp-nrfproxy.
scp-nrfproxy.resources.limits.ephemeral-storage	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scp-nrfproxy.log.level	string	NA	*nrfproxyLogLevelRef	O	Enables desired level of logging for the service.
scp-nrfproxy.extraContainers	string	DISABLED, ENABLED, USE_GLOBAL_VALUE	USE_GLOBAL_VALUE	M	Spawns debug container along with application container in the pod. This debug container is used for debugging purposes. For more information about the debug tool, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.
scp-nrfproxy.minreplicas	integer	NA	1	M	Indicates the minimum replica count of the ocscp-nrfproxy microservice.
scp-nrfproxy.maxreplicas	integer	NA	1	M	Indicates the maximum replica count of the ocscp-nrfproxy microservice.

Table 3-10 (Cont.) SCP-nrfproxy Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-nrfproxy.downstream.idleTimeout`	integer	NA	600 seconds	M	The idle timeout is defined as the period in which there are no active requests. When the idle timeout is reached, the connection is closed. For more information, see the scenarios or recommendations mentioned in `systemOptions` under **scpSoothsayerConfig**. **Note**: The request based timeouts mean that HTTP/2 PINGs will not keep the connection alive.
`scp-nrfproxy.downstream.tcpKeepalive.probes`	integer	Min: 1 min Max: 16 minutes	9 minutes	*tcpKeepalive*- O *tcpKeepalive.probes*- M. if tcpKeepalive is set.	Sets the `tcpKeepalive` parameter to enable TCP Keepalives. `tcpKeepalive.probes` - Maximum number of keepalive probes to send without response before deciding the connection is dead.
`scp-nrfproxy.downstream.tcpKeepalive.time`	integer	Min: 1 Max: 7200 (in seconds)	180 seconds	M. if *tcpKeepalive* is set.	The time duration that a connection must be idle before keep-alive probes start is sent.
`scp-nrfproxy.downstream.tcpKeepalive.interval`	integer	Min: 1 Max: 120 (in seconds)	1 second	M. if *tcpKeepalive* is set.	The time duration between keep-alive probes.
`scp-nrfproxy.maxPdbUnavailable`	integer	NA	25%	M	Defines maximum unavailable value for Kubernetes pod disruption budget.

Table 3-10 (Cont.) SCP-nrfproxy Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-nrfproxy.istioSidecarQuitUrl`	string	NA	*sidecarQuitUrl	M	Defines the URL that is used for quitting service mesh sidecar. This URL is used to quit the istio sidecar after the completion of hook job. The reference variable `&sidecarQuitUrl` should not be changed, however, the value `"http://127.0.0.1:15000/quitquitquit"` can be changed. It is applicable only when `serviceMeshEnabled` is set to `true`.
`scp-nrfproxy.istioSidecarReadyUrl`	string	NA	*sidecarReadyUrl	C	Defines the URL that is used for checking service mesh sidecar status and start the application once status is ready. It is applicable when `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.

`scp-nrfproxy.service.customExtension.labels`	string	Kubernetes label object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific labels applicable to the "Service" resource type.
					Format is:
					
					`<string_label_1_key>:`
					
					`<string_label_1_value>`
					
					`<string_label_2_key>:`
					
					`<string_label_2_value>`

Table 3-10 (Cont.) SCP-nrfproxy Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-nrfproxy.service.customExtension.annotations`	string	Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific annotations applicable to the "Service" resource type.
					Format is:
					
					`<string_annotation_1_key>:`
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					`<string_annotation_2_value>`

`scp-nrfproxy.service.ipFamilyPolicy`	*nrfproxyIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpNrfproxy service. This value depends on the value of global.serviceIpFamilyPolicy.scpNrfproxy.
`scp-nrfproxy.service.ipFamilies`	*nrfproxyIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpNrfproxy service. This value depends on the value of global.serviceIpFamilies.scpNrfproxy.

`scp-nrfproxy.deployment.customExtension.labels`	string	Kubernetes label object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific labels applicable to "Service" Resource Type.
					Format is:
					`<string_label_1_key>:`
					`<string_label_1_value>`
					
					`<string_label_2_key>:`
					`<string_label_2_value>`

Table 3-10 (Cont.) SCP-nrfproxy Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-nrfproxy.deployment.customExtension.annotations`	string	Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			` {}`
				O	An optional field to configure service specific annotations applicable to "Service" Resource Type.
					Format is:
					`<string_annotation_1_key>:`
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					`<string_annotation_2_value>`
					
					Note: The following annotations is mandatory if you are deploying SCP in Aspen Service Mesh:
					
					`sidecar.istio.io/inject: "true"`
					
					If SCP is integrated with OSO 1.6 (with ASM), use the following annotations:
					`traffic.sidecar.istio.io/excludeInboundPorts: "8001"`

`scpc-nrfproxy.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Nrfproxy service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Nrfproxy service pods.
`scpc-nrfproxy.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scpc-nrfproxy	O	Value of the node label.

3.1.10 SCP-Mediation Parameters

The following table lists the SCP-Mediation parameters.

Table 3-11 SCP-Mediation Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-mediation.imageDetails.image`	string	image: 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.	ocmed-nfmediation	M	Indicates the Image name of scp-mediation.
`scp-mediation.imageDetails.tag`	string	Tag: 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.	SCP Images	M	Indicates the Image tag of scp-mediation.
`scp-mediation.imageDetails.pullPolicy`	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
`scp-mediation.resources.requests.memory`	integer	NA	4Gi	M	Indicates the requested memory (RAM) for scp-mediation in Giga Bytes.

Table 3-11 (Cont.) SCP-Mediation Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-mediation.resources.requests.cpu`	integer	NA	4	M	Indicates the maximum allocated vCPU for scp-mediation.
`scp-mediation.resources.requests.ephemeral-storage`	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scp-mediation.resources.limits.memory`	integer	NA	4Gi	M	Indicates the maximum limit of memory for scp-mediation.
`scp-mediation.resources.limits.cpu`	integer	NA	4	M	Indicates the maximum limit of CPU scp-mediation.
`scp-mediation.resources.limits.ephemeral-storage`	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
`scp-mediation.log.level`	string	NA	*mediationLogLevelRef	O	Enables desired level of logging for the service.
`scp-mediation.upgradeStrategy`	string	NA	rollingUpgrade	O	Specifies the strategy used during upgrade process. The only supported upgradeStrategy is rollingUpgrade.
`scp-mediation.extraContainers`	string	DISABLED, ENABLED, USE_GLOBAL_VALUE	USE_GLOBAL_VALUE	M	Spawns debug container along with application container in the pod. This debug container is used for debugging purposes. For more information about the debug tool, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.
`scp-mediation.minreplicas`	integer	NA	1	M	Indicates the minimum replica count of the scp-mediation microservice.

Table 3-11 (Cont.) SCP-Mediation Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-mediation.maxreplicas	integer	NA	1	M	Indicates the maximum replica count of the scp-mediation microservice.
scp-mediation.jaegerTracingEnabled	boolean	true or false	false	O	Enables Jaeger traces for mediation.
scp-mediation.bodyInTraceEnabled	boolean	true or false	true	O	Enables body traces for mediation.
scp-mediation.otel.jaeger.udpSender.host	string	NA	"jaeger-agent.occne-infra"	O	Indicates the host details of the Jaeger server.
scp-mediation.otel.jaeger.udpSender.port	integer	0 - 65535	6831	O	Indicates the port details of the Jaeger server.
scp-mediation.otel.jaeger.logSpans	boolean	true or false	false	O	Enables Jaeger log spans.
scp-mediation.otel.jaeger.probabilisticSamplingRate	string	0-1	0.001	O	Indicates the sampling rate for Jaeger
scp-mediation.service.active.forwardToTest	boolean	true or false	false	O	Enables mediation test mode and forward requests to test the deployment.
scp-mediation.service.type	string	ClusterIP, LoadBalancer, NodePort	ClusterIP	O	Indicates the default service type used is ClusterIP.

Table 3-11 (Cont.) SCP-Mediation Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-mediation.service.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	K8s label object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.
scp-mediation.service.customExtension.annotations	<string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>	K8s annotations object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific annotations applicable to "Service" Resource Type.
scp-mediation.service.ipFamilyPolicy	*mediationTestIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpMediation service. This value depends on the value of global.serviceIpFamilyPolicy.scpMediation.
scp-mediation.service.ipFamilies	*mediationTestIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpMediation service. This value depends on the value of global.serviceIpFamilies.scpMediation.
scp-mediation.deployment.customExtension.labels	<string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>	K8s label object syntax	customExtension: labels: {} annotations: {}	O	Optional field to configure service specific labels applicable to "Service" Resource Type.

Table 3-11 (Cont.) SCP-Mediation Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-mediation.deployment.customExtension.annotations`	`<string_annotation_1_key>: <string_annotation_1_value>`
	
	`<string_annotation_2_key>: <string_annotation_2_value>`
		K8s annotations object syntax	`customExtension: labels: {}`
			
			`annotations: {}`
				O	Optional field to configure service specific annotations applicable to "Service" Resource Type.

`scp-mediation.mediationConfig.serviceUrl`	string	NA	`mediationConfig: serviceUrl:<service>:<servicePort>/<baseUrl>`	M	Indicates the setup URL to be used by the mediation service to connect to the mediation config. **Note**: <baseUrl> must match the mediationConfig.baseUrl property from the service application properties.
`scpc-mediation.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Mediation service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Mediation service pods.
`scpc-mediation.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scpc-mediation	O	Value of the node label.
`nfName`	string	NA	OSCP	M	This parameter is appended to the `ProblemDetails` implementation to specify the source NF name. This parameter must be configured during the SCP deployment.

