Oracle® Communications

Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide

Release 24.1.1
F90670-02
December 2024

Oracle Communications Cloud Native Configuration Console Installation, Upgrade, and Fault Recovery Guide, Release 24.1.1

F90670-02

Contents

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:

1. Select **2** for New Service Request.
2. Select **3** for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
   - 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**.

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 provides information about the acronyms and terminologies used in the document:

Table Acronyms

Acronym	Definition
AD	Active Directory
ASM	Aspen Service Mesh
BSF	Oracle Communications Cloud Native Core, Binding Support Function
cnDBTier	Oracle Communications Cloud Native Core, cnDBTier
CNC Console	Oracle Communications Cloud Native Configuration Console
CNE	Oracle Communications Cloud Native Core, Cloud Native Environment
CS	Common Service
CRUD Operations	CREATE, READ, UPDATE, DELETE
OCNADD	Oracle Communications Network Analytics Data Director
ECDSA	Elliptic Curve Digital Signature Algorithm
EIR	Equipment Identity Register
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity Access Management
KPI	Key Performance Indicator
M-CNCC	Manager CNC Console or mCncc is a CNC Console instance which manages multiple A-CNCC and local instances. **Non OCI**: M-CNCC has two components M-CNCC IAM and M-CNCC Core **OCI**: M-CNCC has only M-CNCC Core component. M-CNCC IAM is substituted with OCI IAM.
M-CNCC IAM	Manager CNC Console IAM or M-CNCC IAM (also known as mCncc Iam) is an IAM component of M-CNCC. M-CNCC IAM contains M-CNCC IAM Ingress Gateway and M-CNCC IAM back-end microservices.
M-CNCC Core	Manager CNC Console Core or M-CNCC Core (also known as mCncc Core) is a core component of M-CNCC that provides GUI and API access portal for accessing NF and OCCNE common services. M-CNCC Core contains M-CNCC Core Ingress Gateway and M-CNCC Core back-end microservices.
A-CNCC Core	Agent CNC Console is a CNCC Core instance which manages local NF(s) and local OCCNE common services(s). A-CNCC is managed by M-CNCC. A-CNCC contains A-CNCC Core Ingress Gateway. A-CNCC has no IAM component. A-CNCC is also known as A-CNCC Core or aCncc Core.

Table (Cont.) Acronyms

Acronym	Definition
M-CNCC Kubernetes cluster	Kubernetes cluster hosting M-CNCC
mTLS	Mutual Transport Layer Security
OCNWDAF	Oracle Communications Networks Data Analytics Function
Instance	NF or CNE common service managed by either M-CNCC Core or A-CNCC Core.
Site	Kubernetes Cluster
CS	CNE Common Services like Grafana, Kibana, Jaeger, Prometheus, Alertmanager and so on.
MC	Multi Cluster. In multi cluster, a single CNCC can manage NF instances that accessess different Kubernetes clusters.
MO	Mananged Objects
MOS	My Oracle Support
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol (Over SSL)
NRF	Oracle Communications Cloud Native Core, Network Repository Function
OCNF	Oracle Communications Network Function
OSDC	Oracle Software Delivery Cloud
OSO	Oracle Communications Operations Services Overlay
OCI	Oracle Cloud Infrastructure
PROVGW	Provisioning Gateway
REST API	Representational State Transfer Application Programming Interface
SCP	Oracle Communications Cloud Native Core, Service Communication Proxy
SAML	Security Assertion Markup Language
SBA	Service Based Architecture
SEPP	Oracle Communications Cloud Native Core, Security Edge Protection Proxy
TLS	Transport Layer Security
UDR	Oracle Communications Cloud Native Core, Unified Data Repository
UE	User Equipment
URI	Subscriber Location Function
SSO	Single Sign On

What's New in This Guide

Release 24.1.1 - F90670-03, December 2024

- Updated the release number to 24.1.1 in the entire document.
- Added the `cncc-iam.global.iamSettingEnabled` parameter to the CNC Console IAM Configuration Parameters section.
- Added the Configuring M-CNCC IAM to Enable Additional Settings.

This section introduces the documentation updates for Release 24.1.x

Release 24.1.0 - F90670-02, May 2024

- Added a note for support of N-2 NF versions in the CNC Console Compatibility Matrix.

Release 24.1.0 - F90670-01, April 2024

- Updated the following sections with details on CNC Console integration with Oracle Cloud Infrastructure (OCI):
  - Introduction
  - Overview
  - Updated CNC Console Deployment Architecture with the OCI CNC console component overview.
  - Updated the Supported Deployment Models section
  - Added Configuring OCI IAM Secret with the procedure to configure OCI IAM secret.
  - Added a note in the Installing CNC Console Package section with annotations to assign Load-Balancer IP to the CNC Console Services in OCI environment.
  - Added the following parameters in the Global Configuration Options table:
    - global.isMultiClusterDeployment
    - global.oci-iam.enabled
    - global.oci-iam.existingSecret
    - global.oci-iam.existingSecretClientIdKey
    - global.oci-iam.existingSecretClientSecretKey
  - Updated error scenario for error code 1001 in the CNC Console Validation-hook Error Codes section to highlight that only one of the flags among oci-iam, cncc-iam should be enabled at a time.
  - Updated the **CNC Console Instances Configuration Examples** with the `oci-iam : enabled` flag
  - Added a note in the CNC Console Resource Requirement section to highlight that the M-CNCC IAM Resource component is not applicable when CNC Console is deployed on OCI.
  - Added notes for workflow in OCI deployment in the Configuration Workflow section.
  - Added CNC Console Metric Dashboard file for OCI deployment and CNC Console Alert Rules file for OCI deployment in the scripts folder list in the Pushing the Images to Customer Docker Registry section.

  - Added oci-iam enabled column to the CNC Console deployment configurations table in the **Global Configurations** section.
  - Added the Postinstallation Steps for OCI IAM section.
  - Updated the global.mCnccIams.[] attribute in the CNC Console Instances Configuration Options section.
  - Added the Accessing OCI IAM section.
- Updated the cnDBTier Profilesection.
- Added NEF Instance Configuration Examples.
- Added the Support for IPv4 or IPV6 Configuration for CNC Console section.

1 Introduction

This guide describes how to install or upgrade Oracle Communications Cloud Native Configuration Console (CNC Console) in a cloud native environment or Oracle Cloud Infrastructure (OCI), using Continuous Delivery Control Server (CDCS) or Command Line Interface (CLI) procedures. It also includes information on performing fault recovery for CNC Console.

> **Note**
>
> - This guide covers the installation instructions when Podman is the container platform and Helm is 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 accirding to the CNE version of kube-api server.

> **Caution**
>
> User, computer and applications, and character encoding settings may cause issues 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 hyphens, or any special characters are a part of the copied content.

1.1 Overview

CNC Console is a single screen solution to configure and manage Network Functions (NFs). The CNC Console has the following two modules:

- CNC Console Core: CNC Console Core acts as GUI or API portal for NFs and CNE common services. CNC Console Core module includes CNC Console and its integration with other Cloud Native Core network functions. The CNC Console provides user interface that can be used to configure parameters for the following CNC network functions:
  - Oracle Communications Cloud Native Core, Binding Support Function (BSF)
  - Oracle Communications Cloud Native Core, Service Communication Proxy (SCP)
  - Oracle Communications Cloud Native Core, Network Repository Function (NRF)
  - Oracle Communications Cloud Native Core, Network Exposure Function (NEF)
  - Oracle Communications Cloud Native Core, Converged Policy (Policy)
  - Oracle Communications Cloud Native Core, Security Edge Protection Proxy (SEPP)
  - Oracle Communications Cloud Native Core, Unified Data Repository (UDR)

  - CNE Common Services
  - Data Director (DD)
  - Oracle Communications Network Data Analytics Function (NWDAF)
  - Provisioning Gateway (PROVGW)
  - Oracle Communications Cloud Native Core, Certificate Management (OCCM)
- CNC Console Identity Access Management (IAM): CNC Console IAM acts as local identity provider and broker for external identity providers. CNC Console IAM module includes the required authentication and authorization procedures such as creating and assigning roles to users.

Continuous Delivery Control Server (CDCS)

CNC Console can be deployed using Continuous Delivery Control Server (CDCS) or Command Line Interface (CLI) procedures as described in Installing CNC Console. CDCS provides continuous delivery functionality for multisite Cloud Native Core (CNC) installations. For more information about CDCS, see *Oracle Communications CD Control Server User Guide.*

CDCS is a centralized server that automates CNC Console deployment processes such as install, upgrade, and rollback CNC Console. CLI provides an interface to run various commands required to install, upgrade, and roll back CNC Console.

Oracle Cloud Infrastructure (OCI)

OCI is a set of complementary cloud services that enable you to build and run CNC Console in an HA hosted environment with high performance computer capabilities (as physical hardware instances) and storage capacity in a flexible overlay virtual network that is securely accessible from your on-premises network.

> **Note**
>
> **CNC Console on OCI Deployment:**
> The Manager CNC Console IAM Resource component is inconsequential when deploying CNC Console on OCI. Consequently, any sections related to M-CNCC IAM in the installation guide should be ignored.

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

Task	Sub tasks	Reference	Non OCI Environment		OCI Environment
			Applicable for CDCS	Applicable for CLI	Applicable for OCI
Prerequisites: This section describes how to set up the installation environment.		Prerequisites	Yes	Yes	Yes

Task	Sub tasks	Reference	Non OCI Environment		OCI Environment
			Applicable for CDCS	Applicable for CLI	Applicable for OCI
	Software Requirements	Software Requirements	Yes	Yes	Yes
	Environment Setup Requirements	Environment Setup Requirements	Yes	Yes	Yes
	Resource Requirements	Resource Requirements	Yes	Yes	Yes
Downloading CNC Console		Downloading CNC Console package	See Oracle Communications CD Control Server Installation and Upgrade Guide	Yes	Yes
Preinstallation Tasks		Preinstallation Tasks	Yes	Yes	Yes
	Verifying and Creating CNC Console Namespace	Verifying and Creating CNC Console Namespace	Yes	Yes	Yes
	Configuring Database	Configuring Database	Yes	Yes	Yes
	Installing CNC Console	Installing CNC Console			Yes
	Global Configurations	Global Configurations	Yes	Yes	Yes
	OCI IAM Preinstallation Steps	Configuring OCI IAM	No	No	Yes
	CNC Console Configuration for Service Account	CNC Console Configuration for Service Account	Yes	Yes	Yes
	Configuring ASM and OSO in M-CNCC IAM	\Configuring CNC Console to support Aspen Service Mesh	Yes	Yes	No
CNC Console IAM Pre-deployment Configuration		CNC Console IAM Pre-deployment Configuration	Yes	Yes	No
	Configuring M-CNCC IAM Database	Configuring M-CNCC IAM Database	Yes	Yes	No
	Configuring Secret for Default or Admin User in M-CNCC IAM	Configuring Secret for Default or Admin User in M-CNCC IAM	Yes	Yes	No

Task	Sub tasks	Reference	Non OCI Environment		OCI Environment
			Applicable for CDCS	Applicable for CLI	Applicable for OCI
	Configuring OCI IAM Secret	Configuring OCI IAM Secret	Yes	Yes	Yes
	Configuring Secret to Enable HTTPS in M-CNCC IAM	Configuring Secret to Enable HTTPS in M-CNCC IAM	Yes	Yes	No
	Configuring LDAPS in M-CNCC IAM	Configuring LDAPS in M-CNCC IAM	Yes	Yes	No
M-CNCC Core Pre-deployment Configuration		M-CNCC Core Pre-deployment Configuration	Yes	Yes	Yes
	Configuring MySQL in M-CNCC Core	Configuring MySQL in M-CNCC Core	Yes	Yes	Yes
	Configuring Secret to Enable HTTPS in M-CNCC Core	Configuring Secret to Enable HTTPS in M-CNCC Core	Yes	Yes	Yes
A-CNCC Core Pre-deployment Configuration		A-CNCC Core Pre-deployment Configuration	Yes	Yes	Yes
	Configuring Secret to Enable HTTPS in A-CNCC Core	Configuring Secret to Enable HTTPS in A-CNCC Core	Yes	Yes	Yes
	Configuring A-CNCC Core mTLS	Configuring A-CNCC Core mTLS	Yes	Yes	Yes
Deploying CNC Console		Deploying CNC Console	See Oracle Communications CD Control Server Installation and Upgrade Guide	Yes	Yes
	Verifying CNC Console Installation	Verifying CNC Console Installation	Yes	Yes	Yes
Customizing CNC Console		Customizing CNC Console	Yes	Yes	Yes
Accessing CNC Console		Accessing CNC Console	Yes	Yes	Yes
Upgrading CNC Console		Upgrading CNC Console	See Oracle Communications CD Control Server Installation and Upgrade Guide	Yes	Yes

Task	Sub tasks	Reference	Non OCI Environment		OCI Environment
			Applicable for CDCS	Applicable for CLI	Applicable for OCI
Uninstalling CNC Console		Uninstalling CNC Console	Yes	Yes	Yes
CNC Console IAM PostInstallation Steps		CNC Console IAM PostInstallation Steps	Yes	Yes	Yes
Performing Helm Test		Performing Helm Test	Yes	Yes	Yes
Configuring CNC Console to support ASM and OSO		Configuring CNC Console to support ASM and OSO	Yes	Yes	Yes

1.2 CNC Console Compatibility Matrix

This section lists the versions of added or updated components in release 24.1.x. To know the list of all the supported versions, see Oracle Communications Cloud Native Core Release Notes.

Release 24.1.1

There is no change in the compatibility matrix in this release.

Release 24.1.0

The following table lists the versions of added or updated components in release 24.1.0:

Table 1-1 Compatibility Matrix

Network Functions	Compatible Versions
BSF	24.1.x
NRF	24.1.x
NSSF	24.1.x
Policy	24.1.x
SCP	24.1.x
SEPP	24.1.x
UDR	24.1.x
NEF	24.1.x

CNC Console is compatible with the following components:

Table 1-2 Compatibility Matrix

Components	Compatible Versions
OCNADD	24.1.x
CNE	24.1.x, 23.4.x, 23.3.x
cnDBTier	24.1.x, 23.4.x, 23.3.x

Table 1-2 (Cont.) Compatibility Matrix

Components	Compatible Versions
CDCS	23.4.x, 23.3.x, 23.2.x
OSO	23.4.x, 23.3.x, 23.2.x
ASM	1.14.6-am1, 1.11.8-am1, 1.9.8-am1
OCNWDAF	24.1.x
PROVGW	24.1.x
OCCM	24.1.x
OCI Adaptor	24.1.x

1.3 CNC Console Deployment Architecture

Introduction

The CNC Console supports both single and multicluster deployments. In a single cluster deployment, the CNC Console manages NFs and CNE common services deployed in the local Kubernetes clusters. In a multicluster deployment, the CNC Console manages NFs and CNE common services deployed in the remote Kubernetes clusters. This section explains the CNC Console component overview, terminologies used, and CNC Console single Cluster and multicluster deployment details.