Table 3-11 (Cont.) SCP-Mediation Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
nfFqdn	string	NA	ocscp-scp-worker.scpsvc.svc.cluster.local	M	This parameter is appended to the ProblemDetails implementation to specify the source NF FQDN as SCP's FQDN. This parameter must be configured during the SCP deployment.
partOf	string	NA	Release.Name	O	Indicates the value for the network-policy rule pertaining to mediation traffic.

3.1.11 SCP-Load-Manager Parameters

The following table lists the SCP-Load-Manager Parameters.

> **Note**
>
> The minimum and maximum vCPU of SCP-Load-Manager can be set to 4 vCPUs if the number of supported NFs is less than 150. If the number of NFs is more than 150, use the default value, 8 vCPUs.

Table 3-12 SCP-Load-Manager Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-load-manager.imageDetails.image	string	image: 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.	ocscp-load-manager	M	Indicates the Image name of ocscp-load-manager.

Table 3-12 (Cont.) SCP-Load-Manager Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-load-manager.imageDetails.tag	string	Tag: 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.	SCP Images	M	Indicates the Image tag of ocscp-load-manager.
scp-load-manager.imageDetails.pullPolicy	string	Always, IfNotPresent, Never	Always	M	Indicates if the image has to be pulled.
scp-load-manager.resources.requests.memory	integer	NA	8Gi	M	Indicates the requested memory (RAM) for ocscp-load-manager in Giga Bytes.
scp-load-manager.resources.requests.cpu	integer	NA	8	M	Indicates the maximum allocated vCPU for ocscp-load-manager.
scp-load-manager.resources.requests.ephemeral-storage		NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scp-load-manager.resources.limits.memory	integer	NA	8Gi	M	Indicates the maximum limit of memory for ocscp-load-manager.
scp-load-manager.resources.limits.cpu	integer	NA	8	M	Indicates the maximum limit of CPU ocscp-load-manager.
scp-load-manager.resources.limits.ephemeral-storage	integer	NA	1Gi	O	Indicates the maximum limit of the ephemeral storage that can be allocated. **Note**: Commenting this parameter does not enable it.
scp-load-manager.log.level	string		WARN	O	Enables desired level of logging for the service.

Table 3-12 (Cont.) SCP-Load-Manager Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-load-manager.extraContainers`	string	DISABLED, ENABLED, USE_GLOBAL_VALUE	USE_GLOBAL_VALUE	M	Spawns debug container along with application container in the pod. This debug container is used for debugging purposes. For more information about the debug tool, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.
`scp-load-manager.minreplicas`	integer	NA	2	M	Indicates the minimum replica count of the ocscp-load-manager microservice.
`scp-load-manager.maxreplicas`	integer	NA	3	M	Indicates the maximum replica count of the ocscp-load-manager microservice.
`scp-load-manager.maxPdbUnavailable`	integer	NA	1	M	Defines maximum unavailable value for Kubernetes pod disruption budget.
`scp-load-manager.istioSidecarQuitUrl`	string	NA	*sidecarQuitUrl	M	Defines the URL that is used for quitting service mesh sidecar. This URL is used to quit the istio sidecar after the completion of hook job. The reference variable `&sidecarQuitUrl` should not be changed, however, the value `"http://127.0.0.1:15000/quitquitquit"` can be changed. It is applicable only when `serviceMeshEnabled` is set to `true`.
`scp-load-manager.istioSidecarReadyUrl`	string	NA	*sidecarReadyUrl	C	Defines the URL that is used for checking service mesh sidecar status and start the application once status is ready. It is applicable when `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.
`scp-load-manager.service.type`	string	ClusterIP, LoadBalancer, NodePort	LoadBalancer	O	When this value is enabled, it overrides the default derivation of service type.

Table 3-12 (Cont.) SCP-Load-Manager Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-load-manager.service.port.coherenceMgmtSvcPort	integer	Min-1024, Max-65535	9000	M	The service port to access the coherence cluster status using the rest based URI.
scp-load-manager.service.port.coherenceMsgPort1	integer	Min- 1024, Max-65535	8095	M	The coherence communication port start range.
scp-load-manager.service.port.coherenceMsgPort2	integer	Min- 1024, Max-65535	8096	M	The coherence communication port end range.
scp-load-manager.service.customExtension.labels	string	Kubernetes label object syntax	customExtension: labels: {} annotations: {}	O	An optional field to configure service specific labels applicable to the "Service" resource type. Format is: <string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>
scp-load-manager.service.customExtension.annotations	string	Kubernetes annotations object syntax	customExtension: labels: {} annotations: {}	O	An optional field to configure service specific annotations applicable to the "Service" resource type. Format is: <string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>
scp-load-manager.service.ipFamilyPolicy	*loadManagerIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpcLoadManager service. This value depends on the value of global.serviceIpFamilyPolicy.scpcLoadManager.

Table 3-12 (Cont.) SCP-Load-Manager Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-load-manager.service.ipFamilies`	*loadManagerIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpcLoadManager service. This value depends on the value of global.serviceIpFamilyPolicy.scpcLoadManager.

`scp-load-manager.deployment.customExtension.labels`	string	Kubernetes label object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			`{}`
				O	An optional field to configure service specific labels applicable to "Service" Resource Type.
					Format is:
					`<string_label_1_key>:`
					`<string_label_1_value>`
					`  <string_label_2_key>:`
					`<string_label_2_value>`

`scp-load-manager.deployment.customExtension.annotations`	string	Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			`{}`
				O	An optional field to configure service specific annotations applicable to "Service" Resource Type.
					Format is:
					`<string_annotation_1_key>:`
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					`<string_annotation_2_value>`
					
					Note: The following annotations is mandatory if you are deploying SCP in Aspen Service Mesh:
					
					`sidecar.istio.io/inject: "true"`
					
					If SCP is integrated with OSO 1.6 (with ASM), use the following annotations:
					`traffic.sidecar.istio.io/excludeInboundPorts: "8001"`

`scp-load-manager.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Load Manager service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Load Manager service pods.

Table 3-12 (Cont.) SCP-Load-Manager Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-load-manager.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scp-load-manager	O	Value of the node label.

> **Note**
>
> Coherence communication between scp-worker to or from scp-load-manager and between scp-load-manager instances is excluded from ASM.

3.1.12 SCP-nrfProxy-oauth Parameters

The following table lists the SCP-nrfProxy-oauth parameters.

Table 3-13 SCP-nrfProxy-oauth Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-nrfproxy-oauth.imageDetails.image`	string	image: 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.	NA	M	Indicates the Image name of scp-nrfproxy-oauth micro service.

Table 3-13 (Cont.) SCP-nrfProxy-oauth Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-nrfproxy-oauth.imageDetails.tag	string	Tag: 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.	NA	M	Indicates the Image tag of scp-nrfproxy-oauth micro service.
scp-nrfproxy-oauth.imageDetails.pullPolicy	string	Always, IfNotPresent, Never	Always	O	Indicates if the image has to be pulled. pullPolicy: Image Pull Policy made available from 1.7.0
scp-nrfproxy-oauth.memory	integer	NA	8Gi	M	Indicates the requested memory (RAM) for ocscp-nrfproxy-oauth in Giga Bytes.
scp-nrfproxy-oauth.cpu	integer	NA	8	M	Indicates the maximum allocated vCPU for ocscp-nrfproxy-oauth.
scp-nrfproxy-oauth.ephemeral-storage	integer	NA	70Mi	O	Indicates the minimum limit of the ephemeral storage that can be allocated.
scp-nrfproxy-oauth.log.level	string	NA	*nrfProxyOauthLogLevelRef	C	Enables desired level of logging for the service.
scp-nrfproxy-oauth.extraContainers	string	DISABLED, ENABLED, USE_GLOBAL_VALUE	USE_GLOBAL_VALUE	O	Spawns debug container along with application container in the pod. This debug container is used for debugging purposes. For more information about the debug tool, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.
scp-nrfproxy-oauth.minreplicas	integer	NA	2	C	Indicates the minimum replica count of the ocscp-nrfproxy-oauth microservice.
scp-nrfproxy-oauth.maxreplicas	integer	NA	16	C	Indicates the maximum replica count of the ocscp-nrfproxy-oauth microservice.
scp-nrfproxy-oauth.maxPdbUnavailable	integer	NA	1	C	Defines maximum unavailable value for Kubernetes pod disruption budget.

Table 3-13 (Cont.) SCP-nrfProxy-oauth Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
`scp-nrfproxy-oauth.istioSidecarQuitUrl`	string	NA	*sidecarQuitUrl	O	Defines the URL that is used for quitting service mesh sidecar. This URL is used to quit the istio sidecar after the completion of hook job. The reference variable `&sidecarQuitUrl` should not be changed, however, the value `"http://127.0.0.1:15000/quitquitquit"` can be changed. It is applicable only when `serviceMeshEnabled` is set to `true`.
`scp-nrfproxy-oauth.istioSidecarReadyUrl`	string	NA	*sidecarReadyUrl	O	Defines the URL that is used for checking service mesh sidecar status and start the application once status is ready. It is applicable only when `serviceMeshEnabled` is set to `true`. **Note**: Do not modify this reference variable.
`scp-nrfproxy-oauth.commonJCServiceMeshCheck`	string	NA	*svcMeshEnabled	M	Indicates the system supports service mesh.
`scp-nrfproxy-oauth.service.type`	string	ClusterIP, LoadBalancer, NodePort	LoadBalancer	M	Indicates that when this value is enabled, it overrides the default derivation of the service type.
`scp-nrfproxy-oauth.service.port.coherenceMgmtSvcPort`	integer	Min-1024, Max-65535	9000	M	Indicates the service port to access the coherence cluster status using the rest-based URI.
`scp-nrfproxy-oauth.service.port.coherenceMsgPort1`	integer	Min-1024, Max-65535	8095	M	Indicates the coherence communication port start range.
`scp-nrfproxy-oauth.service.port.coherenceMsgPort2`	integer	Min-1024, Max-65535	8096	M	Indicates the coherence communication port end range.

Table 3-13 (Cont.) SCP-nrfProxy-oauth Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description
scp-nrfproxy-oauth.service.customExtension.labels	string	Kubernetes label object syntax	customExtension: labels: {} annotations: {}	O	An optional field to configure service specific labels applicable to the "Service" resource type. Format is: <string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>
scp-nrfproxy-oauth.service.customExtension.annotations	string	Kubernetes annotations object syntax	customExtension: labels: {} annotations: {}	O	An optional field to configure service specific annotations applicable to the "Service" resource type. Format is: <string_annotation_1_key>: <string_annotation_1_value> <string_annotation_2_key>: <string_annotation_2_value>
scp-nrfproxy-oauth.service.ipFamilyPolicy	*nrfProxyOauthIpFamilyPolicy	SingleStack, PreferDualStack, or RequireDualStack	NA	C	ipFamilyPolicy to be allocated to scpNrfProxyOauth service. This value depends on the value of global.serviceIpFamilyPolicy.scpNrfProxyOauth.
scp-nrfproxy-oauth.service.ipFamilies	*nrfProxyOauthIpFamilies	[IPv4], [IPv6], [IPv4,IPv6], [IPv6,IPv4]	NA	C	ipFamilies to be allocated to scpNrfProxyOauth service. This value depends on the value of global.serviceIpFamilyPolicy.scpNrfProxyOauth.
scp-nrfproxy-oauth.deployment.customExtension.labels	string	Kubernetes label object syntax	customExtension: labels: {} annotations: {}	O	An optional field to configure service specific labels applicable to "Service" Resource Type. Format is: <string_label_1_key>: <string_label_1_value> <string_label_2_key>: <string_label_2_value>

Table 3-13 (Cont.) SCP-nrfProxy-oauth Parameters

Parameter Name	DataType	Range	Default Value	Mandatory(M)/ Optional(O)/ Conditional(C)	Description

`scp-nrfproxy-oauth.deployment.customExtension.annotations`	string	Kubernetes annotations object syntax	`customExtension:`
			`  labels: {}`
			
			`annotations:`
			`{}`
				O	An optional field to configure service specific annotations applicable to "Service" Resource Type.
					Format is:
					`<string_annotation_1_key>:`
					`<string_annotation_1_value>`
					
					`<string_annotation_2_key>:`
					`<string_annotation_2_value>`
					
					Note: The following annotations is mandatory if you are deploying SCP in Aspen Service Mesh:
					
					`sidecar.istio.io/inject: "true"`
					
					If SCP is integrated with OSO 1.6 (with ASM), use the following annotations:
					`traffic.sidecar.istio.io/excludeInboundPorts: "8001"`

`scp-nrfproxy-oauth.nodeSelector.nodeKey`	string	nodeSelector: Use this configuration to apply nodeSelector to Nrfproxy Oauth service pods nodeKey: Key of the node label	ocscp	O	Enables node selector for Nrfproxy Oauth service pods.
`scp-nrfproxy-oauth.nodeSelector.nodeValue`	string	nodeValue: Value of the node label	scp-nrfproxy-oauth	O	Value of the node label.

3.2 cnDBTier Customization Parameters

By default, the `ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml` provided with the SCP installation is for a three-site georedundant deployment of cnDBteir.

cnDBTier can be supported in the following modes:

- Two-site cnDBTier georeplication mode: A DB backup from one of the sites can be used for fault recovery of SCP.

- Three-site georeplication mode: A DB backup from one of the sites can be used for fault recovery of SCP.
- One-site cnDBTier deployment mode: The georeplication is unavailable. User must continue taking DB backup periodically, preferably on a daily basis, so that the same can be used when fault recovery scenarios arise.

> **Note**
>
> The cnDBTier georeplication at SCP is used for keeping DB backup so that it can be used in case of fault recovery.

The following table lists the customized cnDBTier parameters for SCP.

> **Note**
>
> - For information about the values of the following parameters, see the `ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml` file.
> - Any change in the cnDBTier custom_values file introduced by the cnDBTier patch must be updated in the custom_values file provided by SCP before deployment.

Table 3-14 cnDBTier Customization Parameters for SCP

Parameter Name	Parameter Values	Added or Modified in Release
`MaxNoOfOrderedIndexes`	The following default values are recommended: • 3072 for a one-site deployment (1024 for SCP and the rest for CNC Console). • 4096 for a two-site deployment. • 5120 for a three-site deployment.	25.2.100
`MaxNoOfAttributes`	The following default values are recommended: • 6500 for a one-site deployment. • 13000 for a two-site deployment • 20000 for a three-site deployment	25.2.100
`global.apiReplicaCount`	The default value in the `ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml` file to be updated as follows: • A two-site replication requires minimum 2 SQL nodes. • A three-site replication requires minimum 4 SQL nodes. • The default value of this parameter is set to 4 for three-site replication. • In case of no replication, the minimum number of sql nodes required is 0.	23.2.0
`global.ndbappReplicaMaxCount`	Default value to be used as in the file	23.2.0
`global.ndbconfigurations.ndb.NoOfFragmentLogParts`	Default value to be used as in the file	23.2.0
`global.ndbconfigurations.ndb.MaxNoOfExecutionThreads`	Default value to be used as in the file	23.2.0

Table 3-14 (Cont.) cnDBTier Customization Parameters for SCP

Parameter Name	Parameter Values	Added or Modified in Release
global.additionalndbconfigurations.ndb.CompressedLCP	Default value to be used as in the file	23.2.0
additionalndbconfigurations.mysqld.ndb_batch_size	Default value to be used as in the file	23.2.0
global.additionalndbconfigurations.mysqld.ndb_blob_write_batch_bytes	Default value to be used as in the file	23.2.0
additionalndbconfigurations.mysqld.replica_skip_errors	Default value to be used as in the file	23.2.0
global.mgm.ndbdisksize	Default value to be used as in the file	23.2.0
global.ndb.ndbdisksize	Default value to be used as in the file	23.2.0
global.ndb.ndbbackupdisksize	Default value to be used as in the file	23.2.0
global.ndb.datamemory	Default value to be used as in the file	23.2.0
global.api.ndbdisksize	Default value to be used as in the file	23.2.0
global.ndbapp.ndbdisksize	Default value to be used as in the file	23.2.0
global.replicationskiperrors.replicationerrornumbers	Default value to be used as in the file	23.2.0
mgm.resources.limits.cpu	Default value to be used as in the file	23.2.0
mgm.resources.limits.memory	Default value to be used as in the file	23.2.0
mgm.resources.requests.cpu	Default value to be used as in the file	23.2.0
mgm.resources.requests.memory	Default value to be used as in the file	23.2.0
ndb.sidecar.resources.limits.cpu	Default value to be used as in the file	23.2.0
ndb.sidecar.resources.limits.memory	Default value to be used as in the file	23.2.0
ndb.sidecar.resources.limits.ephemeral-storage	Default value to be used as in the file	23.2.0
ndb.sidecar.resources.requests.cpu	Default value to be used as in the file	23.2.0
ndb.sidecar.resources.requests.memory	Default value to be used as in the file	23.2.0
ndb.resources.limits.cpu	Default value to be used as in the file	23.2.0
ndb.resources.limits.memory	Default value to be used as in the file	23.2.0
ndb.resources.requests.cpu	Default value to be used as in the file	23.2.0
ndb.resources.requests.memory	Default value to be used as in the file	23.2.0
api.resources.limits.cpu	Default value to be used as in the file	23.2.0
api.resources.limits.memory	Default value to be used as in the file	23.2.0
api.resources.requests.cpu	Default value to be used as in the file	23.2.0
api.resources.requests.memory	Default value to be used as in the file	23.2.0
api.ndbapp.resources.limits.cpu	Default value to be used as in the file	23.2.0
api.ndbapp.resources.limits.memory	Default value to be used as in the file	23.2.0
api.ndbapp.resources.requests.cpu	Default value to be used as in the file	23.2.0

Table 3-14 (Cont.) cnDBTier Customization Parameters for SCP

Parameter Name	Parameter Values	Added or Modified in Release
`api.ndbapp.resources.requests.memory`	Default value to be used as in the file	23.2.0
`db-replication-svc.dbreplsvcdeployments.resources.limits.cpu`	Default value to be used as in the file	23.2.0
`db-replication-svc.dbreplsvcdeployments.resources.limits.memory`	Default value to be used as in the file	23.2.0
`db-replication-svc.dbreplsvcdeployments.resources.requests.cpu`	Default value to be used as in the file	23.2.0
`db-replication-svc.dbreplsvcdeployments.resources.requests.memory`	Default value to be used as in the file	23.2.0
`db-monitor-svc.resources.limits.cpu`	Default value to be used as in the file	23.2.0
`db-monitor-svc.resources.limits.memory`	Default value to be used as in the file	23.2.0
`db-monitor-svc.resources.requests.cpu`	Default value to be used as in the file	23.2.0
`db-monitor-svc.resources.requests.memory`	Default value to be used as in the file	23.2.0
`additionalndbconfigurations.ndb.ODirect`	Default value to be used as in the file	23.2.0
`MaxNoOfTables`	Default value to be used as in the file	25.2.100
`MaxNoOfUniqueHashIndexes`	Default value to be used as in the file	25.2.100

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

4
Upgrading SCP

You can upgrade SCP from a source release to a target release using procedures outlined in this chapter.