CNC Console Component Overview

The following diagram represents the component overview of CNC Console:

Figure 1-1 NON OCI

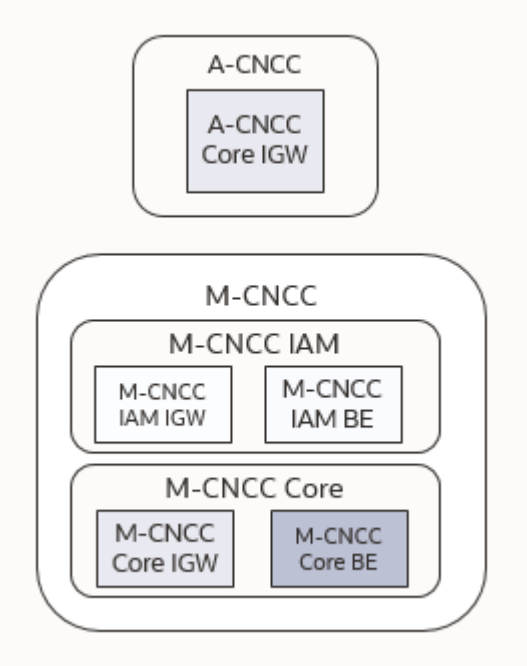
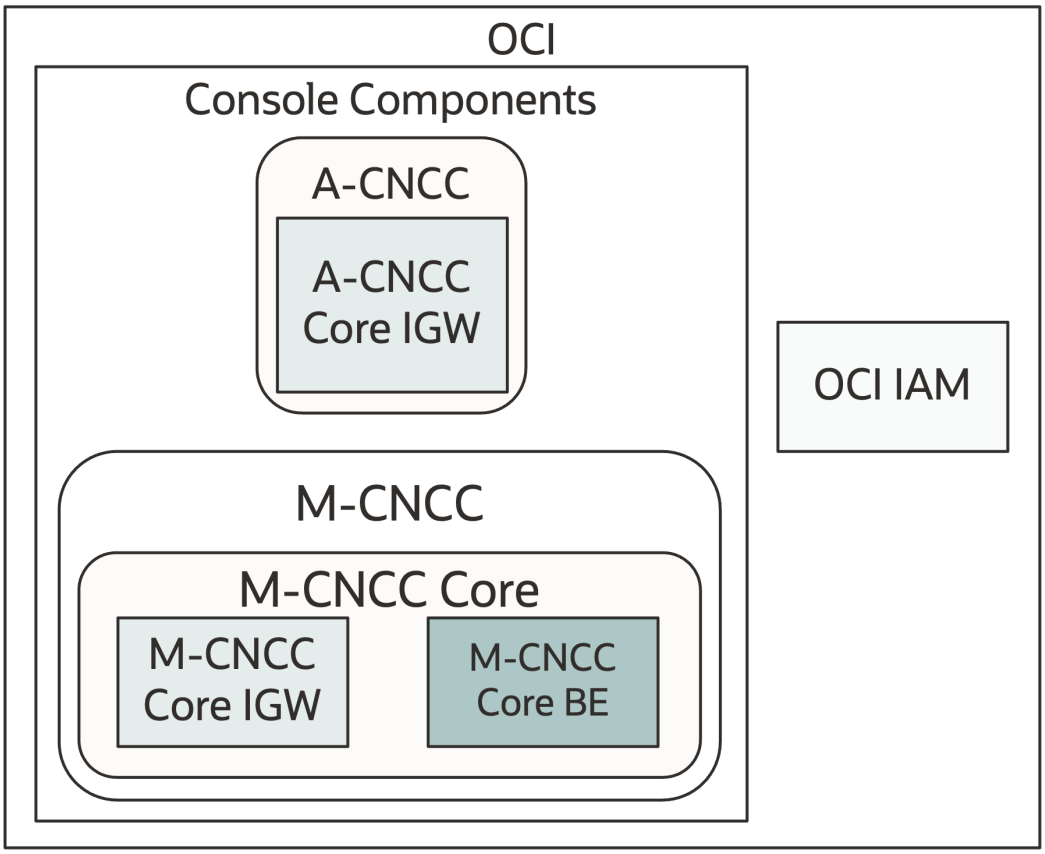


Figure 1-2 OCI



The CNC Console has following two components:

- M-CNCC
- A-CNCC

M-CNCC

Manager CNC Console or M-CNCC is a CNC Console instance which manages multiple A-CNCC and local instances.

For Non OCI:

M-CNCC has two components M-CNCC IAM and M-CNCC Core.

For OCI:

M-CNCC has only M-CNCC Core component. M-CNCC IAM is substituted with OCI IAM.

M-CNCC IAM
Manager CNC Console IAM or M-CNCC IAM is an IAM component of M-CNCC. M-CNCC IAM contains M-CNCC IAM Ingress Gateway (CNC Console IAM IGW) and M-CNCC IAM Back End (M-CNCC IAM BE) microservices.

M-CNCC Core
Manager CNC Console Core or M-CNCC Core is a core component of M-CNCC which provides GUI and API access portal for accessing NF and OCCNE common service. M-CNCC

Core contains M-CNCC Core Ingress Gateway (CNC Console Core IGW) and M-CNCC Core Back End (M-CNCC Core BE) microservices.

A-CNCC

A-CNCC Core

Agent CNC Console or A-CNCC Core is a CNC Console Core instance which manages local NF(s) and local CNE common services(s). It is managed by M-CNCC.

- A-CNCC Core contains A-CNCC Core Ingress Gateway.
- A-CNCC Core has no IAM component.

1.3.1 Single Cluster Deployment Architecture

In a single cluster deployment, CNC Console can manage NFs and CNE common services deployed in the local Kubernetes cluster.

The following diagram represents the CNC Console single cluster deployment:

Figure 1-3 CNC Console Single Cluster Deployment Architecture

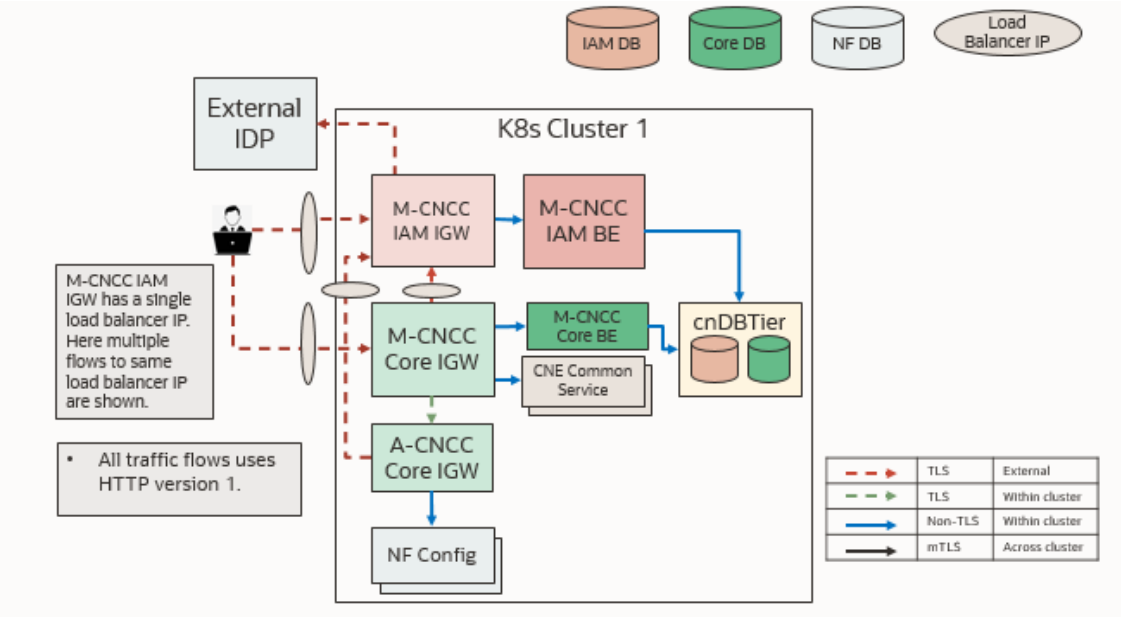
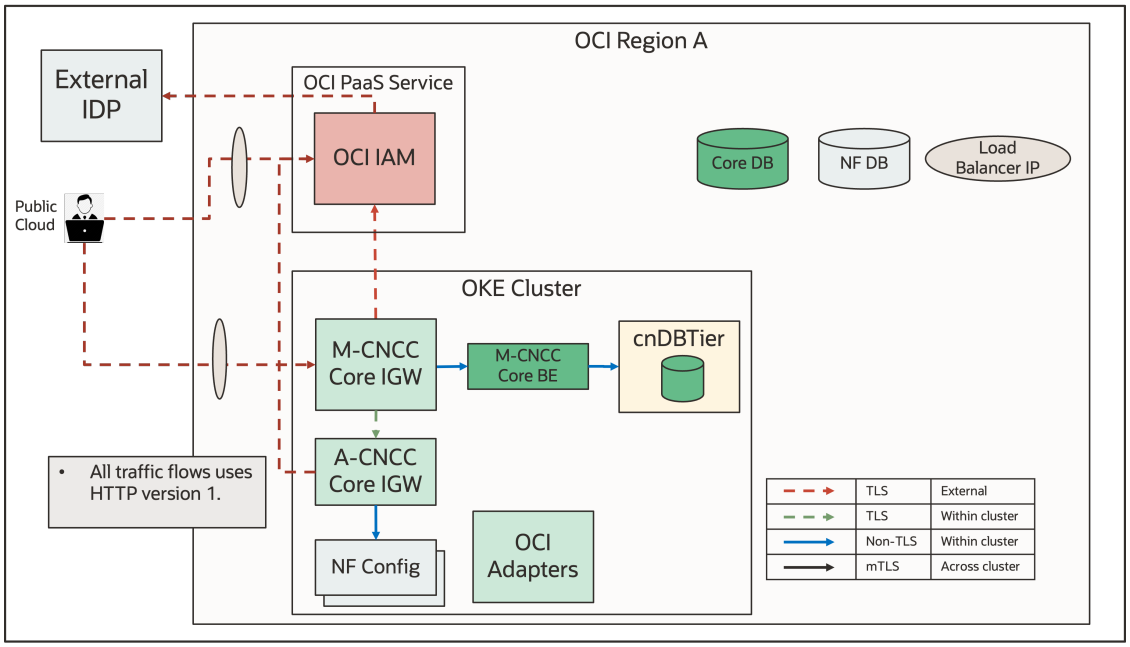


Figure 1-4 OCI



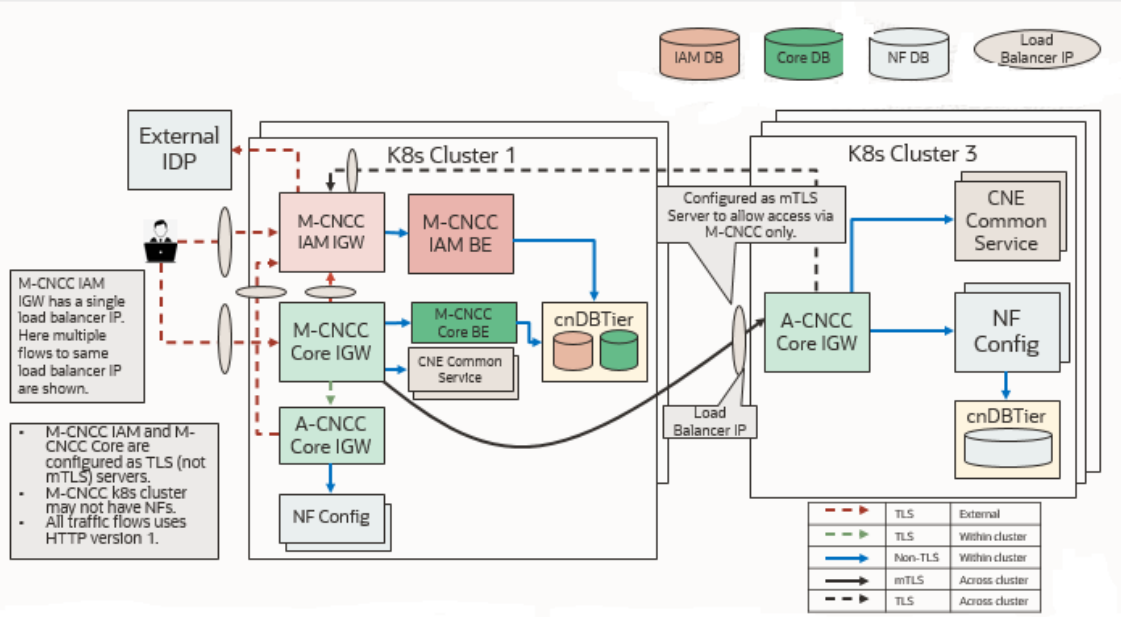
1.3.2 Multicluster Deployment Architecture

> **Note**
>
> Not supported for OCI deployment.

In a multicluster deployment, CNC Console can manage NFs and CNE common services deployed in the remote Kubernetes cluster(s). CNC Console instance called A-CNCC is needed on remote kubernetes clusters for this deployment. CNC Console instance that provides the API access through GUI portal and manages the A-CNCC(s) is called M-CNCC.

The following diagram represents the CNC Console multicluster deployment:

Figure 1-5 CNC Console Multi Cluster Deployment Architecture



> **Note**
>
> - For a single cluster deployment, both Manager (M-CNCC) and Agent (A-CNCC) is deployed on the same cluster.
> - For a multicluster deployment,
>   - If the manager cluster has a local NF deployment, both M-CNCC and A-CNCC should be deployed on the same cluster.
>   - If the manager cluster does not have a local NF deployment, only M-CNCC should be deployed. A-CNCC should be deployed on a cluster where NFs are present.
> - The Manager manages CNE or OSO common service if present in a cluster.
>   - Manager in a cluster is preferred over Agent in the same cluster to manage the CNE common services.
>   - Agent in a cluster can manage CNE common service in absence of a Manager in the same cluster.
> - Agent is needed only when NFs are present on the cluster.