4.1 Supported Upgrade Paths

The following table lists the supported upgrade paths for SCP:

Table 4-1 SCP Supported Upgrade Paths

Source Release	Target Release
25.1.2xx	25.2.201
25.2.1xx	25.2.201

> **Note**
>
> SCP must be upgraded before upgrading cnDBTier.

4.2 Upgrade Strategy

SCP 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. The following configuration parameters define the upgrade strategy:

- The `upgradeStrategy` parameter indicates the update strategy in SCP.
- The `maxUnavailable` parameter determines the number of pods that are unavailable during the update.
- The `maxSurge` parameter determines the number of pods that can be created above the desired amount of pods during an upgrade.

Table 4-2 Predefined Upgrade Strategy Value

Microservice	Upgrade Value (maxUnavailable)	Upgrade Value (maxSurge)
scp-worker	25%	25%
scp-nrfproxy	25%	25%
scp-mediation	25%	25%

4.3 Preupgrade Tasks

Perform the following procedure before upgrading SCP.

> **Note**
>
> - The `releaseVersion` value in the `ocscp_values.yaml` file can not be changed.
> - While performing an upgrade from an older release to a newer release, you must align the `ocscp_values.yaml` file of the new release as per the `ocscp_values.yaml` file of the older release. Ensure that you do not change any Helm parameter values. During the upgrade, modifications are allowed for the following parameters: `scpProfileInfo.plmnList`, `scpProfileInfo.customInfo.mateScpInfoList`, `scpProfileInfo.customInfo.mateSiteInfo`, and TLS configuration. Other parameters should not be modified during the upgrade process. Do not enable any new feature during the upgrade. Any `ocscp_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, Service Communication Proxy User Guide*.
> - Install or upgrade the network policies, if applicable. For more information, see Configuring Network Policies for SCP
> - Ensure that the Service Account, Role, and Rolebinding are as per the current release. For more information, see Manually Creating Service Account, Role, and Rolebinding.

1. Download the SCP package from My Oracle Support (MOS) as described in Downloading the SCP Package.
2. Push the images to Customer Docker Registry as described in Pushing the Images to Customer Docker Registry.
3. Keep the `ocscp_values.yaml` file of the source release (25.2.1xx and 25.1.2xx) as backup while upgrading from the source release to 25.2.201.
4. Update the `ocscp_values.yaml` (25.2.201) file as per the target release as described in Customizing SCP.
5. Before upgrading cnDBTier, for any change related to cnDBTier disk size, PVC size, or resources from source release to target release, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*
6. Update `MaxNoOfAttributes`, `MaxNoOfOrderedIndexes`, `MaxNoOfTables`, and `MaxNoOfUniqueHashIndexes` parameters before upgrading cnDBTier. For more information about these parameters, see cnDBTier Customization Parameters.
7. While upgrading from 25.2.1xx or 25.1.2xx to 25.2.201, do the following:
   - To configure multiple TLS certificates for ingress and egress connections, update the values of the following Helm parameters in `server` and `client` subsections of the `sbiProxySslConfigurations` parameter in the 25.2.201 `ocscp_values.yaml` file with the same values available for the `sslConfigurations` parameter in the 25.2.1xx or 25.1.2xx `ocscp_values.yaml` file:
     – primary.secretName

  - primary.privateKey
  - primary.certificate
  - primary.caBundle
  - primary.keyStorePassword
  - primary.trustStorePassword
- To configure Oracle Communications Network Analytics Data Director (OCNADD) connection, update the values of the following Helm parameters in the `ddSslConfiguration` section in the 25.2.201 `ocscp_values.yaml` file with the same values available for the `ddSslConfiguration` parameter in the 25.2.1xx and 25.1.2xx `ocscp_values.yaml` file:
  - primary.k8SecretName
  - primary.trustStorePassword
  - primary.caBundle
  - primary.trustStoreType
  - primary.certificate
  - primary.privateKey
  - primary.keyStorePassword
  - primary.keyStoreType

8. Ensure that the `coherence.clusterName` parameter value is the same as the previous releases.

   You must edit the `coherence.clusterName` parameter value to be equivalent with the `${RELEASE_NAME}-${COHERENCE_CLUSTER_NAME}-${POD_NAMESPACE}` format, which was used in the previous releases. To edit the `coherence.clusterName` parameter value, prefix the SCP release name with a hyphen (-), and then suffix with a hyphen (-) and the namespace. A sample `coherence.clusterName` is as follows: `ocscp-scp-coherence-cluster-scpsvc`, where `ocscp` is the SCP release name and `scpsvc` is the namespace.
   In case of a fresh installation, this parameter value can be set to any required value with a maximum of 66 characters.
9. Ensure that the minimum resource requirements are achieved for SCP upgrade as described in Upgrade.
10. Delete all the older versions backup tables from the backup DB except the ReleaseConfig table.

    For example, if the current SCP deployed version is 24.3.0 (numeric value 2400300), then all the tables with the string 'backup' and a version field less than 2400300 can be deleted.

    Sample backup table name:
    TRAFFIC_FEED_DATA_DIRECTOR_CONFIG_backup_2200200. Here, the version value is 2200200. In this example, the given table can be deleted before upgrading.
11. Perform sanity check using Helm test as described in Performing Helm Test.

4.4 Upgrade Tasks

Perform this procedure to upgrade SCP.

> **Note**
>
> - SCP might raise alerts while performing an upgrade. To clear any alert, see "Alerts" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
> - SCP uses the `upgraderollbackevents` resource to retrieve the list of upgrade and rollback events. For more information, see *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.
> - While performing the upgrade, you may observe some deviation in SCP traffic processing rate for some of the data plane services, such as SCP-Worker, SCP-nrfProxy, SCP-Mediation, and so on, on Grafana as the pods are scaling down and scaling up. To verify whether there is any actual traffic deviation, it is recommended to check the traffic rate for the same time duration at the consumer NF's side.
> - The SCP-Load-Manager and SCP-Cache pods running on the target release will re-spin as part of the postupgrade hooks.

- Ensure that no SCP pod is in the failed state.
- Complete the tasks as described in Preupgrade Tasks.

> **Caution**
>
> No configuration should be performed during upgrade.

> **Note**
>
> - If there are less than or equal to 32 SCP-worker pods, the timeout value during the Helm upgrade must be set to 30 minutes.
> - If there are more than 32 SCP-worker pods, the timeout value during the Helm upgrade must be changed to 60 minutes.

Helm Upgrade

Upgrading an existing deployment replaces the running containers and pods with target release containers and pods. If there is no change in the pod configuration, then it is not replaced. Unless there is a change in the service configuration of a microservice, the service endpoints remain unchanged. For example, ClusterIP.

1. To upgrade an existing SCP deployment, run the following command:
   a. Using the local Helm chart:

      ```
      helm upgrade <release_name> <helm_chart> -f <ocscp_values.yaml>--
      namespace <namespace-name> --timeout=30m
      ```

      Where,

      - `<release_name>` is the release name used by the Helm command.

- <helm_chart> is the location of the Helm chart extracted from the target file.
- <ocscp_values.yaml> is the SCP customized values.yaml for target release.
- <namespace-name> is the SCP namespace in which release is deployed.

Example:

```
helm upgrade ocscp  -f ocscp_values_25.2.201.yaml --namespace ocscp --
timeout=30m
```

b. Using chart from Helm repo:

```
helm upgrade <release_name> <helm_repo/helm_chart> --version
<chart_version> -f <ocscp_values.yaml> --namespace <namespace-name> --
timeout=30m
```

Where,

- <helm_repo> is the SCP Helm repo.
- <chart_version> is the version of the Helm chart extracted from the file.

Example:

```
helm upgrade ocscp ocscp-helm-repo/ocscp --version -f
ocscp_values_25.2.201.yaml --namespace ocscp --timeout=30m
```

⚠ Caution

Do not exit from the Helm upgrade command manually. After running the Helm upgrade command, wait until all of the services are upgraded. Do not press "ctrl+c" to come out from the Helm upgrade command. It may lead to uncommon behavior.

2. To check the status of the upgrade, run the following command:

```
helm history <release_name> --namespace <namespace-name>
```

ⓘ Note

After upgrading to SCP 25.2.201, the <release_name>-scp-worker-headless service is present with no active pods. It is removed in 25.2.201.

Sample output of a successful upgrade

```
REVISION        UPDATED                         STATUS
CHART           APP VERSION     DESCRIPTION
1               Mon December 08 06:55:48 2025        superseded
ocscp_25.2.201   25.2.201.0.0      Install complete
2               Mon December 08 07:08:08 2025        deployed
ocscp_25.2.201   25.2.201.0.0      Upgrade complete
```

3. If the upgrade fails, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.

> **Note**
>
> You must clean up any residual job from the SCP deployment after the upgrade is complete.

4. Perform sanity check using Helm test as described in Performing Helm Test.

4.5 Postupgrade Tasks

> **Note**
>
> - To upgrade cnDBTier with resources recommended for SCP, customize the `ocscp_dbtier_25.2.201_custom_values_25.2.201.yaml` file in the `ocscp_csar_25_2_2_0_1_0.zip` folder with the required deployment parameters. cnDBTier parameters will vary depending on whether the deployment is on a single site, two site, or three site. For more information, see cnDBTier Customization Parameters.
> For more information about cnDBTier upgrade, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
> - To automate the lifecycle management of the certificates through OCCM, you can migrate the lifecycle of certificates and key management from manual to OCCM. For more information, see "Introducing OCCM in an Existing NF Deployment" section in *Oracle Communications Cloud Native Core, Certificate Management User Guide*. SCP application does not manage the LCM of the certificate and key.

4.5.1 Alert Configuration

This section describes how to modify or update SCP alerts as required, based on requirements, after performing the upgrade.

For more information, see the following sections:

- Alert Configuration
- Configuring SCP Alerts for OCI

4.6 Migrating SCP to Support an ASM Disabled cnDBTier

Perform the following procedure to migrate SCP to an ASM-disabled cnDBTier.
Prerequisites

- Ensure that SCP is deployed with ASM enabled.
- cnDBTier is deployed with istioSidecarInject.mode parameter set to All.

1. Upgrade cnDBTier with the `istioSidecarInject.mode` parameter set to All as described in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
2. Upgrade SCP as described in Upgrade Tasks.

3. Upgrade the CNC Console as described in *Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide* .

> **Note**
>
> In-service upgrade is not supported for migrating from an ASM-enabled cnDBTier configuration to one that removes ASM from internal communication while retaining ASM only for external communication. You must first divert traffic to another site, then isolate the current site from georeplication before making any change.

4. Migrate cnDBTier deployment to one with the `istioSidecarInject.mode` parameter set to external.

   This deployment should have sidecar injected only in the pods used for external communication after migration. For more information about the migration procedure, see *Oracle Communications Cloud Native Core, cnDBTier User Guide*.

5. Verify if the `SCPMicroServiceUnreachable` alert is raised.

   For more information about the `SCPMicroServiceUnreachable` alert, see *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

6. Ensure that the DestinationRule is present in the `ocscp_servicemesh_config_values_25.2.201.yaml` file:

   DestinationRule for mysql-connectivity-service:

```
- host: <db-service-name>.<db-namespace>.svc.<domain>
    exportTo:
      - "."                              # refers to the current namespace
    mode: DISABLE
    name: scp-db-service-dr
    namespace: <scp-namespace>         # change the namespace according to
deployment
    sbitimers: true
    tcpConnectTimeout: "750ms"
    tcpKeepAliveProbes: 3
    tcpKeepAliveTime: "1500ms"
    tcpKeepAliveInterval: "1s"
```

   DestinationRule for mysql-cluster-db-monitor-svc

```
- host: <db-service-name>.<db-namespace>.svc.<domain>
    exportTo:
      - "."                              # refers to the current namespace
    mode: DISABLE
    name: cncc-db-monitor-dr
    namespace: <cncc-namespace>         # change the namespace according
to deployment
```

7. Run the following command to upgrade `ocscp-servicemesh-config` with DestinationRule scp-db-service-dr, where TLS communication to mysql-connectivity-service is set to

DISABLE and DestinationRule cncc-db-monitor-dr, where TLS communication to mysql-cluster-db-monitor-svc is set to DISABLE:

```
helm upgrade ocscp-servicemesh-config -f values.yaml charts.tgz -n <scp-
namespace> --timeout=30m
```

8. Ensure that the `SCPMicroServiceUnreachable` alert is cleared.

   For more information about the `SCPMicroServiceUnreachable` alert, see *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.

9. Verify the connection between SCP microservices and cnDBTier to ensure that all SCP pods are up and running after the migration.

   Sample migration output:

```
cicdocscp-scp-cache-5f4f7f8476-ffsbp                    2/2   Running
0           15h
cicdocscp-scp-load-manager-5d6f776f5d-rjhkp             2/2   Running
0           15h
cicdocscp-scp-mediation-844d4f9c47-94ksm                2/2   Running
0           15h
cicdocscp-scp-nrfproxy-6cfcb66b49-kcvdm                 2/2   Running
0           15h
cicdocscp-scp-nrfproxy-oauth-74844b8f85-928st           2/2   Running
0           15h
cicdocscp-scp-worker-557c6bf4fc-z4s7s                   2/2   Running
1           15h
cicdocscp-scpc-alternate-resolution-8845f5d98-k7q9l     2/2   Running
0           15h
cicdocscp-scpc-audit-7b856c5bd5-dlc78                   2/2   Running
0           15h
cicdocscp-scpc-configuration-774845fb49-6qn88           2/2   Running
0           15h
cicdocscp-scpc-notification-5d68d7d998-9xbhl            2/2   Running
0           9h
cicdocscp-scpc-subscription-6d446749ff-v84gf            2/2   Running
0           15h
cncc-acore-ingress-gateway-7545797b4f-w488t             2/2   Running
0           46m
cncc-iam-ingress-gateway-8449f57d48-xd8gw               2/2   Running
0           46m
cncc-iam-kc-0                                           3/3   Running
0           46m
cncc-mcore-cmservice-6786679cc4-9v54w                   2/2   Running
0           46m
cncc-mcore-ingress-gateway-546fb4f79c-6dv62             2/2   Running
0           40m
mysql-cluster-db-backup-manager-svc-6cc6fc5fc7-287wq    1/1   Running
0           11m
mysql-cluster-db-monitor-svc-d47766d56-rz956            1/1   Running
0           12m
ndbappmysqld-0                                          3/3   Running
0           12m
ndbappmysqld-1                                          3/3   Running
0           12m
ndbmgmd-0                                               2/2   Running
```

```
0          13m
ndbmgmd-1                                                 2/2   Running
0          13m
ndbmtd-0                                                  3/3   Running
0          13m
ndbmtd-1                                                  3/3   Running
0          13m
ndbmtd-2                                                  3/3   Running
0          13m
ndbmtd-3                                                  3/3   Running
0          13m
ndbmysqld-0                                               4/4   Running
0          12m
ndbmysqld-1                                               4/4   Running
0          12m
ndbmysqld-2                                               4/4   Running
0          12m
ndbmysqld-3                                               4/4   Running
0          12m
```

10. Run the following command to perform Helm test to check the state of the deployments:

    ```
    helm test ocscp -n  <scp-namespace> --logs
    ```

    No error logs should be present in the output of this command.

11. Divert the traffic back to this SCP site.

5
Rolling Back SCP

You can roll back SCP from a target release to any supported source release using procedures outlined in this chapter.

5.1 Supported Rollback Paths

The following table lists the supported rollback paths for SCP:

Table 5-1 SCP Supported Rollback Paths

Source Release	Target Release
25.2.201	25.1.2xx
25.2.201	25.2.1xx

5.2 Rollback Tasks

To roll back from SCP 25.2.201 to a previous version:

Note

- SCP might raise alerts while performing rollback. To clear any alert, see "Alerts" in *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*.
- SCP uses the `upgraderollbackevents` resource to retrieve the list of upgrade and rollback events. For more information, see "Fetching Upgrade and Rollback Events" in *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.
- A timeout interval of 30 minutes is set while performing rollback because only one instance of scp-worker is rolled back at a time.
- Ensure that no SCP pod is in the failed state.
- While performing the rollback, you may observe some deviation in SCP traffic processing rate for some of the data plane services, such as SCP-Worker, SCP-nrfProxy, SCP-Mediation, and so on, on Grafana as the pods are scaling down and scaling up. To verify whether there is any actual traffic deviation, it is recommended to check the traffic rate for the same time duration at the consumer NF's side.
- The SCP-Load-Manager and SCP-Cache pods running on the target release will re-spin as part of the postrollback hooks.

1. To obtain the release number to which SCP has to be rolled back, check the revision by running the following command:

   ```
   helm history <release_name> --namespace <release_namespace
   ```

   Where,

   - `<release_name>` is the release name used by the Helm command.
   - `<release_namespace>` is the SCP release name, for example, ocscp.

   Example:

   ```
   helm history ocscp --namespace ocscp
   ```

2. Rollback to the required revision:

   ```
   helm rollback <release_name> <revision_number> --namespace
   <release_namespace> --timeout=30m
   ```

   Where, `<revision_number>` is the release number which SCP can be rolled back to.

   Example:

   ```
   helm rollback ocscp 1 --namespace ocscp --timeout=30m
   ```

3. If the rollback fails, see *Oracle Communications Cloud Native Core, Service Communication Proxy Troubleshooting Guide*.

> **Note**
>
> You must clean up any residual job from the SCP deployment after the rollback is complete.

5.3 Postrollback 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 SCP, then accordingly, if any update is required, individual service APIs defined for different resources can be used to reconfigure the data backup taken before the upgrade.

For information about REST APIs, see *Oracle Communications Cloud Native Core, Service Communication Proxy REST Specification Guide*.

6
Uninstalling SCP

This chapter provides information about uninstalling SCP.

6.1 Uninstalling SCP Using Helm

To uninstall SCP using Helm, perform the following procedure on a server that has access to Kubectl and Helm commands.

1. To uninstall SCP, run the following command:

   ```
   helm uninstall <release_name> --namespace <namespace>
   ```

   Where, `<release_name>` is a name provided by the user to identify the Helm deployment.

   Helm keeps a record of its releases, so you can still reactivate the release after uninstalling it.

   Example:

   ```
   helm uninstall ocscp --namespace scp
   ```

> **Note**
>
> By default, SCP uses Helm 3.

6.2 Deleting Kubernetes Namespace

This section describes how to delete Kubernetes namespace where SCP is deployed.
To delete kubernetes namespace, run the following command:

```
kubectl delete namespace <release_namespace>
```

Where, `<release_namespace>` is the deployment namespace used by the Helm command.

Example:

```
kubectl delete namespace ocscp
```

6.3 Removing Database Users

This section describes how to remove MySQL users.
To remove MySQL users while uninstalling SCP, run the following commands:

Remove Privileged User:

```
DROP USER IF EXISTS <SCP Privileged-User Name>;
```

Example:

```
DROP USER IF EXISTS scpprivilegedusr';
```

Remove Application User:

```
DROP USER IF EXISTS <SCP Application User Name>;
```

Example:

```
DROP USER IF EXISTS scpusr;
```

> ⚠ **Caution**
>
> Removal of users must be done on all the SQL nodes for all SCP sites.