1.4 Supported Deployment Models

The following deployment models are supported by CNC Console:

- Single Cluster, Single Instance (Dedicated Console for each NF in a cluster)
- Single Cluster, Multiple Instances (One Console for many NFs or Instances in a cluster)

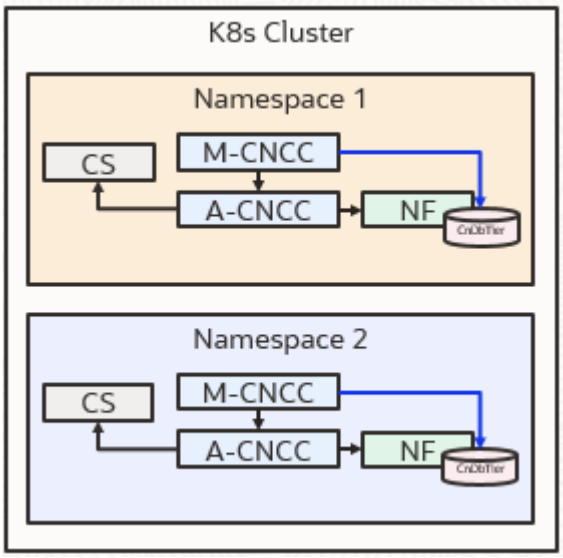
- Multiple Clusters, Single Instance (Multiple clusters with single NF or Instance in each cluster, M-CNCC/A-CNCC sitting in same or different clusters)
- Multiple Clusters, Multiple Instances (Multiple clusters with multiple NF/Instance in each cluster, M-CNCC/A-CNCC sitting in same or different clusters)

1.4.1 Deployment Model 1 - Single Cluster, Single Instance (Dedicated Console for each NF in a cluster)

> **Note**
>
> Common Service (CS) is not applicable for OCI deployment.

This deployment model has dedicated Console for each NF in a cluster.

Figure 1-6 Deployment Model 1 - Single Cluster, Single Instance (Dedicated Console for each NF in a cluster)



The Deployment Model 1 has the following characteristics:

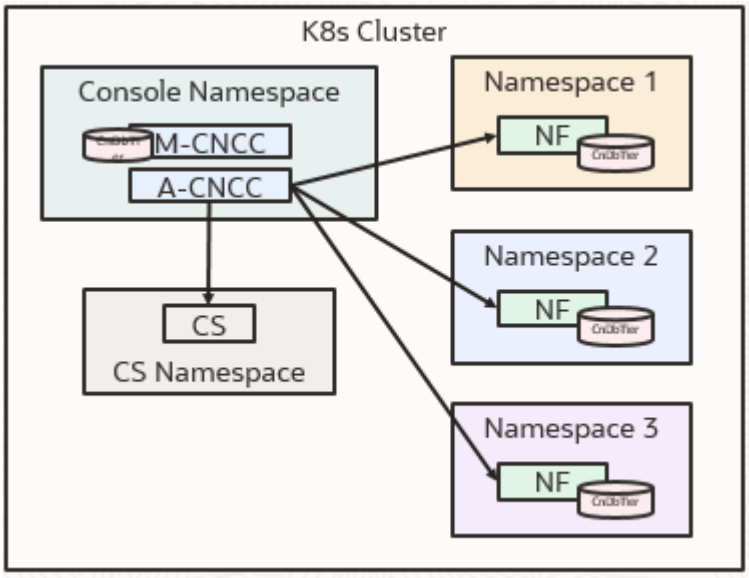
- Dedicated CNC Console for a NF. Only single instance of NF is supported.
- CNC Console shares the cnDBTier with NF.
- Any failure in NF cnDBTier impacts CNC Console. Access to CNE Common Services (CS) is lost in case of any failure in NF cnDBTier.
- NFs and CNC Console release compatibility must be maintained.
- M-CNCC and A-CNCC are managed by single Helm chart.

1.4.2 Deployment Model 2 - Single Cluster, Multiple Instances (One Console for many NFs/Instances in a cluster)

> **Note**
>
> Common Service (CS) is not applicable for OCI deployment.

This deployment model has one Console for many NFs/Instances in a cluster.

Figure 1-7 Deployment Model 2 - Single Cluster, Multiple Instances (One Console for many NFs/Instances in a cluster)



The Deployment Model 2 has the following characteristics:

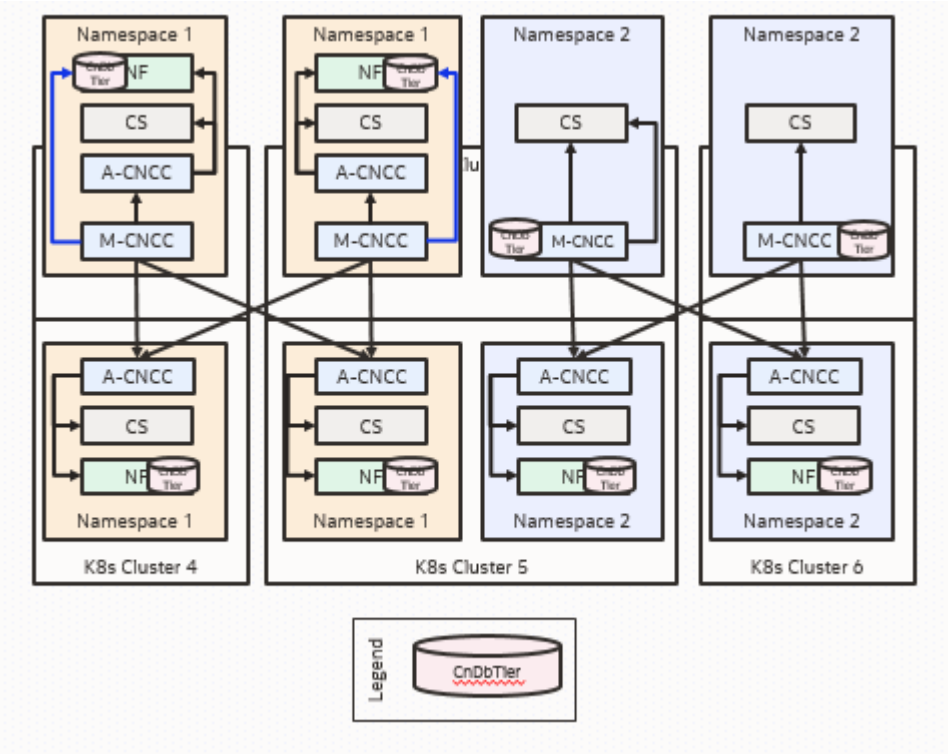
- Shared CNC Console for multiple NFs. NFs can be of same or different NF Type.
- CNC Console needs dedicated cnDBTier for M-CNCC.
- NFs and CNC Console release compatibility must be maintained.
- M-CNCC and A-CNCC are managed by single Helm chart.

1.4.3 Deployment Model 3 - Multiple Clusters, Single Instance (Multiple clusters with single NF or Instance in each cluster, M-CNCC or A-CNCC sitting in the same or different clusters)

> **Note**
>
> Not supported for OCI deployment.

This deployment model is for multiple clusters with single NF or Instance in each cluster. M-CNCC or A-CNCC can be in same or different clusters.

Figure 1-8 Deployment Model 3 - Multiple Clusters, Single Instance (Multiple clusters with single NF/Instance in each cluster, M-CNCC/A-CNCC sitting in same/different clusters)



The deployment model 3 has the following characteristics:

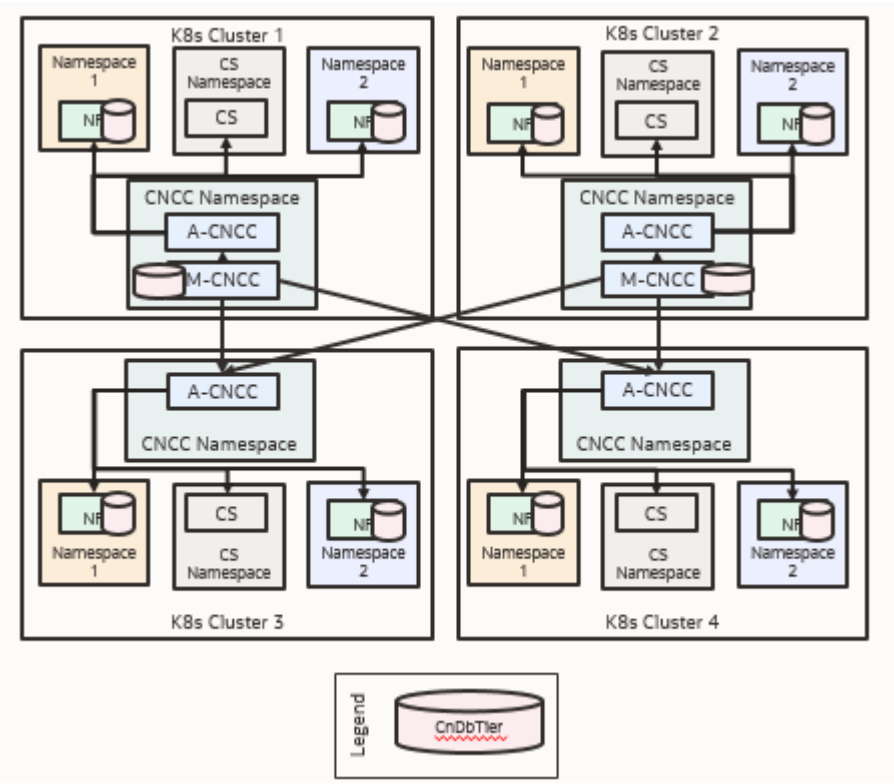
- Dedicated CNC Console for a single NF
- CNC Console shares the cnDBTier with N.
- Any failure in NF cnDBTier impacts CNC Console. Access to CNE Common Services (CS) is lost on any failure in NF cnDBTier.
- NFs and Console release compatibility must be maintained.
- Managers can be deployed as Active/Active/Active.
- Multiple Agents are supported.
- M-CNCC can be deployed without A-CNCC in case there are no local NFs to be managed at the Kubernetes Cluster.
- M-CNCC and A-CNCC are managed by single Helm chart.
- M-CNCC cannot manage NFs located in another M-CNCC Kubernetes Cluster.

1.4.4 Deployment Model 4 - Multiple Clusters, Multiple Instances (Multiple clusters with multiple NF/Instance in each cluster, M-CNCC/A-CNCC sitting in same/different clusters)

> **Note**
>
> Not supported for OCI deployment.

This deployment model is for multiple clusters with multiple NF/Instance in each cluster. M-CNCC/A-CNCC can be in same/different clusters.

Figure 1-9 Deployment Model 4 - Multiple Clusters, Multiple Instances (Multiple clusters with multiple NF/Instance in each cluster, M-CNCC/A-CNCC sitting in same/different clusters)



The deployment model 4 has the following characteristics:

- Shared Console for multiple NFs. NFs can be of same or different NF Type.
- Console needs dedicated cnDBTier for M-CNCC.
- NFs and Console release compatibility must be maintained.

- Managers can be deployed as Active/Active/Active.
- Multiple Agents are supported.
- M-CNCC and A-CNCC are managed by Single Helm Chart.
- M-CNCC cannot manage NFs located in another M-CNCC Kubernetes Cluster.

1.5 CNC Console Deployment Model Matrix

CNC Console Deployment Model Matrix

The following table provides details on support of console deployment models for various network functions:

> **Note**
>
> In the following table, only Model 1 and Model 2 are supported for OCI deployment.

Table 1-3 CNC Console Deployment Model Matrix

Deployment Models	Policy	BSF	SCP	UDR	NRF	NEF	SEPP	NSSF	DD	PROVGW	NWDAF	OCCM
Model 1 - Single Cluster, Single Instance (Dedicated Console for each NF in a cluster)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Model 2 - Single Cluster, Multiple Instances (One Console for many NFs/ Instances in a cluster)	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes

Table 1-3 (Cont.) CNC Console Deployment Model Matrix

Deployment Models	Policy	BSF	SCP	UDR	NRF	NEF	SEPP	NSSF	DD	PROVGW	NWDAF	OCCM
Model 3 - Multiple Clusters, Single Instance (Multiple clusters with single NF/ Instance in each cluster, M-CNCC/A-CNCC sitting in same/ different clusters)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Model 4 - Multiple Clusters, Multiple Instances (Multiple clusters with multiple NF/ Instance in each cluster, M-CNCC/A-CNCC sitting in same/ different clusters)	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes

Note

- Single instance of CNC Console supports either single instances of all NFs or multiple instances of a single NF types within a Kubernetes cluster.
- For example, a single instance of CNC Console can either handle a single instance of Policy, SCP, NRF and so on, or multiple instances of Policy or SCP within a Kubernetes cluster.

1.6 Configuration Workflow

> **Note**
>
> Not applicable for OCI deployment because multicluster is not supported.

This section explains the configuration workflow for the following scenarios:

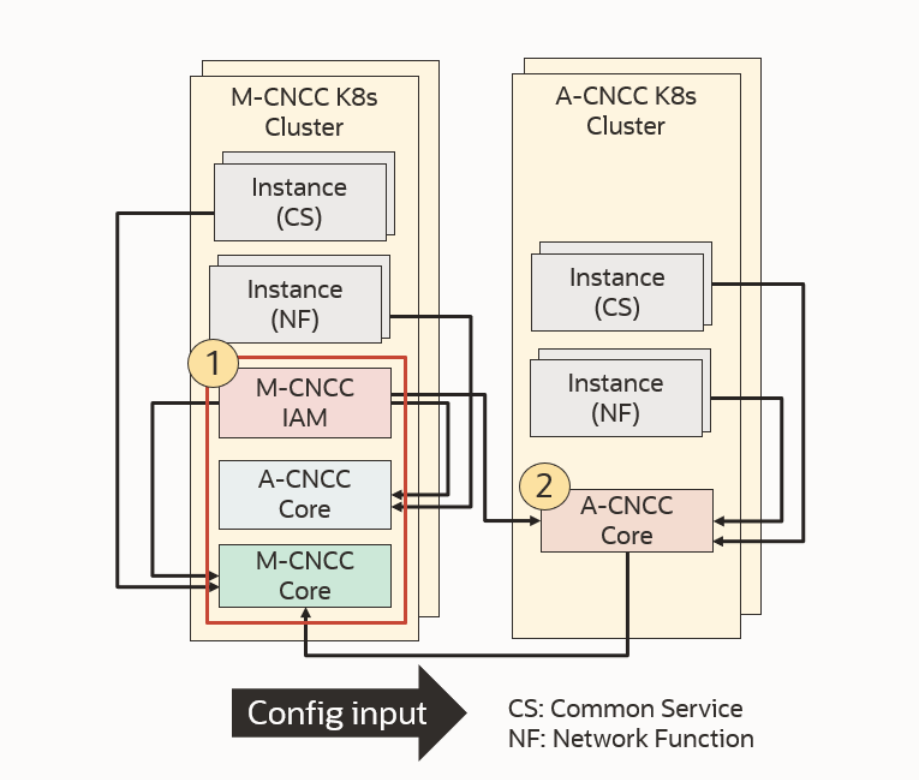
- Fresh Installation
- Add a new M-CNCC
- Add a new A-CNCC
- Remove M-CNCC from A-CNCC
- Remove A-CNCC from M-CNCC

1.6.1 Fresh Installation of M-CNCC and A-CNCC

This section explains how to do a fresh installation of M-CNCC and A-CNCC.