6.4 Removing the Application and Backup Database

This section describes how to remove the application and backup database.
Run the following commands to remove the application and backup database:

- For application database:

  ```
  DROP DATABASE <scp_dbname>;
  ```

  Example:

  ```
  DROP DATABASE ocscpdb;
  ```

- For backup database:

  ```
  DROP DATABASE <scp_backupdbname>;
  ```

  Example:

  ```
  DROP DATABASE ocscpbackupdb;
  ```

7 Fault Recovery

This chapter provides information about fault recovery for Oracle Communications Cloud Native Core, Service Communication Proxy (SCP) deployment.

7.1 Overview

You must take database backup and restore it either on the same or a different cluster. It uses the SCP database to run any command or follow instructions.

> **Note**
>
> This document describes recovery procedures to restore SCP completely or partially.

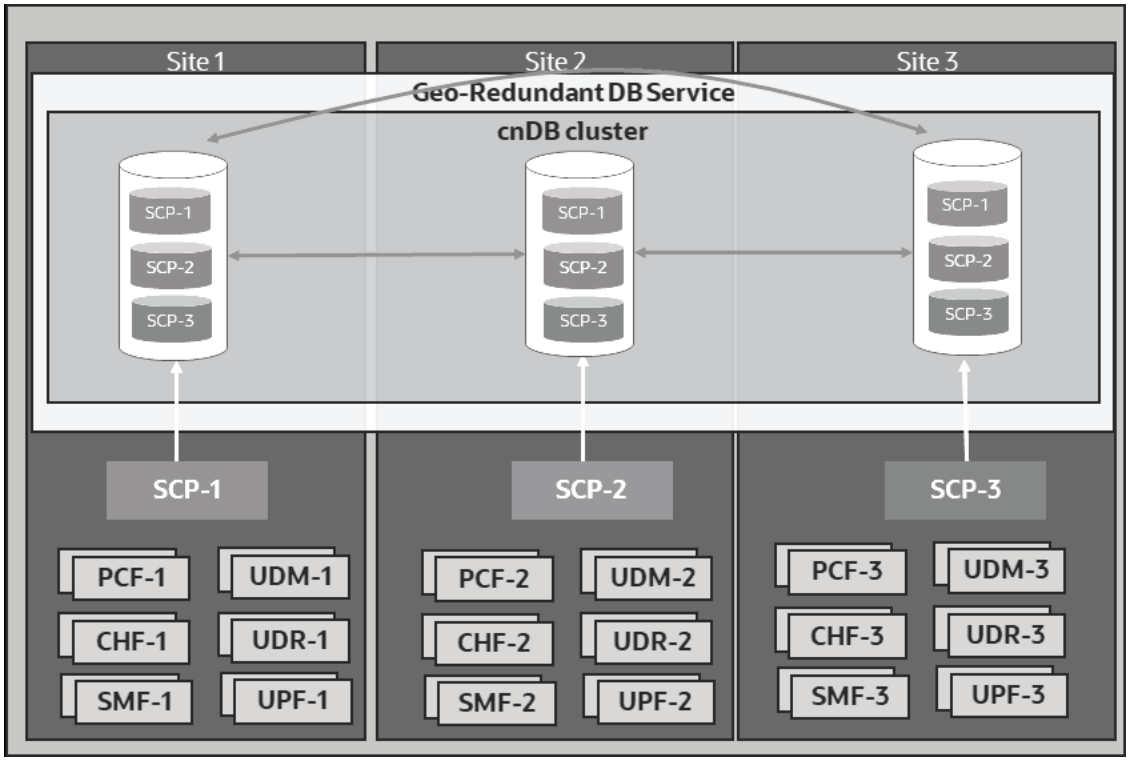
Database Model of SCP

The SCP database consists of the following:

- Configuration Data: The configuration data is exclusive for a given SCP instance. Therefore, an exclusive logical database is created and used by an SCP instance to store its configuration data. You can configure SCP instance specific configurations using RESTful config API exposed by scpc-configuration service through the Oracle Communications Cloud Native Configuration Console (CNC Console).
- Routing Data: This is the routing rules data that SCP determines from Network Repository Function (NRF) in 5G Core network topology.
- Status Data: This data provides the status of upgrade or rollback.

The following image shows SCP database model in three different sites.

Figure 7-1 Database Model



This image represents how each SCP instance is using it's dedicated database. The data is getting replicated to all other sites of the cnDBTier cluster so that the data is available on all the cnDBTier cluster sites in case of a cnDBTier instance failure.

> **Note**
>
> To recover cnDBTier through automated backup file or on-demand backup from mate site, see the restore procedure in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

7.2 Impacted Areas

The following table shares information about the impacted areas during SCP fault recovery:

Table 7-1 Impacted Areas

Scenario	Requires Fault Recovery or Reinstallation of CNE	Requires Fault Recovery or Reinstallation of cnDBTier	Requires Fault Recovery or Reinstallation of SCP	Requires SCP Service Restart
Scenario 1: Recovering SCP (SCP services) when its deployment corrupts	No	No	Yes	NA
Scenario 2: Recovering corrupted cnDBTier	No	Yes	No, use Helm upgrade of the same SCP version to update the SCP configuration if required. For example, change in cnDBTier service information, such as cnDB endpoints, DB credentials, and so on.	Requires SCPC-Configuration service restart by using the `kubectl delete <scpc-configuration pod> -n <namespace>` command.
Scenario 3: Recovering corrupted SCP configuration and routing database	No	No	No	Requires SCPC-Configuration service restart by using the `kubectl delete <scpc-configuration pod> -n <namespace>` command.
Scenario 4: Complete site failure due to infrastructure failure, for example, hardware, CNE, and so on.	Yes	Yes	Yes	NA

7.3 Prerequisites

Before performing any fault recovery procedure, ensure that the following prerequisites are met:

- cnDBTier must be in a healthy state and available on multiple sites along with SCP. If cnDBTier is unhealthy, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*
- Automatic backup must be enabled on cnDBTier. Scheduled regular backups help to:
  - Restore stable version of the SCP database
  - Minimize significant loss of data due to upgrade or rollback failure
  - Minimize loss of data due to system failure

  - Minimize loss of data due to data corruption or deletion due to external input
  - Migrate the SCP database information from one site to another
- Docker images used during the last installation or upgrade must be retained in the external data source.
- Custom values file used at the time of SCP deployment is retained. If the `custom_values.yaml` file is not retained, then regenerate it manually. This task increases the overall fault recovery time.

> **Note**
>
> Do not change DB Secret or cnDBTier MySQL FQDN or IP or PORT configurations.

7.4 Fault Recovery Scenarios

This section describes the fault recovery procedures for various scenarios.

7.4.1 Deployment Failure

Perform this procedure to recover SCP when its deployment corrupts.
Restore SCP as described in Restoring SCP.

7.4.2 cnDBTier Corruption

This section describes how to recover cnDBTier from the corrupted database.
When the database corrupts, the database on all other sites may corrupt due to data replication. It depends on the replication status after the corruption has occurred.

If the data replication is interrupted due to database corruption, then cnDBTier fails in either single or multiple sites, not all the sites. If the data replication is successful, then database corruption replicates to all the cnDBTier sites and cnDBTier fails in all the sites.

To recover cnDBTier when cnDBTier corrupts in single, multiple, or all sites, see *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

> **Note**
>
> When cnDBTier is restored, restart the SCPC-Configuration service by running the following command:
>
> ```
> kubectl delete <scpc-configuration pod> -n <namespace>
> ```

7.4.3 SCP Data Corruption

Perform this procedure to recover SCP configuration and routing database (DB) from the corrupted database.

Take a backup of the SCP database (DB) and restore the database on a different Network Database (NDB) cluster. This procedure is for on-demand backup and restore of SCP DB. The commands used for these procedures are provided by the MySQL NDB cluster.

Ensure that the MySQL NDB cluster is in a healthy state, and each database node of it should 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 scpsvc 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 ~]$
```

1. If the SCP database backup is required, do the following:
   a. 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.

   b. Enter the SCP database name and password in the command when prompted.

Example:

```
kubectl exec -it ndbmysqld-0 -n scpsvc bash
mysqldump --quick -h127.0.0.1 -uSCPuser -p SCPdb | gzip >
SCPdbBackup.sql.gz
```

> **Note**
>
> Ensure that there is enough space on the directory to save the backup file.

2. If the SCP database restore is required, do the following:
   a. Transfer the `<backup_ filename>.sql.gz` file to the SQL node where you want to restore it.
   b. 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.
   c. Create database, database user, and grant permissions as described in Configuring Database for SCP.

   > **Note**
   >
   > The database name created in this step should be the same as the database name created in the next substep. Also, the Kubernetes secret should be the same as in the `values.yaml` file used for installing SCP.

   d. 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 < SCPdbBackup.sql.gz | mysql -h127.0.0.1 -uSCPuser -p newSCPdb
   ```

   e. Enter the password when prompted.
   f. Restart the SCPC-Configuration service by running the following command:

   ```
   kubectl delete <scpc-configuration pod> -n <namespace>
   ```

7.4.4 Single or Multiple Site Failure

This section describes how to perform fault recovery when either one, many, or all of the sites have 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

When both cnDBTier and SCP are installed on multiple sites with automatic data replication and backup enabled. It is observed that one or more sites, not all of them, have failed and there is a requirement to perform fault recovery.

1. Install a new Kubernetes cluster by performing the Cloud Native Environment (CNE) installation procedure as described in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
2. Install cnDBTier as described in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
3. Perform cnDBTier fault recovery procedure to take data backup from an older site and restore it to a new site.

   For more information about cnDBTier backup, see "Create On-demand Database Backup" and to restore the database to a new site, see "Restore DB with Backup" in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
4. Restore SCP as described in Restoring SCP.