The following diagram represents the fresh installation of M-CNCC and A-CNCC.

Figure 1-10 Fresh Installation of M-CNCC and A-CNCC



Procedure:

1. Install M-CNCC IAM, A-CNCC Core, and M-CNCC Core on M-CNCC Kubernetes clusters.
   - Configuration Input: M-CNCC IAM(s), A-CNCC Core(s), and instances
   - A-CNCC Core on M-CNCC Kubernetes cluster is optional and needed only if there are NF instances on the M-CNCC Kubernetes cluster.

   > **Note**
   >
   > CS Instances are managed directly by M-CNCC Core and does not need A-CNCC Core.

2. Install A-CNCC Core on A-CNCC Kubernetes clusters.
   - Configuration Input: M-CNCC IAMs and local instances

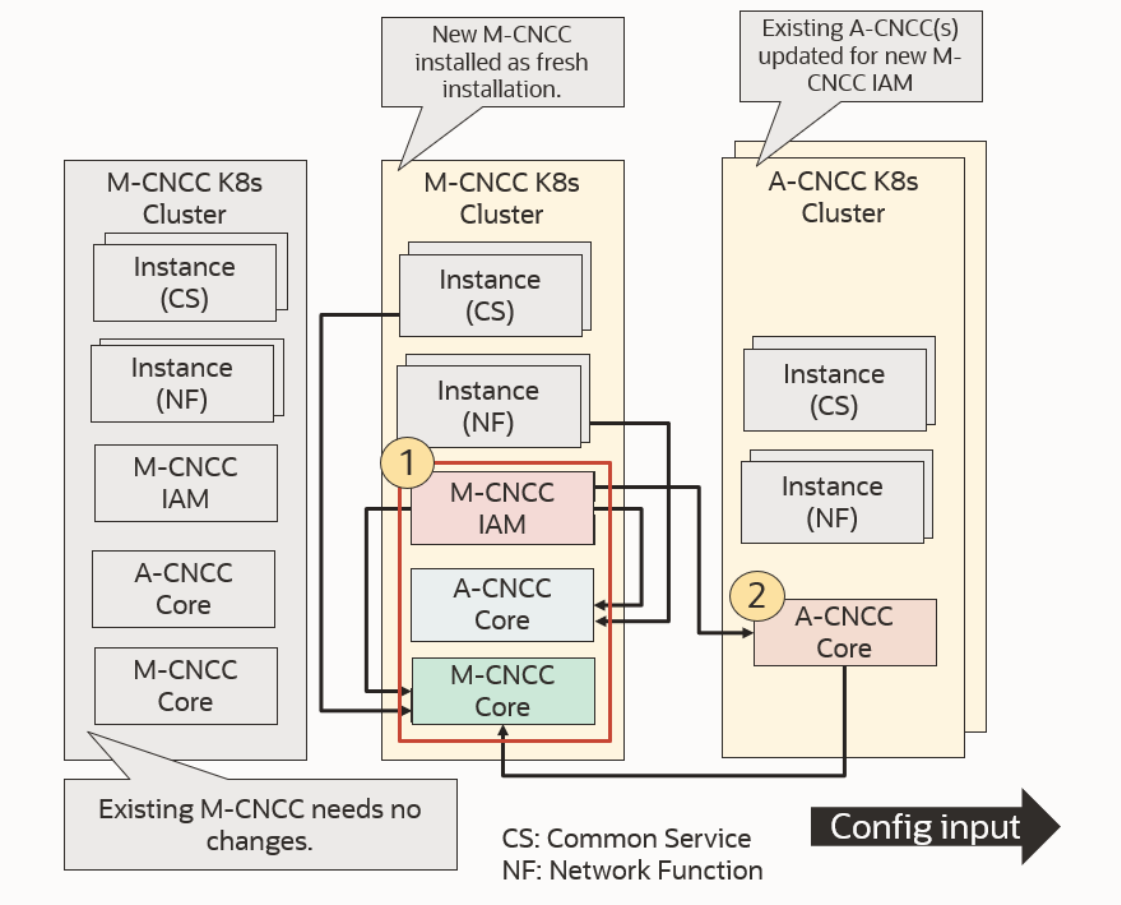
See Installing CNC Console section for installation procedure.

1.6.2 Add a New M-CNCC

This section explains how to add a new M-CNCC.

The following diagram represents the addition of a new M-CNCC:

Figure 1-11 Add a new M-CNCC



Procedure:

1. Install M-CNCC IAM, A-CNCC Core, M-CNCC Core on M-CNCC Kubernetes cluster.

- Configuration Input: M-CNCC IAM(s), A-CNCC Core(s) and instances
- A-CNCC Core on M-CNCC Kubernetes cluster is optional and needed only if there are NF instances on the M-CNCC k8s cluster.

> **Note**
>
> CS Instances are managed directly by M-CNCC Core and does not need A-CNCC Core.

2. Update A-CNCC Core(s) on A-CNCC Kubernetes cluster(s)

- Configuration Update: Newly added M-CNCC IAM

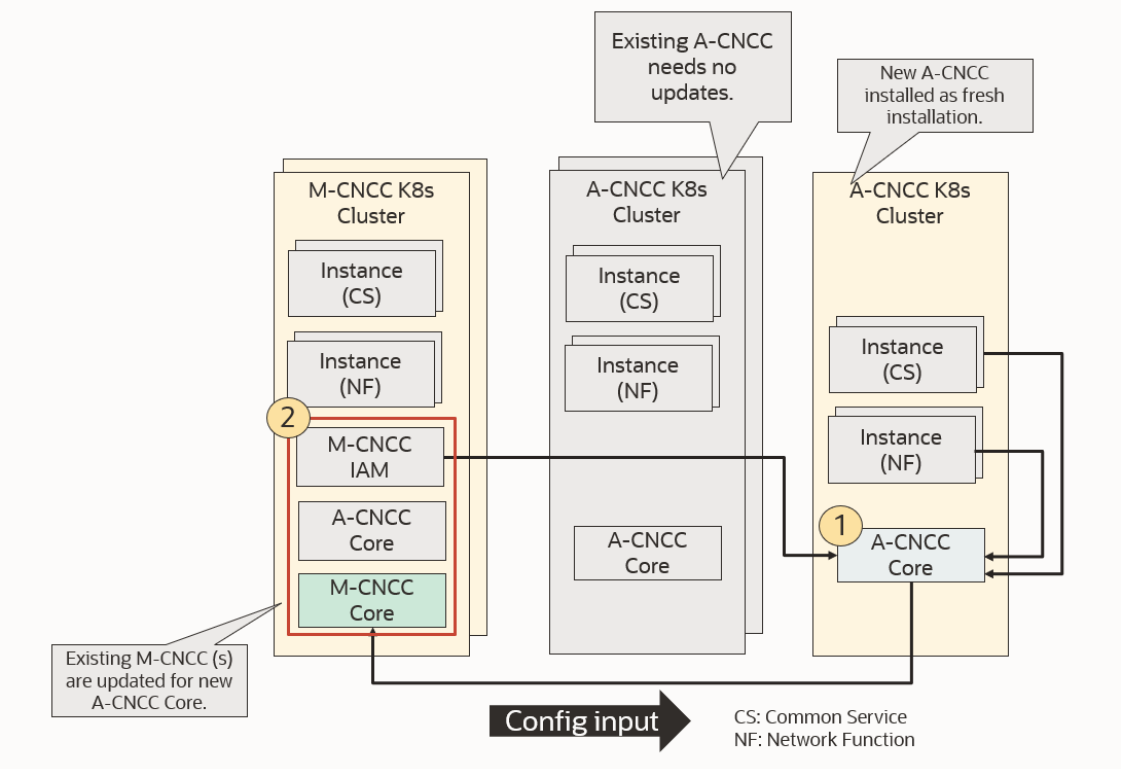
See Installing CNC Console section for installation procedure.

1.6.3 Add a New A-CNCC

This section explains how to add a new A-CNCC.

The following diagram represents the addition of a new A-CNCC:

Figure 1-12 Add a new A-CNCC



Procedure

1.Install A-CNCC Core on new A-CNCC Kubernetes cluster.

- Configuration Input: M-CNCC IAMs and local instances.

2.Update M-CNCC Core on existing M-CNCC Kubernetes clusters.

- Configuration Update: Newly added A-CNCC.

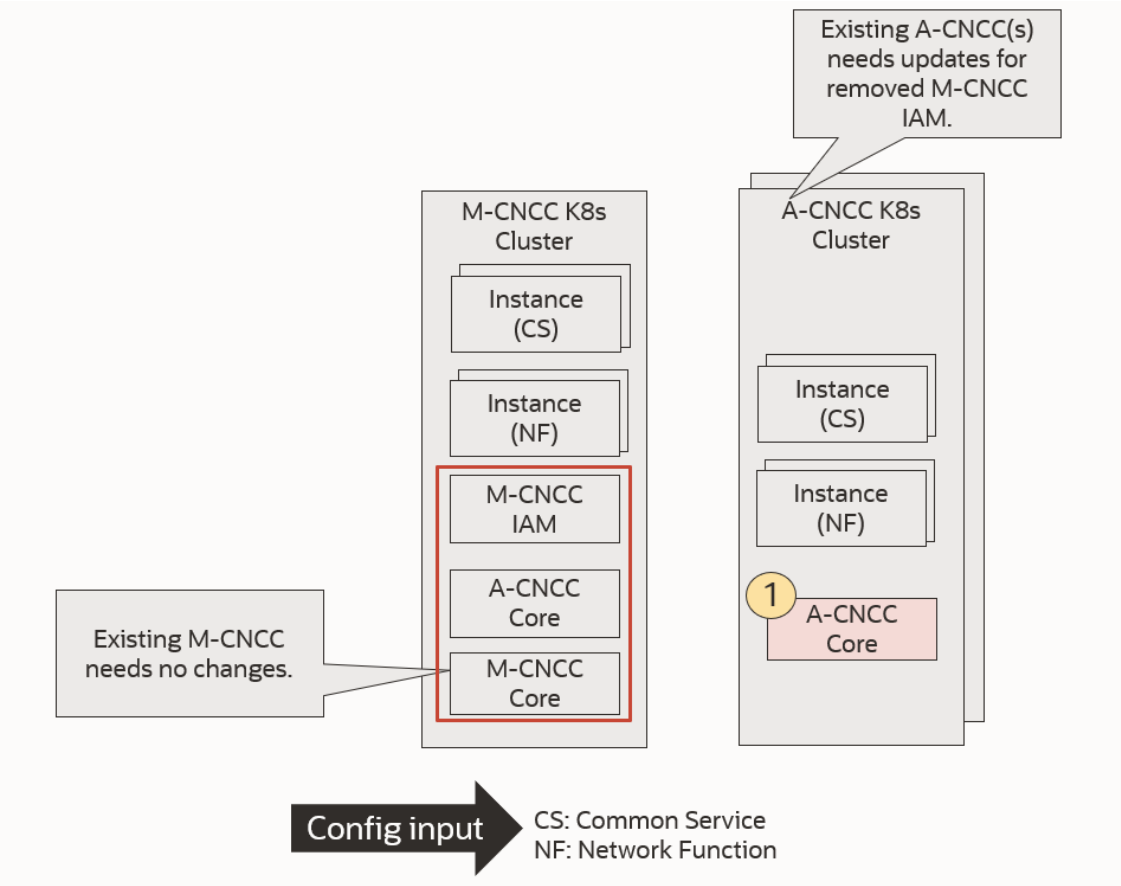
See Installing CNC Console section for installation procedure.

1.6.4 Remove M-CNCC from A-CNCC

This section explains how to remove M-CNCC from A-CNCC.

The following diagram represents the removal of M-CNCC from A-CNCC:

Figure 1-13 Remove M-CNCC from A-CNCC



Procedure

1.Update A-CNCC (one or more)

- Configuration Update: Edit A-CNCC configuration to remove M-CNCC IAM

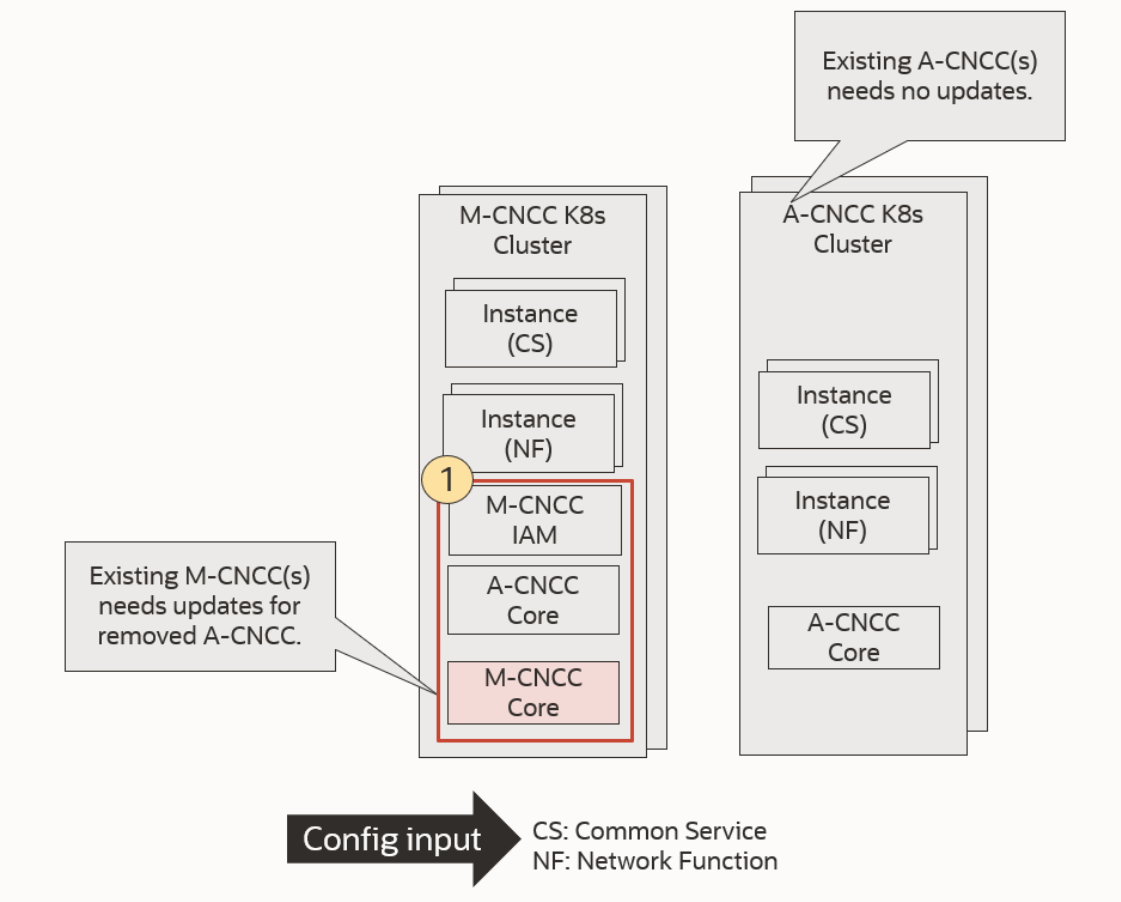
See Installing CNC Console section for installation procedure.