7.4.4.2 All Sites Failure

When both cnDBTier and SCP are installed on multiple sites with automatic data replication and backup enabled. It is observed that all the sites have failed and there is a requirement to perform fault recovery.

1. Install a new Kubernetes cluster by performing the Cloud Native Environment (CNE) installation procedure as described in *Oracle Communications Cloud Native Core, Cloud Native Environment Installation, Upgrade, and Fault Recovery Guide*.
2. Install cnDBTier as described in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
3. To perform cnDBTier fault recovery, restore the latest backed up data as described in *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide*.
4. Restore SCP as described in Restoring SCP.

A
ASM Configuration

In the current release 25.2.201, the "cluster.service" and "type" fields are added as a part of ASM Envoy Filter configuration enhancements.

The following list includes the Custom Resource Definitions (CRDs) with supported fields:

- Service Entry:
  - hosts
  - exportTo
  - addresses
  - ports.name
  - ports.number
  - ports.protocol
  - resolution
- Destination Rule:
  - host
  - mode
  - sbitimers
  - tcpConnectTimeout
  - tcpKeepAliveProbes
  - tcpKeepAliveTime
  - tcpKeepAliveInterval
- Envoy Filter:
  - labelselector
  - applyTo
  - filtername
  - operation
  - typeconfig
  - configkey
  - configvalue
  - stream_idle_timeout
  - max_stream_duration
  - patchContext
  - networkFilter_listener_port
  - transport_socket_connect_timeout
  - filterChain_listener_port

  - route_idle_timeout
  - route_max_stream_duration
  - httpRoute_routeConfiguration_port
  - vhostname
  - cluster.service
  - type
- Peer Authentication:
  - labelselector
  - tlsmode
- Virtual Service:
  - host
  - destinationhost
  - port
  - exportTo
  - retryon
  - timeout
- Request Authentication:
  - labelselector
  - issuer
  - jwks/jwksUri
- Policy Authorization:
  - labelselector
  - action
  - hosts
  - paths
  - xfccvalues

> **Note**
>
> - For virtual service CRD, when the destinationhost is any SCP microservice, do not configure the timeout value.
> - For details of these CRDs and parameters, see the Configuring SCP to Support Aspen Service Mesh section.

B
Restoring SCP

Perform this procedure to restore SCP when SCP deployment is corrupted.

Take a backup of the following:

- The `custom_values.yaml` file that was used for installing SCP.
- The SCP database and restore the database as described in SCP Data Corruption. Perform the SCP database backup daily or when there is any network change.

1. Run the following command to uninstall the corrupted SCP deployment:

   ```
   helm uninstall <release_name> --namespace <namespace>
   ```

   Where,

   - `<release_name>` is a name used to track this installation instance.
   - `<namespace>` is the namespace of SCP deployment.

   Example:

   ```
   helm uninstall ocscp --namespace scpsvc
   ```

2. Install SCP using the backed up copy of the `custom_values.yaml` file.

   For information about installing SCP using Helm, see Installation Tasks.

3. To verify whether SCP installation is complete, see Postinstallation Tasks.

C

PodDisruptionBudget Kubernetes Resource

PodDisruptionBudget (PDB) is a Kubernetes resource. It helps to achieve the high availability of scalable application services in voluntary disruptions performed by cluster administrators to manage the cluster nodes. PDB can be defined for highly available and scalable SCP services such as scp-worker, scp-cache, and scp-nrfproxy microservices. PDB restricts the number of pods of a highly available and scalable application that are down simultaneously from voluntary disruptions.

PDB allows safe eviction of pods when a Kubernetes node is drained of pods to perform maintenance on the node. SCP uses the default value of `maxPdbUnavailable` parameter specified in the Helm chart to 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.

> **Note**
>
> The performance and capacity of the SCP system may vary based on the call model, feature or interface configuration, network conditions, and underlying CNE and hardware environment.

For more information about this functionality, see https://kubernetes.io/docs/concepts/workloads/pods/disruptions/#pod-disruption-budgets.

The following table provides information about PDB values of different SCP microservices.

Table C-1 Default PodDisruptionBudget for SCP Deployment

Microservice	Default PodDisruptionBudget	PodDisruptionBudget Supported
scpc-subscription	NA	No It is a single pod instance service. PDB is not recommended for single pod instance services because it may not help for service availability and manual intervention is not accepted by defining PDB maxPdbUnavailable=0.
scpc-notification	NA	No It is a single pod instance service. PDB is not recommended for single pod instance services because it may not help for service availability and manual intervention is not accepted by defining PDB maxPdbUnavailable=0.

Table C-1 (Cont.) Default PodDisruptionBudget for SCP Deployment

Microservice	Default PodDisruptionBudget	PodDisruptionBudget Supported
scpc-audit	NA	No It is a single pod instance service. PDB is not recommended for single pod instance services because it may not help for service availability and manual intervention is not accepted by defining PDB maxPdbUnavailable=0.
scpc-configuration	NA	No It is a single pod instance service. PDB is not recommended for single pod instance services because it may not help for service availability and manual intervention is not accepted by defining PDB maxPdbUnavailable=0.
scpc-alternate-resolution	NA	No It is a single pod instance service. PDB is not recommended for single pod instance services because it may not help for service availability and manual intervention is not accepted by defining PDB maxPdbUnavailable=0.
scp-cache	maxPdbUnavailable is 1	Yes To have uninterrupted service during voluntary disruptions in the Kubernetes cluster.
scp-nrfproxy	maxPdbUnavailable is 25%	Yes To have uninterrupted service during voluntary disruptions in the Kubernetes cluster.
scp-worker	maxPdbUnavailable is 25%	Yes To have uninterrupted service during voluntary disruptions in the Kubernetes cluster.
scp-load-manager	maxPdbUnavailable is 1	Yes To have uninterrupted service during voluntary disruptions in the Kubernetes cluster.
scp-mediation	maxPdbUnavailable is 25%	Yes To have uninterrupted service during voluntary disruptions in the Kubernetes cluster.
scp-nrfProxy-oauth	maxPdbUnavailable is 25%	Yes To have uninterrupted service during voluntary disruptions in the Kubernetes cluster.

maxPdbUnavailable indicates how many pods are allowed for eviction.

D
SCP Traffic IP Flow

This section describes the Internet Protocol (IP) flow between the IP services.

Table D-1 SCP Traffic IP Flow of SCP-Worker (SCP Data Plane)

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
Peer 5G Network Function	F5 Service Proxy	8000/9443	Load Balancer	External	IPv4	Yes
F5 Service Proxy	SCP-W Pods	8080	Container Target Port	Internal	IPv4	Yes
SCPC-Subscription	SCP-W Pods (Service fqdn)	8000/8080	Service Port or Container Target Port	Internal	IPv4	Yes
SCPC-Audit	SCP-W Pods (Service fqdn)	8000/8080	Service Port or Container Target Port	Internal	IPv4	Yes
Prometheus	SCP-W Pods	8091	Container Target Port	Internal	IPv4	Yes
SCP-Worker	Peer 5G NF	Peer NF port	Load balancer port	External	IPv4	Yes
Kubelet (readiness)	SCP-W Pods	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (liveness)	SCP-W Pods	8091	Container Target Port	Internal	IPv4	Yes
SCPC-Configuration	SCP-W Pods (Service fqdn)	8080	Container Target Port	Internal	IPv4	Yes
SCP-Worker Coherence	SCP-Worker/SCP-Cache Coherence	8095/8096	Container Target Port	Internal	IPv4	No
Operator/ User	SCP Worker Coherence Mgmt	9000/30000	Service Port or Container Target Port	Internal	IPv4	Yes
SCP-Worker	SCP-Nrfproxy	8086	Container Target Port	Internal	IPv4	Yes
SCP-Nrfproxy	SCP-Worker	8000	Container Target Port	Internal	IPv4	Yes
SCP-Worker	scp-mediation	9090/30081	Service Port or Container Target Port	Internal	IPv4	No
SCP-Worker	scp-nrfproxy-oauth	8040	Container target port	Internal	IPv4	Yes
SCP-Worker	SCPC-Configuration	8092	Container target port	Internal	IPv4	No

Table D-1 (Cont.) SCP Traffic IP Flow of SCP-Worker (SCP Data Plane)

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCP-Worker	SCPC-Notification	8092	Container target port	Internal	IPv4	No
SCP-Worker	SCPC-Audit	8092	Container target port	Internal	IPv4	No

Table D-2 SCP Traffic IP Flow SCP Control plane SCPC- Configuration

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
Operator/ User	F5 Service Proxy	443	Load Balance Port	External	IPv4	Yes
F5 Service Proxy	CNCC Ingress API GW Pods	8081	Container Target Port	Internal	IPv4	Yes
CNCC	SCP Configuration Pod	8081/8081	Internal Service Port / Container Target Port	Internal	IPv4	Yes
Prometheus	SCPC-Config Pods	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (readiness)	SCPC-Config Pods	8091	Container Target Port	Internal	IPv4	Yes
SCPC-Configuration	Kubenetes API server	API Server Port	Kube API Server Ports	Infrastructure	IPv4	Yes
SCPC-Configuration	DB service	3306	Container Target Port	External	IPv4	Yes
SCPC-Configuration	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No
SCPC-Configuration	SCPC-Alternate-Resolution	8092	Container Target Port	Internal	IPv4	No

Table D-3 SCP Traffic IP Flow SCP Control plane SCPC- Subscription

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCPC-Subscription	SCP-W Pods (Service fqdn)	8000/8080	Service Port / Container Target Port	Internal	IPv4	Yes