1.6.5 Remove A-CNCC from M-CNCC

This section explains how to remove A-CNCC from M-CNCC.

The following diagram represents the removal of A-CNCC from M-CNCC:

Figure 1-14 Remove A-CNCC from M-CNCC



Procedure

1.Update M-CNCC (one or more)

- Configuration Update: Edit M-CNCC Core configuration to remove A-CNCC

See Installing CNC Console section for installation procedure.

1.7 CNC Console Configuration Maximum Limits

The following table covers the maximum limit defined in CNC Console configuration.

Table 1-4 CNC Console Configuration Maximum Limits

Attribute Name	Max Limit
Max length of cnccId	40
Max length of instanceId	80
Max number of A-CNCC (aCnccs)	36
Max number of instances	288
Max number of M-CNCC (mCnccs)	3

1.8 Reference

Refer to the following documents for more information:

- *Oracle Communications Cloud Native Core, Service Communication Proxy User Guide*
- *Oracle Communications Cloud Native Core, Network Repository Function User Guide*
- *Oracle Communications Cloud Native Core, Policy User Guide*
- *Oracle Communications Cloud Native Core, Unified Data Repository User Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function User Guide*
- *Oracle Communications Cloud Native Core, Security Edge Protection Proxy User Guide*
- *Oracle Communications Cloud Native Core, Network Slice Selection Function User Guide*
- *Oracle Communications Cloud Native Core, Network Repository Function Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Service Communication Proxy Installation Guide*
- *Oracle Communications Cloud Native Core, Unified Data Repository Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Binding Support Function Installation Guide*
- *Oracle Communications Cloud Native Core, Policy Installation Guide*
- *Oracle Communications Cloud Native Core, Security Edge Protection Proxy Installation Guide*
- *Oracle Communications Cloud Native Core, Network Slice Selection Function Installation Guide*
- *Oracle Communications Networks Data Analytics Installation and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Certificate Management User Guide*
- *Oracle Communications Cloud Native Core, Certificate Management Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Network Exposure Function Installation, Upgrade, and Fault Recovery Guide*
- *Oracle Communications Cloud Native Core, Network Exposure Function User Guide*

2
Installing CNC Console

This chapter provides information about installing Oracle Communications Cloud Native Configuration Console (CNC Console) in a cloud native environment.

> **Note**
>
> CNC Console supports fresh installation. For more information on how to upgrade CNC Console, see Upgrading CNC Console section.

2.1 Prerequisites

Before installing Oracle Communications CNC Console, make sure that the following requirements are met:

2.1.1 Software Requirements

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

Install the following software before installing CNC Console:

Table 2-1 Preinstalled Software

Software	Version
Kubernetes	1.28.x, 1.27.x, 1.26.x
Helm	3.12.3
Podman	4.4.1

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

```
kubectl version
```

```
helm version
```

```
podman version
```

The following software are available if CNC Console is deployed in CNE. If you are deploying CNC Console in any other cloud native environment, these additional software must be installed before installing CNC Console. 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 2-2 Additional Software

Software	Version	Required For
Opensearch	2.3.0	Logging
OpenSearch Dashboard	2.3.0	Logging
Kyverno	1.9	Logging
FluentBit	1.9.4	Logging
Grafana	9.5.3	KPIs
Prometheus	2.50.1	Metrics
MetalLB	0.13.11	External IP
Jaeger	1.52.0	Tracing
snmp-notifier	1.2.1	Alerts

> **Note**
>
> Not applicable for OCI deployment.

2.1.2 Environment Setup Requirements

This section provides information on environment setup requirements for installing CNC Console.

Client Machine Requirement

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

Client machine must 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 the `kubectl`, `docker`, and `podman` commands. The environment must 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.

Network Access Requirement

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

- Local helm repository, where the CNC Console helm charts are available.
  To check if the Kubernetes cluster hosts have network access to the local helm repository, run the following command:

  ```
  helm repo update
  ```

- Local docker image repository: It contains the CNC Console Docker images.

To check if the Kubernetes cluster hosts can access the the local Docker image repository, try to retrieve any image with tag name to check connectivity by running the following command:

```
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 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 the image used for the CNC Console pod.

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

Server or Space Requirement

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

CNE Requirement

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

To check the CNE version, run the following command:

```
echo $OCCNE_VERSION
```

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

cnDBTier Requirement

CNC Console supports cnDBTier . cnDBTier must be configured and running before installing CNC Console. For more information about installation procedure, see *Oracle Communications cnDBTier Installation, Upgrade, and Fault Recovery Guide*.

OSO Requirement

CNC Console supports OSO for common operation services (Prometheus and components such as alertmanager, pushgateway) for Kubernetes cluster which does not have these common services. For more information on installation procedure, see *Oracle Communications OSO Installation Guide*.

OCI Requirements

CNC Console can be deployed in OCI.

While deploying CNC Console in OCI, the user must use the Operator instance or VM instead of Bastion Host.

For more information about OCI deployment, see *Oracle Communications Oracle Cloud Interface, NF Deployment on OCI using OCI Adaptor.*

2.1.3 CNC Console Resource Requirement

This section lists the resource requirements to install and run CNC Console.

CNC Console and cnDBTier Resource Usage Guidelines

This section explains the guidelines for CNC Console and cnDBTier resource usage guidelines.

> **Note**
>
> **For OCI:**
>
> - In the OCI environment, the M-CNCC IAM DB is not applicable but M-CNCC Core DB is applicable, and therefore, there are no changes to the database requirement. The CNC Console and cnDBTier Resource Usage table remains valid.
> - In the CNC Console and cnDBTier Resource Usage table, only Model 1 and Model 2 are supported for OCI deployment.

> **Note**
>
> In case of deployment using shared DBTier between NF and Console, you must include Console DB Profile sizing in NF DB Profile sizing.

> **Note**
>
> - DBProfile replica count to be updated as per GR setup.
> - Depending on GR setup of two, three, or four site choose replica count two, four, or six for **SQL** (ndbmysqld).

Table 2-3 CNC Console and cnDBTier Resource Usage

Deployment Model	cnDBTier Usage	DBTier Resource Profile	Console Resources
Model 1 - Single Cluster, Single Instance (dedicated Console for each NF in a cluster)	Console and NF have a single shared DBTier • M-CNCC on same Kubernetes cluster use shared DBTier	• DBProfile • A-CNCC on a same Kubernetes cluster does not have any DBTier dependency. For the details, see cnDBTier Profiles	• For CNC Console Single Cluster Deployment Resource usage, see CNC Console Resource Requirement
Model 2 - Single Cluster, Multiple Instances (One Console for many NFs/ Instances in a cluster)	Dedicated DBTier for Console • M-CNCC on same Kubernetes cluster use single Console DBTier	• DBProfile • A-CNCC on a same Kubernetes cluster does not have anyDBTier dependency. For the details, see cnDBTier Profiles	• For CNC Console Single Cluster Deployment Resource usage, see CNC Console Resource Requirement
Model 3 - Multiple Clusters, Single Instance. (Multiple clusters with single NF/ Instance in each cluster, M-CNCC/A-CNCC sitting in same/different clusters)	Console and NF have a single shared DBTier • M-CNCC on same Kubernetes cluster use shared DBTier	• Manager - DBProfile • A-CNCC on a remote Kubernetes cluster does not have any DBTier dependency. For the details, see cnDBTier Profiles	• For CNC Console Manager with Agent Deployment, see CNC Console Resource Requirement • For CNC Console Manager Only Deployment, see CNC Console Resource Requirement • For CNC Console Agent Only Deployment, see CNC Console Resource Requirement
Model 4 - Multiple Clusters, Multiple Instances (Multiple clusters with multiple NF/Instance in each cluster, M-CNCC/A-CNCC sitting in same/ different clusters)	Dedicated DBTier for Console per Kubernetes cluster • M-CNCC on same Kubernetes cluster use single Console DBTier	• Manager - DBProfile • A-CNCC on a remote Kubernetes cluster does not have any DBTier dependency. For the details, see cnDBTier profiles	• For CNC Console Manager with Agent Deployment, see CNC Console Resource Requirement • For CNC Console Manager Only Deployment , see CNC Console Resource Requirement • For CNC Console Agent Only Deployment , see CNC Console Resource Requirement

> **Note**
>
> - Time synchronization is required between Kubernetes nodes across cluster for functioning of CNC Console security procedures.
> - Ensure NTP sync before proceeding with M-CNCC IAM, M-CNCC Core, and A-CNCC Core installation.

Resource Usage for CNC Console Deployment
Resource usage for CNC Console Single Cluster and Multicluster deployment is listed in the following tables.

> **Note**
>
> The M-CNCC IAM Resource component is not applicable in OCI deployment.

Resource Usage for CNC Console Single Cluster Deployment
Single Cluster Deployment includes M-CNCC IAM, M-CNCC Core and A-CNCC Core components. It also includes common resource needed for manager or agent deployment.

Table 2-4 Resource Usage for CNC Console Single Cluster Deployment

Component	Max		Min	
	CPU	Memory (Gi)	CPU	Memory (Gi)
M-CNCC IAM	4.5	4.5	4.5	4.5
M-CNCC Core	4	4	4	4
A-CNCC Core	2	2	2	2
CNCC Common Resource	2	2	2	2
Total	12.5	12.5	12.5	12.5

Formula

Total Resource = M-CNCC IAM Resource + M-CNCC Core Resource + A-CNCC Core Resource + CNCC Common Resource

Resource Usage for CNC Console Multicluster Deployment
Multicluster Deployment will include M-CNCC IAM and M-CNCC Core components in Manager cluster. A-CNCC Core component shall be deployed in Manager cluster if there is a local NF.

A-CNCC Core is needed in each Agent cluster for managing local NF. CNC Console Common Resource is a common resource needed for manager or agent deployment.

Table 2-5 Resource Usage for CNC Console Multicluster Deployment

Component	Max		Min	
	CPU	Memory (Gi)	CPU	Memory (Gi)
M-CNCC IAM	4.5	4.5	4.5	4.5
M-CNCC Core	4	4	4	4
A-CNCC Core	2	2	2	2

Table 2-5 (Cont.) Resource Usage for CNC Console Multicluster Deployment

CNCC Common Resource	2	2	2	2
*No Of Agents In Other Clusters	2			
Total	18.5	18.5	18.5	18.5

* Assumed number of Agents (A-CNCC Core deployments) for the calculation

Formula to calculate total resource usage:

Total Resource = M-CNCC IAM Resource + M-CNCC Core Resource + Common Resources + (No Of Agents In Other Clusters x (CNCC Common Resource + A-CNCC Core Resource))

CNC Console Manager Only Deployment
The following table shows resource requirement for manager only deployment. In this case, agent will be deployed in separate cluster.

Table 2-6 CNC Console Manager Only Deployment

Component	Max		Min	
	CPU	Memory (Gi)	CPU	Memory (Gi)
M-CNCC IAM	4.5	4.5	4.5	4.5
M-CNCC Core	4	4	4	4
A-CNCC Core	0	0	0	0
CNCC Common Resource	2	2	2	2
Total	10.5	10.5	10.5	10.5

CNC Console Agent Only Deployment
The following table shows resource requirement for agent only deployment, in this case manager will be deployed in separate cluster.

Table 2-7 CNC Console Agent Only Deployment

Component	Max		Min	
	CPU	Memory (Gi)	CPU	Memory (Gi)
M-CNCC IAM	0	0	0	0
M-CNCC Core	0	0	0	0
A-CNCC Core	2	2	2	2
CNCC Common Resource	2	2	2	2
Total	4	4	4	4

CNC Console Manager with Agent Deployment
The following table shows resource requirement for manager with agent deployment, in this case agent will be deployed along with manager to manage local NF.

This manager can manage agents deployed in other clusters.

Table 2-8 CNC Console Manager with Agent Deployment

Component	Max		Min	
	CPU	Memory (Gi)	CPU	Memory (Gi)
M-CNCC IAM	4.5	4.5	4.5	4.5
M-CNCC Core	4	4	4	4
A-CNCC Core	2	2	2	2
CNCC Common Resource	2	2	2	2
Total	12.5	12.5	12.5	12.5

CNC Console Component wise Resource Usage

Table 2-9 CNCC Common Resource Usage

Microservice Name	Containers	Max		Min		Comments
		CPU	Memory	CPU	Memory	
hookJobResources	NA	2	2	2	2	Common Hook Resource
helm test	cncc-test	0	0	0	0	Uses hookJobResources
Total		2	2	2	2	

> **Note**
>
> - Debug tool resources are not considered in the calculation. Debug tool resources usage is per pod, if debug tool is enabled for more than one pod then max 1vCPU and 2Gi Memory per pod is needed.
> - Service Mesh (ASM) sidecar resources are not considered in the calculation. Service Mesh sidecar resources usage is per pod, that is, if Service Mesh is enabled and sidecar is injected, then max 1vCPU and 1Gi Memory per pod is needed.

Table 2-10 M-CNCC IAM Resource Usage

Microservice Name	Containers	Max		Min		Comments
		CPU	Memory	CPU	Memory	
cncc-iam-ingress-gateway	ingress-gateway	2	2	2	2	

Table 2-10 (Cont.) M-CNCC IAM Resource Usage

Microservice Name	Containers	Max		Min		Comments
		CPU	Memory	CPU	Memory	
	init-service*	0	0	0	0	Applicable when HTTPS is enabled. *Init-service container's resources are not counted because the container gets terminated after initialization completes.
	common_config_hook	0	0	0	0	common_config_hook not used in IAM
cncc-iam-kc-http	kc	2	2	2	2	
	init-service*	0	0	0	0	Optional, used for enabling LDAPS. *Init-service container's resources are not counted because the container gets terminated after initialization completes.
	healthcheck	0.5	0.5	0.3	0.3	
	cnnc-iam--pre-install	0	0	0	0	Uses hookJobResources
	cnnc-iam-pre-upgrade	0	0	0	0	Uses hookJobResources
	cnnc-iam-post-install	0	0	0	0	Uses hookJobResources
	cnnc-iam-post-upgrade	0	0	0	0	Uses hookJobResources
Total		4.5	4.5	4.5	4.5	

Table 2-11 M-CNCC Core Resource Usage

Microservice Name	Containers	Max		Min		Comments
		CPU	Memory	CPU	Memory	
cncc-mcore-ingress-gateway	ingress-gateway	2	2	2	2	
	init-service*	0	0	0	9	Applicable when HTTPS is enabled. *Init-service container's resources are not counted because the container gets terminated after initialization completes.
	common_config_hook*	0	0	0	0	Common Configuration Hook container creates databases which are used by Common Configuration Client. *common_config_hook container's resources are not counted because the container gets terminated after initialization completes.
cncc-mcore-cmservice	cmservice	2	2	2	2	
	validation-hook	0	0	0	0	Uses common hookJobResources
Total		4	4	4	4	

Table 2-12 A-CNCC Core Resource Usage

Microservice Name	Containers	Max		Min		Comments
		CPU	Memory	CPU	Memory	
cncc-acore-ingress-gateway	ingress-gateway	2	2	2	2	
	init-service*	0	0	0	0	Applicable when HTTPS is enabled. *Init-service container's resources are not counted because the container gets terminated after initialization completes.
	common_config_hook*	0	0	0	0	Common Configuration Hook container creates databases which are used by Common Configuration Client. *Init-service container's resources are not counted because the container gets terminated after initialization completes.
	validation-hook	0	0	0	0	Uses common hookJobResources
Total		2	2	2	2	

2.2 Installation Sequence

This section describes the CNC Console preinstallation, installation, and postinstallation tasks.

2.2.1 Preinstallation Tasks

Before installing CNC Console, perform the tasks described in this section.

> **Note**
>
> For IPv4 or IPv6 configurations, see Support for IPv4 or IPV6 Configuration for CNC Console.

2.2.1.1 Configuring OCI IAM

> **Note**
>
> Only applicable for OCI deployment.

Configure OCI IAM for Authentication and Authorization

Before working with OCI IAM, you must have OCI tenancy along with Identity Domain created.

When seeking a more secure connection method to access CNC Console beyond basic authentication, OAuth 2.0 is the preferred choice. To implement OAuth 2.0 with CNC Console to connect Integration Cloud, you must configure client-server confidential applications in OCI IAM (formerly known as OCI IAM – Identity Cloud Service). This section provides a step-by-step guide on setting up this application for a CNC Console.

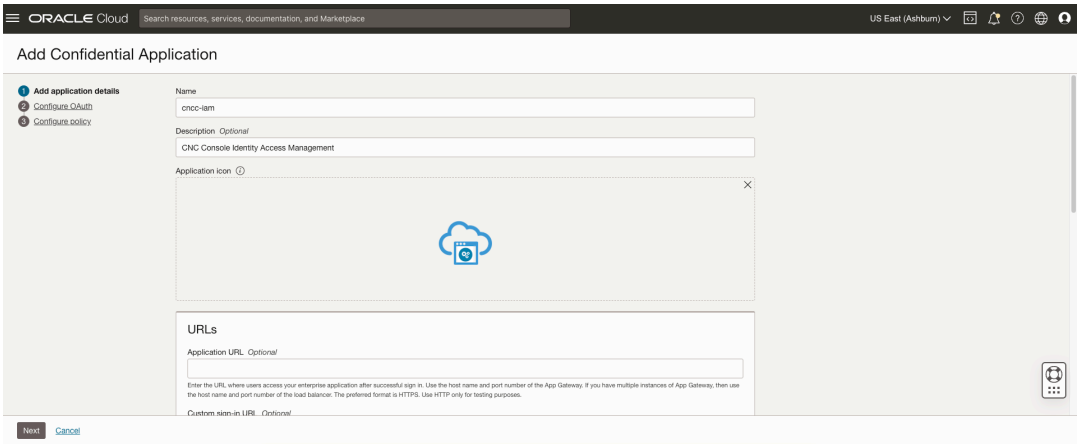
> **Note**
>
> To perform the following steps, **only OCI Admins** are allowed to configure OCI IAM and Custom Claims. For more information, see the *Oracle Communications Cloud Native Core OCI Adaptor, NF Deployment in OCI Guide*

2.2.1.1.1 Create a Confidential Application Under OCI IAM

To create a confidential application under OCI IAM:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Click the name of the identity domain that you want to work in. You might need to change the compartment to find the domain that you want. Then, click **Integrated applications**.
3. Click **Add application.**
4. In the **Add application** window, click **Confidential Application**, and then click **Launch workflow**.
5. In the Add application details page, update the following fields:

Figure 2-1 Add Application



a. **Name**: Enter a name for the confidential application. You can enter up to 125 characters. Ex: **cncc-iam**.

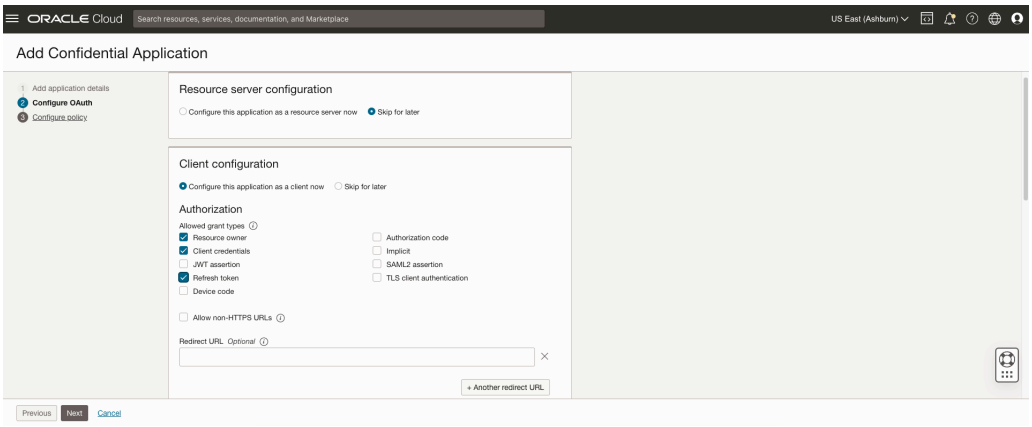
b. **Description:** Enter a description for the confidential application. You can enter up to 250 characters.

6. Click **Next**.

7. On the **Configure OAuth** pane, click **Configure this application as a client now**. Update the following fields.

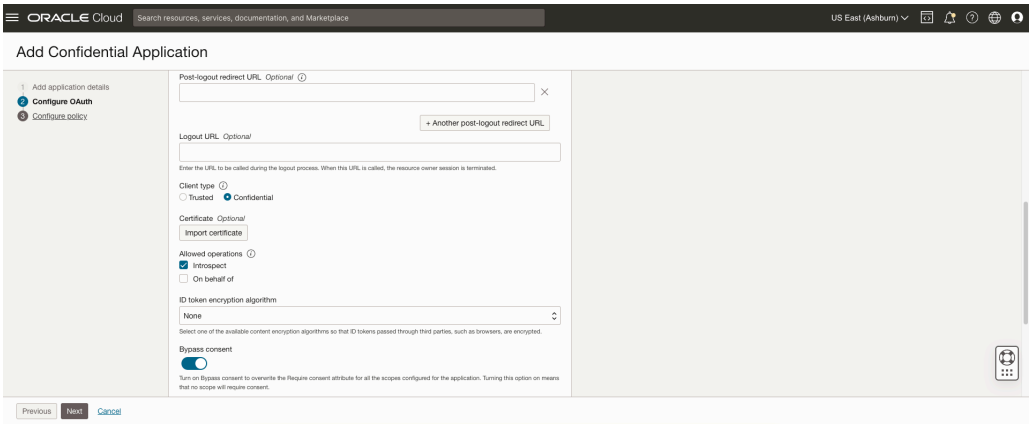
   a. **Authorization Types:** Within the configuration page, toggle on the **Resource owner, Client Credentials** and **Refresh token**.

Figure 2-2 Authorization Types



b. **Client type**: Select **Confidential**.

Figure 2-3 Client Type



c. **Allowed Operations**: Select **Introspect**.

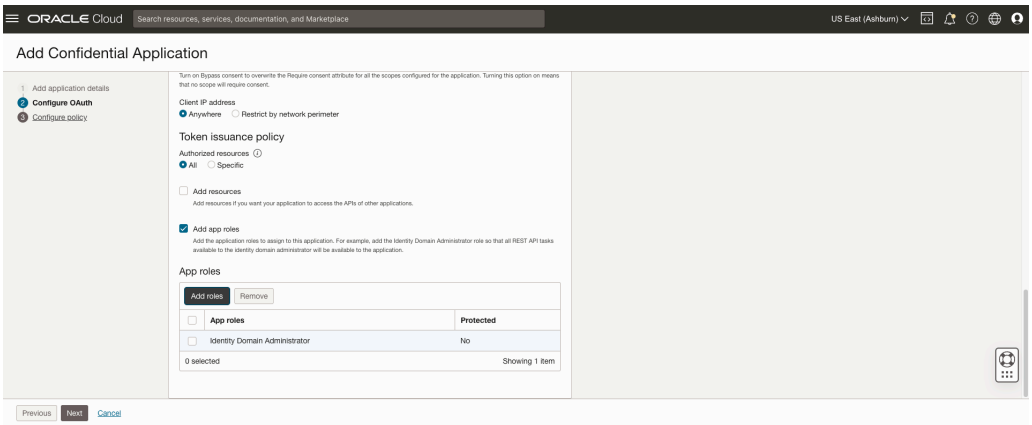
d. **Bypass Consent**: Enable it.

e. **Client IP address**: Select **Anywhere**.

f. **Token Issuance Policy:** From the available options, select **All**.

g. **Add App Role:**

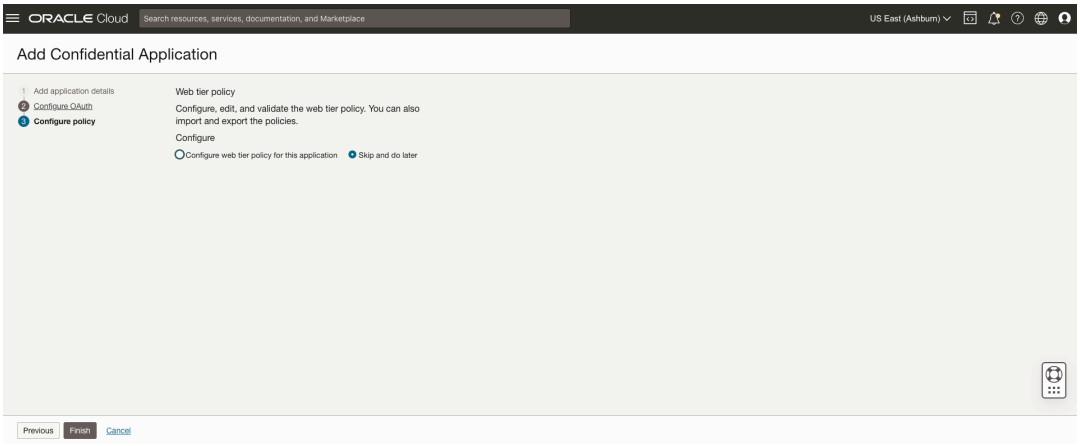
Figure 2-4 Add App Roles



- Click the **Add roles** button to open a side panel for additional configurations.
- In this new panel, locate the role **Identity Domain Administrator**.
- Confirm that the **Identity Domain Administrator** role is checked and added.

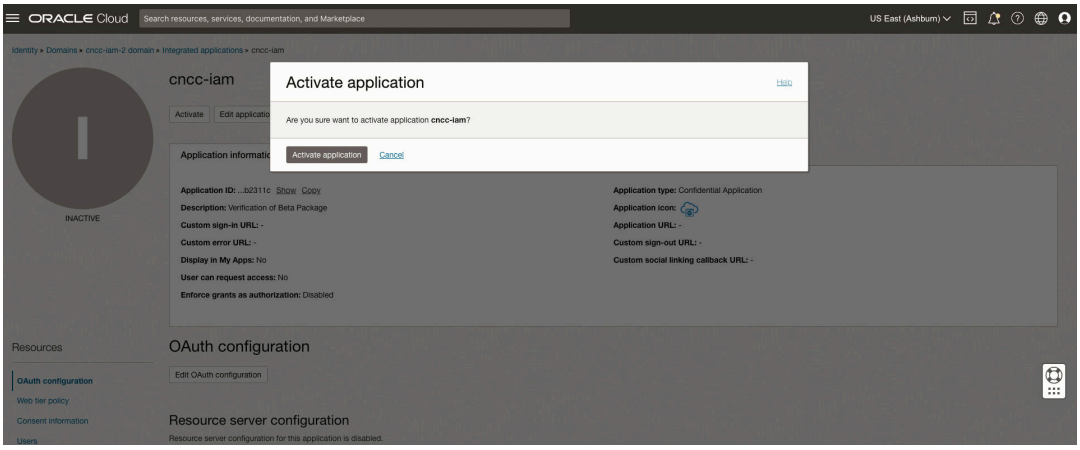
8. Click **Next**.
9. Click **Finish**.

Figure 2-5 Finish



10. At the top of the page, to the right of the application name, click **Activate**.
11. In the **Activate application** dialog box, click **Activate application**.

Figure 2-6 Activate Application

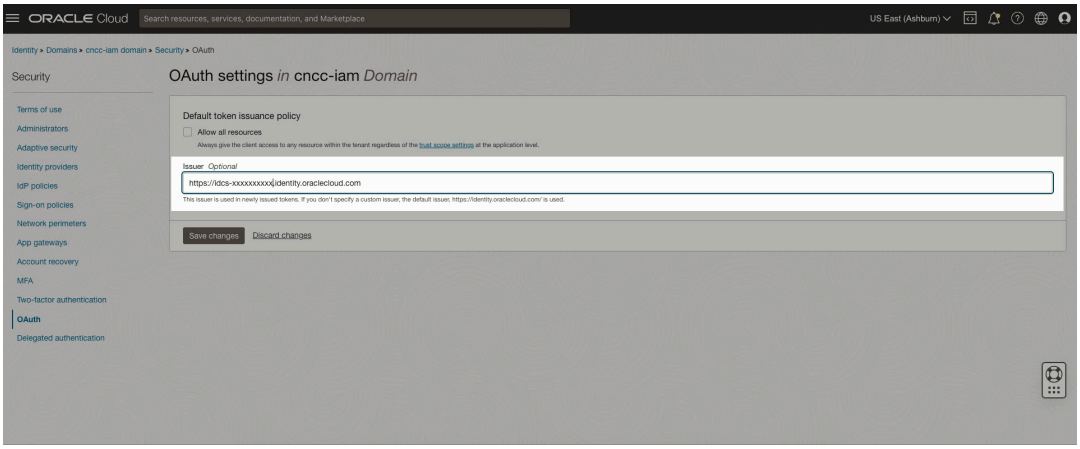


2.2.1.1.2 Update OCI IAM Issuer URL

To updated OCI IAM issuer url:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Click the name of the identity domain that you want to work in. You might need to change the compartment to find the domain that you want.
3. On the domain details page, click **Security**.
4. On the **Security** page, click **OAuth**.
5. In the **Issuer** field, enter the domain URL. This issuer value is used in the newly issued tokens. For more information, see Accessing OCI IAM.

Figure 2-7 Update Issuer



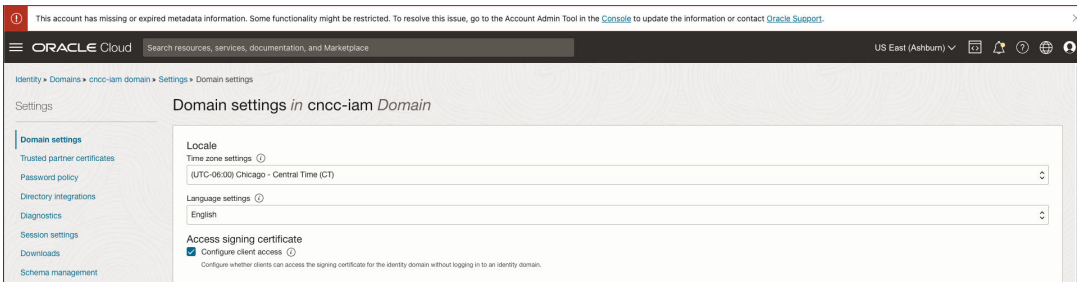
> **Note**
>
> - If the OCI IAM domain URL is with default ports 80 or 443, remove the port from the domain URL while updating the **Issuer** field. Please refer the attached screenshot.
> - The OCI IAM domain URL needs to be configured in **mCnccIams** while installing CNC Console.

2.2.1.1.3 Enabling Access to the Signing Certificate

To allow CNC Console to access the signing certificate for the identity domain in IAM without logging in to an identity domain:

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Click the name of the identity domain that you want to work in. You might need to change the compartment to find the domain that you want.
3. Click **Settings** and then click **Domain settings**.

Figure 2-8 Domain Settings



4. Under **Access signing certificate**, select **Configure client access** to allow CNC Console to access the tenant signing certificate and the SAML metadata without logging in to the identity domain.
   If this option is cleared, CNC Console can access the tenant signing certificate and the SAML metadata only after they authenticate by logging in to the identity domain.

5. Click **Save changes**.

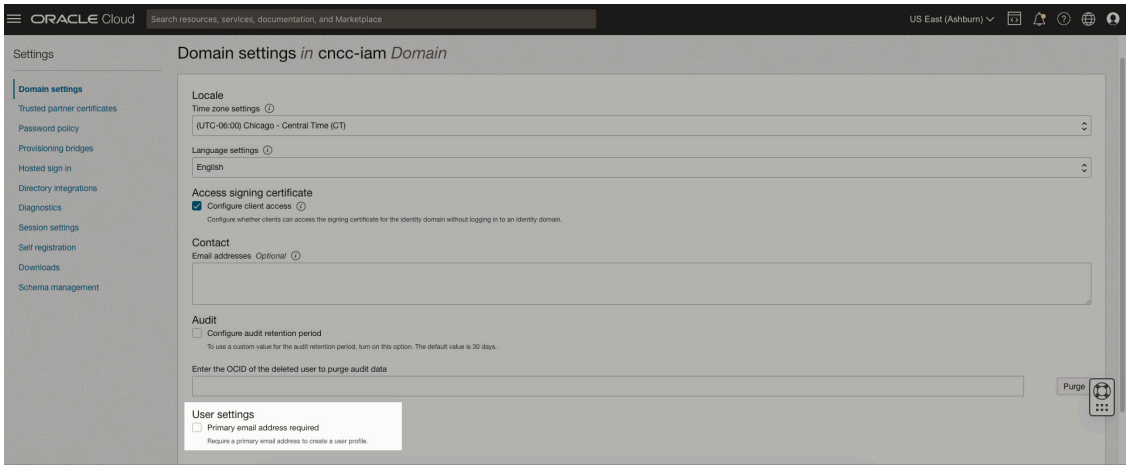
2.2.1.1.4 Disabling User's Email Address for Account Creation (Optional)

> **Note**
>
> By default, **Primary email address required** is enabled for OCI IAM unless OCI IAM Admin disables it.

Set whether a primary email address is required to create user accounts in an identity domain in IAM.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
2. Click the name of the identity domain that you want to work in. You might need to change the compartment to find the domain that you want.
3. Click **Settings** and then click **Domain settings**.
4. Under **User settings**, select or unselect **Primary email address required**.
5. Click **Save changes**.

Figure 2-9 User Settings



2.2.1.1.5 Create Custom Claim in OCI IAM

Configure the Custom Claim you use OCI IAM's Custom Claims REST API:

```
curl --location 'https://<oci-iam-domain-url>/admin/v1/CustomClaims' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer <oci-iam-access-token>' \
--data '{
    "schemas": [
        "urn:ietf:params:scim:schemas:oracle:idcs:CustomClaim"
    ],
    "name": "roles",
    "value": "$user.groups.*.display",
```

```
    "expression": true,
    "mode": "always",
    "tokenType": "BOTH",
    "allScopes": true
}'
```

The attributes used in above request are:

Dynamic Attributes	Description
<oci-iam-domain-url>	OCI IAM Domain URL. For information, see Accessing OCI IAM.
<oci-iam-access-token>	OCI IAM Access token of the OCI IAM Admin User. For more information see the Access NF Resources Through Curl or Postman for OCI section in the *Oracle Communications Cloud Native Configuration Console User Guide.*

Static Attributes	Description
name	Value: **roles** - The claim name.
expression	Value: **true** - OCI IAM identifies the value field will be with expression and not static value.
value	Value: **$user.groups.*.display** - Expression.
mode	Value: **always** – Always include the claim.
tokenType	Value: **BOTH** - The claim will be added to Access and ID Token.
allScopes	Value: **true** - It will be added to any scope.

2.2.1.2 Downloading CNC Console Package

To download the CNCC package from My Oracle Support My Oracle Support (MOS), perform the following steps

1. Log in to My Oracle Support using your login credentials.
2. Click the Patches & Updates tab to locate the patch.
3. In the Patch Search console, click the Product or Family (Advanced) option.
4. Enter `Oracle Communications Cloud Native Core - 5G` in Product field and select the product from the Product drop-down list.
5. From the Release drop-down list, select "Oracle Communications Cloud Native Configuration Console <release_number>".
   Where, <release_number> indicates the required release number of CNCC.
6. Click Search.
   The Patch Advanced Search Results list appears.
7. Select the required patch from the list.
   The Patch Details window appears.
8. Click on Download.
   The File Download window appears.
9. Click on the `<p********_<release_number>_Tekelec>.zip` file.
10. Extract the release package zip file to download the network function patch to the system where network function must be installed.

11. Extract the release package zip file.
    Package is named as follows:

    `occncc_csar_<marketing-release-number>.zip`
    Example:

    `occncc_csar_24_1_1_0_0.zip`

> **Note**
>
> The user must have their own repository for storing the CNC Console images and repository which must be accessible from the Kubernetes cluster.

2.2.1.3 Pushing the Images to Customer Docker Registry

CNC Console deployment package includes ready-to-use images and Helm charts to help orchestrate containers in Kubernetes. The communication between Pods of services of CNC Console products are preconfigured in the Helm charts.

To push the images to the registry, perform the following steps:

1. Unzip the CNC Console package file: Unzip the CNC Console package file to the specific repository:
   `unzip occncc_csar_<marketing-release-number>.zip`

   The package consists of following files and folders:

   a. **Files**: CNC Console Docker images file and CNC Console Helm Charts

   b. **Scripts**: Custom values and alert files:

   - CNC Console custom values file: `occncc_custom_values_<version>.yaml`
   - CNC Console cnDBTier custom values file: `occncc_dbtier_<cndbtier_version>_custom_values_<version>.yaml`
   - CNC Console network policy custom values file: `occncc_network_policy_custom_values_<version>.yaml`
   - CNC Console IAM Schema file for rollback to previous version: `occncc_rollback_iam_schema_<version>.sql`
   - CNC Console Metric Dashboard file: `occncc_metric_dashboard_<version>.json`
   - CNC Console Metric Dashboard file for CNE supporting Prometheus HA (CNE 1.9.x onwards): `occncc_metric_dashboard_promha_<version>.json`
   - CNC Console Metric Dashboard file for OCI deployment: `occncc_oci_metric_dashboard_<version>.zip`
   - CNC Console Alert Rules file: `occncc_alertrules_<version>.yaml`
   - CNC Console Alert Rules file for CNE supporting Prometheus HA (CNE 1.9.x onwards): `occncc_metric_dashboard_promha_<version>.json`
   - CNC Console Alert Rules file for OCI deployment: `occncc_oci_alertrules_<version>.zip`
   - CNC Console MIB files: `occncc_mib_<version>.mib`, `occncc_mib_tc_<version>.mib`

- CNC Console Groups CSV files having roles definition for OCI deployment: `occncc_oci_groups_<version>.csv`
- CNC Top level mib file: `toplevel.mib`

c. **Definitions**: Definitions folder contains the CNE Compatibility and definition files.
   - `occncc_cne_compatibility.yaml`
   - `occncc.yaml`

d. TOSCA-Metadata: `TOSCA.meta`

e. The package folder structure is as follows:

```
Definitions
       occncc_cne_compatibility.yaml
       occncc.yaml
Files
    apigw-common-config-hook-24.1.10.tar
    apigw-configurationinit-24.1.10.tar
    ChangeLog.txt
    cncc-apigateway-24.1.10.tar
    cncc-cmservice-24.1.1.tar
    cncc-core-validationhook-24.1.1.tar
    cncc-iam-24.1.1.tar
    cncc-iam-healthcheck-24.1.1.tar
    cncc-iam-hook-24.1.1.tar
    Helm
        occncc-24.1.1.tgz
        occncc-network-policy-24.1.1.tgz
    Licenses
    nf_test-24.1.2.tar
    ocdebug-tools-24.1.3.tar
    Oracle.cert
    Tests
occncc.mf
Scripts
    occncc_alerting_rules_promha_24.1.1.yaml
    occncc_alertrules_24.1.1.yaml
    occncc_custom_values_24.1.1.yaml
    occncc_dbtier_24.1.0_custom_values_24.1.1.yaml
    occncc_metric_dashboard_24.1.1.json
    occncc_metric_dashboard_promha_24.1.1.json
    occncc_mib_24.1.1.mib
    occncc_mib_tc_24.1.1.mib
    occncc_network_policy_custom_values_24.1.1.yaml
    occncc_rollback_iam_schema_24.1.1.sql
    occncc_oci_metric_dashboard_24.1.1.zip
    occncc_oci_alertrules_24.1.1.zip
    occncc_oci_groups_24.1.1.csv
    toplevel.mib
TOSCA-Metadata
    TOSCA.meta

Example: unzip occncc_csar_24_1_1_0_0.zip
Archive: occncc_csar_24_1_1_0_0.zip
creating: Definitions/
inflating: Definitions/occncc_cne_compatibility.yaml
```

```
inflating: Definitions/occncc.yaml
creating: Files/
creating: Files/Tests/
creating: Files/Helm/
inflating: Files/Helm/occncc-24.1.1.tgz
extracting: Files/Helm/occncc-network-policy-24.1.1.tgz
creating: Files/Licenses/
inflating: Files/apigw-configurationinit-24.1.10.tar
inflating: Files/apigw-common-config-hook-24.1.10.tar
inflating: Files/ocdebug-tools-24.1.3.tar
inflating: Files/cncc-apigateway-24.1.10.tar
inflating: Files/cncc-iam-24.1.1.tar
inflating: Files/cncc-iam-hook-24.1.1.tar
inflating: Files/cncc-iam-healthcheck-24.1.1.tar
inflating: Files/nf_test-24.1.2.tar
inflating: Files/cncc-core-validationhook-24.1.1.tar
inflating: Files/cncc-cmservice-24.1.1.tar
inflating: Files/ChangeLog.txt
extracting: Files/Oracle.cert
creating: Scripts/
inflating: Scripts/occncc_custom_values_24.1.1.yaml
inflating: Scripts/occncc_network_policy_custom_values_24.1.1.yaml
inflating: Scripts/occncc_mib_tc_24.1.1.mib
inflating: Scripts/occncc_mib_24.1.1.mib
inflating: Scripts/toplevel.mib
inflating: Scripts/occncc_metric_dashboard_24.1.1.json
inflating: Scripts/occncc_metric_dashboard_promha_24.1.1.json
inflating: Scripts/occncc_alertrules_24.1.1.yaml
inflating: Scripts/occncc_alerting_rules_promha_24.1.1.yaml
inflating: Scripts/occncc_rollback_iam_schema_24.1.1.sql
inflating: Scripts/occncc_dbtier_24.1.0_custom_values_24.1.1.yaml
inflating: Scripts/occncc_oci_metric_dashboard_24.1.1.zip
inflating: Scripts/occncc_oci_alertrules_24.1.1.zip
inflating: Scripts/occncc_oci_groups_24.1.1.csv
creating: TOSCA-Metadata/
inflating: TOSCA-Metadata/TOSCA.meta
inflating: occncc.mf


occncc_oci_metric_dashboard_<version>.zip file contains the metric
dashboard files for OCI deployment.
occncc_oci_metric_dashboard_<version>.json  covers overall metrics
including all the supported NF flows.
occncc_oci_<NF>_metric_dashboard_<version>.json covers NF flow specific
metrics.

Example:
unzip occncc_oci_metric_dashboard_24.1.1.zip
Archive:  occncc_oci_metric_dashboard_24.1.1.zip
   creating: occncc_oci_metric_dashboard/
  inflating: occncc_oci_metric_dashboard/
occncc_oci_bsf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_dd_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_metric_dashboard_24.1.1.json
```

```
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nef_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nrf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nssf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nwdaf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_occm_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_policy_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_provgw_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_scp_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_sepp_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_udr_metric_dashboard_24.1.1.json

occncc_oci_alertrules_<version>.zip file contains the alarm terraform
directory for OCI deployment.
occncc_oci directory contains CNC Console feature specific alarms.
occncc_oci_resources directory contains CNC Console pod/container
memory alarms.