Table D-3 (Cont.) SCP Traffic IP Flow SCP Control plane SCPC- Subscription

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCPC-Subscription	Kubenetes API server	API Server Port	Kube API Server Ports	Infrastructure	IPv4	Yes
SCPC-Subscription	DB service	3306	Container Target Port	External	IPv4	Yes
Prometheus	SCPC-Subscription Pod	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (readiness)	SCPC-Subscription Pod	8091	Container Target Port	Internal	IPv4	Yes
SCPC-Configuration	SCPC-Subscription Pod	8080	Container Target Port	Internal	IPv4	Yes
SCPC-Subscription	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No

Table D-4 SCP Control plane SCPC- Notification

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
NRF	F5 Service Proxy (SCP - Worker svc)	8000	Load Balancer	External	IPv4	Yes
F5 Service Proxy (SCP-Worker svc)	SCP-W Pods	8080	Container Target Port	Internal	IPv4	Yes
SCP-W Pods	SCP-Notificaton Service/ Pods	8082/8082	Internal Service Port / Container Target Port	Internal	IPv4	Yes
SCPC-Configuration	SCP-Notificaton Service/ Pods	8082/8082	Internal Service Port / Container Target Port	Internal	IPv4	Yes
SCPC-Audit	SCP-Notificaton Service/ Pods	8082/8082	Internal Service Port / Container Target Port	Internal	IPv4	Yes
Prometheus	SCP-Notificaton Pods	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (readiness)	SCP-Notificaton Pods	8091	Container Target Port	Internal	IPv4	Yes
SCPC-Notification	Kubenetes API server	API Server Port	Kube API Server Ports	Infrastructure	IPv4	Yes

Table D-4 (Cont.) SCP Control plane SCPC- Notification

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCPC-Notification	DB service	3306	Container Target Port	External	IPv4	Yes
SCPC-Configuration	SCP-Notificaton	8082	Container Target Port	Internal	IPv4	Yes
SCPC-Notification Coherence	SCPC-Notification/SCP-Cache Coherence	8095/8096	Container Target Port	Internal	IPv4	No
SCPC-Notification	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No

Table D-5 SCP Control plane SCPC-Audit

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCPC-Configuration	SCP Audit Service/Pods	8083/8083	Internal Service Port / Container Target Port	Internal	IPv4	Yes
SCPC-Audit	SCP-W Pods (Service fqdn)	8000/8080	service Port/ Container Target Port	Internal	IPv4	Yes
Prometheus	SCPC-Audit Pods	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (readiness)	SCPC-Audit Pods	8091	Container Target Port	Internal	IPv4	Yes
SCPC-Audit	Kubenetes API server	API Server Port	Kube API Server Ports	Infrastructure	IPv4	Yes
SCPC-Audit	DB service	3306	Container Target Port	External	IPv4	Yes
SCPC-Alternate-Resolution	SCP Audit Service/Pods	8083/8083	Internal Service Port / Container Target Port	Internal	IPv4	Yes
SCPC-Audit	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No
SCPC-Audit	SCPC-Notification	8092	Container Target Port	Internal	IPv4	No

Table D-6 SCP Control plane SCPC-Alternate- Resolution

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCPC-Configuration	SCPC-Alternate-Resolution Service/Pods	8084/8084	Internal Service Port / Container target port	Internal	IPv4	Yes
SCPC-Notification	SCPC-Alternate-Resolution Service/Pods	8084/8084	Internal Service Port / Container Target Port	Internal	IPv4	Yes
SCPC-Audit	SCPC-Alternate-Resolution Service/Pods	8084/8084	Internal Service Port / Container Target Port	Internal	IPv4	Yes
Prometheus	SCPC-Alternate-Resolution Pods	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (readiness)	SCPC-Alternate-Resolution Pods	8091	Container Target Port	Internal	IPv4	Yes
SCPC-Alternate-Resolution	DB service	3306	Container Target Port	Infrastructure	IPv4	Yes
SCPC-Alternate-Resolution	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No

Table D-7 SCP-Cache (SCP Data Plane)

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCPC-Configuration	SCP-Cache Service/Pods	8010/8010	Service Port / Container Target Port	Internal	IPv4	Yes
Prometheus	SCP-Cache Pods	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (readiness)	SCP-Cache Pods	8091	Container Target Port	Internal	IPv4	Yes
SCP-Cache Coherence	SCP-Worker/SCP-Cache Coherence	8095/8096	Container Target Port	Internal	IPv4	Yes
Operator/ User	SCP Cache Coherence Mgmt	9000/30000	Service Port / Container Target Port	Internal	IPv4	Yes
SCP-Cache Coherence Federation	SCP Cache Coherence Federation	30001/30001	Service Port / Container Target Port	External	IPv4	Yes

Table D-7 (Cont.) SCP-Cache (SCP Data Plane)

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCP-Cache	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No

Table D-8 SCP-Nrfproxy (SCP Data Plane)

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCP-Nrfproxy	SCPC-Configuration	8081	Container Target Port	Internal	IPv4	Yes
Prometheus	SCP-Nrfpfoxy Pods	8091	Container Target Port	Internal	IPv4	Yes
Kubelet (readiness)	SCP-Nrfproxy Pods	8091	Container Target Port	Internal	IPv4	Yes
SCP-Nrfporxy	DB service	3306	Container Target Port	Infrastructure	IPv4	Yes
SCP-Worker	SCP-Nrfproxy	8086	Container Target Port	Internal	IPv4	Yes
SCP-Nrfproxy	SCP-Worker	8000	Container Target Port	Internal	IPv4	Yes
SCP-Nrfproxy	SCP-Worker-int	8092	Container Target Port	Internal	IPv4	Yes
SCP-Nrfproxy	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No

Table D-9 SCP-Mediation and SCP-Data Director (SCP Data Plane)

Flow Description	Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCP-Mediation(SCP Data plane)	SCP-Worker	SCP-Mediation	9090/30081	Service Port / Container Target Port	Internal	IPv4	No
SCP-Data Director(SCP Data plane)	SCP-Worker	OCNADD	OCNADD Port	Service Port / Container Target Port	External	IPv4	No

Table D-10 SCP-load-manager

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
scp-worker coherence	SCP-Worker/scp-load-manager coherence	8095/8096	Container Target Port	Internal	IPv4	No
scp-load-manager	SCPC-Notification	8082	Container Target Port	Internal	IPv4	Yes
scp-load-manager	SCPC-Configuration	8081	Container Target Port	Internal	IPv4	Yes
scp-load-manager	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No
scp-load-manager	SCPC-Notification	8092	Container Target Port	Internal	IPv4	No

Table D-11 SCP-Nrfproxy-Oauth (SCP Data Plane)

Source Node	Destination Node	Destination Port	Type of Port	Nature of Port	IP Protocol Version	Service Mesh Included(No means excluded from SM)
SCP-Nrfproxy-Oauth	SCPC-Configuration	8081	Container Target Port	Internal	IPv4	Yes
Prometheus	SCP-Nrfproxy-Oauth Pods	8091	Container Target Port	Internal	IPv4	Yes
kubelet (readiness)	SCP-Nrfproxy-Oauth Pods	8091	Container Target Port	Internal	IPv4	Yes
SCP-Worker	SCP-Nrfproxy-Oauth	8040	Container Target Port	Internal	IPv4	Yes
SCP-Nrfproxy-Oauth	SCP-Worker-int	8092	Container Target Port	Internal	IPv4	Yes
SCP-Nrfproxy-Oauth	coherence	8095/8096	Container Target Port	Internal	IPv4	No
SCP-Nrfproxy-Oauth	SCPC-Configuration	8092	Container Target Port	Internal	IPv4	No

SCP Microservices Port Information

The following table lists the port used by SCP microservices.

Table D-12 SCP Microservices Port Information

Service	Application Container Listen Port	Type of Port	Service Mesh Included(No means excluded from SM)
SCP-Worker (SCP Data plane)	8080	Container Target Port	Yes
	8091	Container Target Port	Yes
	8095/8096	Container Target Port	No
	9000/30000	Service Port/Container Target Port	Yes
	9443	Container Target Port	No
scp-worker-int	8092	Container Target Port	No
SCP Control plane SCPC-Configuration	8081	Internal Service Port / Container Target Port	Yes
	8091	Container Target Port	Yes
scpc-configuration-int	8092	Container Target Port	No
SCP Control plane SCPC-Subscription	8091	Container Target Port	Yes
	8080	Container Target Port	Yes
SCP Control plane SCPC-Notification	8082	Container Target Port	Yes
	8091	Container Target Port	Yes
scpc-notification-int	8092	Container Target Port	No
SCP Control plane SCPC-Audit	8083	Container Target Port	Yes
	8091	Container Target Port	Yes
scpc-audit-int	8092	Container Target Port	No
SCP Control plane SCPC-Alternate-Resolution	8084	Container Target Port	Yes
	8091	Container Target Port	Yes
scpc-alternate-resolution-int	8092	Container Target Port	No
SCP-Cache (SCP Data plane)	8010	Container Target Port	Yes
	8091	Container Target Port	Yes
	8095/8096	Container Target Port	No
	9000/30000	Service Port / Container Target Port	Yes
SCP-Nrfproxy (SCP Data plane)	8086	Container Target Port	Yes
	8091	Container Target Port	Yes
SCP-Mediation(SCP Data Plane)	9090/30081	Service Port/Container Target Port	No
SCP-Load-Manager (SCP Data plane)	8091	Container Target Port	Yes
	8095/8096	Container Target Port	No
	9000/30000	Service Port/Container Target Port	Yes
SCP-Nrfproxy-Oauth (SCP Data plane)	8081	container target Port	Yes
	8091	container target Port	Yes
	8091	container target Port	Yes
	8040	container target Port	Yes
	8000	container target Port	Yes
	8095/8096	container target Port	No