Example:
unzip occncc_oci_alertrules_24.1.1.zip
Archive:  occncc_oci_alertrules_24.1.1.zip
   creating: occncc_oci_alertrules/
   creating: occncc_oci_alertrules/occncc_oci_resources/
  inflating: occncc_oci_alertrules/occncc_oci_resources/
notifications.tf
  inflating: occncc_oci_alertrules/occncc_oci_resources/alarms.tf
  inflating: occncc_oci_alertrules/occncc_oci_resources/variables.tf
  inflating: occncc_oci_alertrules/occncc_oci_resources/schema.yaml
   creating: occncc_oci_alertrules/occncc_oci/
  inflating: occncc_oci_alertrules/occncc_oci/notifications.tf
  inflating: occncc_oci_alertrules/occncc_oci/alarms.tf
  inflating: occncc_oci_alertrules/occncc_oci/variables.tf
  inflating: occncc_oci_alertrules/occncc_oci/schema.yaml
```

2. Run the following command to move to Files Folder To load docker image:

   ```
   cd Files
   ```

3. Run the following command to load the tarballs to system and push to registry:

Note

For OCI

- **cncc-iam-*** images are not applicable for OCI deployment.
- CNC Console images must be pushed to OCI Registry. In the following commands, replace `<docker-repo>/<podman-repo>` with `<oci-repo>`

OCI Registry:

a. To push the images to OCI Registry you need to login to the OCI Registry:
Docker command:

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

Podman command:

```
podman 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 Authtoken generated by the user.

For details about the Region Key, refer to Regions and Availability Domains.

Identity Domain is the domain to which the user is present.

Object Storage Namespace is available at OCI Console > Governanace & Administration > Account Management > Tenenancy Details > Object Storage Namespace.

b. Push the images to OCI Registry.

Run the following command to push the images to the required registry:

Docker:

```
docker load --input <image-name>:<image-tag>.tar
docker tag <image-name>:<image-tag> <docker-repo>/<image-name>:<image-tag>
docker push <docker_repo>/<image_name>:<image-tag>
```

For example:

```
docker load --input apigw-common-config-hook-24.1.10.tar
docker tag occncc/apigw-common-config-hook:24.1.10 <docker-repo>/occncc/
apigw-common-config-hook:24.1.10
docker push <docker-repo>/occncc/apigw-common-config-hook:24.1.10

docker load --input cncc-core-validationhook-24.1.1.tar
docker tag occncc/cncc-core-validationhook:24.1.1 <docker-repo>/occncc/
```

```
cncc-core-validationhook:24.1.1
docker push <docker-repo>/occncc/cncc-core-validationhook:24.1.1

docker load --input nf_test-24.1.2.tar
docker tag occncc/nf_test:24.1.2 <docker-repo>/occncc/nf_test:24.1.2
docker push <docker-repo>/occncc/nf_test:24.1.2

docker load --input apigw-configurationinit-24.1.10.tar
docker tag occncc/apigw-configurationinit:24.1.10 <docker-repo>/occncc/
apigw-configurationinit:24.1.10
docker push <docker-repo>/occncc/apigw-configurationinit:24.1.10

docker load --input cncc-iam-24.1.1.tar
docker tag occncc/cncc-iam:24.1.1 <docker-repo>/occncc/cncc-iam:24.1.1
docker push <docker-repo>/occncc/cncc-iam:24.1.1

docker load --input ocdebug-tools-24.1.3.tar
docker tag occncc/ocdebug-tools:24.1.3 <docker-repo>/occncc/ocdebug-
tools:24.1.3
docker push <docker-repo>/occncc/ocdebug-tools:24.1.3

docker load --input cncc-iam-healthcheck-24.1.1.tar
docker tag occncc/cncc-iam-healthcheck:24.1.1 <docker-repo>/occncc/cncc-
iam-healthcheck:24.1.1
docker push <docker-repo>/occncc/cncc-iam-healthcheck:24.1.1

docker load --input cncc-iam-hook-24.1.1.tar
docker tag occncc/cncc-iam-hook:24.1.1 <docker-repo>/occncc/cncc-iam-
hook:24.1.1
docker push <docker-repo>/occncc/cncc-iam-hook:24.1.1

docker load --input cncc-apigateway-24.1.10.tar
docker tag occncc/cncc-apigateway:24.1.10 <docker-repo>/occncc/cncc-
apigateway:24.1.10
docker push <docker-repo>/occncc/cncc-apigateway:24.1.10

docker load --input cncc-cmservice-24.1.1.tar
docker tag occncc/cncc-cmservice:24.1.1<docker-repo>/occncc/cncc-
cmservice:24.1.1
docker push <docker-repo>/occncc/cncc-cmservice:24.1.1
```

Podman:

```
podman load --input <image-name>:<image-tag>.tar
podman tag <image-name>:<image-tag> <podman-repo>/<image-name>:<image-tag>
podman push <podman_repo>/<image_name>:<image-tag>
```

4. Run the following command to check whether all the images are loaded:

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

```
docker images
```

```
podman images
```

5. Run the following command to move to the Helm Directory

   ```
   cd Helm
   ```

   For example:

   ```
   helm cm-push --force occncc-24.1.1.tgz ocspf-helm-repo
   ```

6. Run the following command to push helm charts to Helm Repository:

   ```
   helm cm-push --force <chart name>.tgz <helm repo>
   ```

   For example:

   ```
   helm cm-push --force occncc-24.1.1.tgz ocspf-helm-repo
   ```

2.2.1.4 Verifying and Creating CNC Console Namespace

This section explains how to verify or create new namespace in the system.

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

To verify and create a namespace:

> **Note**
>
> To install CNC Console in NF specific namespace, replace cncc namespace with custom namespace.

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

   ```
   kubectl get namespaces
   ```

2. If the namespace exists, continue with the next steps of installation. If the required namespace is not available, create a namespace using the following command:

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

3. For example:

   ```
   kubectl create namespace cncc
   ```

Sample output: `namespace/cncc created`

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 namespace. The prefix is reserved for Kubernetes system namespaces.

> **Note**
>
> For the information about extra privileges required to enable debug tools, see the steps mentioned in the CNC Console Debug Tools section in the *Oracle Communications, Cloud Native Configuration Console Troubleshooting Guide*.

2.2.1.5 Creating Service Account, Role, and Rolebinding

2.2.1.5.1 Global Service Account Configuration

This section is optional and it describes how to manually create a service account, role, and rolebinding.

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

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

   ```
   vi <occncc-resource-file>
   ```

   For example:`vi occncc-resource-template.yaml`.

2. Update the `occncc-resource-template.yaml` file with release specific information.

   > **Note**
   >
   > Update `<helm-release>` and `<namespace>` with its respective CNC Console namespace and CNC Console Helm release name.

   A sample CNC Console service account yaml file is as follows:

   ```
   ## Service account yaml file for cncc-sa
   apiVersion: v1
   kind: ServiceAccount
   metadata:
     name: cncc-sa
     namespace: cncc
     annotations: {}
   ---
   apiVersion: rbac.authorization.k8s.io/v1
   kind: Role
   metadata:
     name: cncc-role
     namespace: cncc
   rules:
   - apiGroups:
     - "" # "" indicates the core API group
     resources:
     - services
     - configmaps
     - pods
     - secrets
     - endpoints
     - persistentvolumeclaims
     verbs:
     - get
     - watch
     - list
   ---
   apiVersion: rbac.authorization.k8s.io/v1
   kind: RoleBinding
   metadata:
     name: cncc-rolebinding
   ```

```
  namespace: cncc
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: cncc-role
subjects:
- kind: ServiceAccount
  name: cncc-sa
  namespace: cncc
```

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

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

4. Update the `serviceAccountName` parameter in the `occncc_custom_values_<version>.yaml` file with the value updated in the `name` field for ingress-gateway and keycloak.
   For Ingress Gateway and keycloak, provide custom service account under **global.serviceAccountName.** as follows:

   ```
   global:

     serviceAccountName: &serviceAccountName cncc-sa

   cncc-iam:
     kc:
       keycloak:
         serviceAccount:
           # The name of the service account to use.
           name: *serviceAccountName
   ```

2.2.1.5.2 Helm Test Service Account Configuration

This section is optional and it describes how to manually create a service account, role, and rolebinding for helm test.

Custom service account can be provided for helm test in `global.helmTestServiceAccountName`:

```
global:

  # ********    Sub-Section Start: Common Global Parameters        ********
  # ************************************************************************

  helmTestServiceAccountName: cncc-helmtest-serviceaccount
```

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

   ```
   vi <occncc-resource-file>
   ```

   For example:`vi occncc-resource-template.yaml`.

2. Update the `occncc-resource-template.yaml` file with release specific information.

> **Note**
>
> Update <helm-release> and <namespace> with its respective CNC Console namespace and CNC Console Helm release name.

A sample CNC Console service account yaml file is as follows:

Sample helm test service account : cncc-helmtest-serviceaccount.yaml

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cncc-helmtest-serviceaccount
  namespace: cncc
  annotations: {}
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: cncc-helmtest-role
  namespace: cncc
rules:
- apiGroups:
  - "" # "" indicates the core API group
  resources:
  - services
  - configmaps
  - pods
  - secrets
  - endpoints
  - persistentvolumeclaims
  - serviceaccounts
  verbs:
  - get
  - watch
  - list
- apiGroups:
  - policy
  resources:
  - poddisruptionbudgets
  verbs:
  - get
  - watch
  - list
  - update
- apiGroups:
  - apps
  resources:
  - deployments
  - statefulsets
  verbs:
  - get
  - watch
  - list
```

```
  - update
- apiGroups:
  - autoscaling
  resources:
  - horizontalpodautoscalers
  verbs:
  - get
  - watch
  - list
  - update
- apiGroups:
  - rbac.authorization.k8s.io
  resources:
  - roles
  - rolebindings
  verbs:
  - get
  - watch
  - list
  - update
- apiGroups:
  - monitoring.coreos.com
  resources:
  - prometheusrules
  verbs:
  - get
  - watch
  - list
  - update

---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: cncc-helmtest-rolebinding
  namespace: cncc
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: cncc-helmtest-role
subjects:
- kind: ServiceAccount
  name: cncc-helmtest-serviceaccount
  namespace: cncc
```

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

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

4. Update the `global.helmTestServiceAccountName` parameter in the `occncc_custom_values_<version>.yaml` file with the value updated in the `name` field for ingress-gateway and keycloak.

> **Note**
>
> If user doesn't want to create the separate service account for helm test, then logging of resources and complaint check could also be done using global service account. For that, required resources should be added to the global service account. For more details on helmTestserviceAccount, see Helm Test section.

2.2.1.6 Configuring Database

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

> **Note**
>
> - Before running the procedure for georedundant sites, ensure that the DBTier for georedundant sites is up and replication channels are enabled.
> - While performing a fresh installation, if CNCC release is already deployed, purge the deployment, and remove the database and users that were used for the previous deployment. For uninstallation procedure, see Uninstalling CNC Console .
> - If cnDBTier 23.3.0 is used during installation, set the ndb_allow_copying_alter_table parameter to 'ON' in the occncc_dbtier_23.3.0_custom_values_23.3.0.yaml file before installing CNC Console. After CNC Console installation, the parameter value can be set to its default value 'OFF'.

> **Caution**
>
> Verify the value of the following parameters, before deploying CNC Console in a three site georedundency setup:
>
> ndb:
>
> MaxNoOfOrderedIndexes: 1024
>
> MaxNoOfTables: 1024
>
> NoOfFragmentLogFiles: 512

Naming Convention for CNCC Database

As the CNCC instances cannot share the same database, user must provide a unique name to the CNCC DB in the cnDBTier either limited to a site or spanning across sites.

The recommended format for database name is as follows:

```
<database-name>_<site-name>_<cluster>
```

Example:

```
cnccdb_site1_cluster1
```

The name of the database should:

- starts and ends with an alphanumeric character
- contains a maximum of 63 characters
- contains only alphanumeric characters or '-'

2.2.1.6.1 Configuring the Database User

This section explains how to create or verify the existing cncc user.

1. Log in to the server or machine which has permission to access the SQL nodes of the NDB cluster.
2. Connect to the SQL node of the NDB cluster or connect to the cnDbTier.
   Run the following command to connect to cnDbTier:

   ```
   $ kubectl -n <cndbtier_namespace> exec -it <cndbtier_sql_pod_name> -c
   <cndbtier_sql_container_name> -- bash
   ```

   Example:

   ```
   $ kubectl -n cndbtier  exec -it ndbappmysqld-0 -c mysqlndbcluster -- bash
   ```

3. Log in to the MySQL prompt using root permission or user, which has permission to create users with permissions.

   ```
   mysql -h 127.0.0.1 -u root -p
   ```

   > **Note**
   >
   > Provide MySQL password, when prompted.

4. Check if CNC Console user already exists by running the following command:

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

5. If the user does not exist, create a cncc-user by running the following command:

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

   Example:

   ```
   $ CREATE USER IF NOT EXISTS 'cnccusr'@'%' IDENTIFIED BY 'cnccpasswd'
   ```

6. Run the following command to grant NDB_STORED_USER permission to the cncc-user:

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

   Example:

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

2.2.1.6.2 Configuring M-CNCC IAM Database

> **Note**
>
> Not applicable for OCI deployment.

This section explains how to create M-CNCC IAM database and grant permissions to the CNC Console IAM database user for relevant operations on the database.

> **Note**
>
> As the CNC Console instances cannot share the same database, user must provide a unique name to the CNC Console database in the DBTier either limited to a site or spanning across sites.
>
> The recommended format for database name is as follows:
>
> `<database-name>_<site-name>_<cluster>`
>
> Sample database name: `cnccdb_site1_cluster1`
>
> While choosing the name of the database, make sure the following requirements are met:
>
> - It starts and ends with an alphanumeric character.
> - It contains 63 characters or less.
> - It contains only alphanumeric characters or '-'.
>
> In this guide, the commands use "cnccdb" as sample database name. If a custom database name is used, user must use it in place of cnccdb.

1. Log in to the server or machine with permission to access the SQL nodes of NDB cluster.
2. Run the following command to connect to the SQL node of the NDB cluster or connect to the cnDbTier

   ```
   $ kubectl -n <cndbtier_namespace> exec -it <cndbtier_sql_pod_name> -c
   <cndbtier_sql_container_name> -- bash
   ```

   For example:

   ```
   $ kubectl -n cndbtier  exec -it ndbappmysqld-0 -c mysqlndbcluster -- bash
   ```

3. Run the following command to log in to the MySQL prompt as a user with root permissions, which has permission to create users with permissions:

   ```
   mysql -h 127.0.0.1 -u root -p
   ```

   > **Note**
   >
   > After writing the command, user will be prompted to enter the mysql password. Provide MySql password.

4. Run the following command to check if cnccdb already exists:

   ```
   show databases;
   ```

5. Run the following command to drop the existing cnccdb database:

   ```
   DROP DATABASE <CNCC IAM Database>
   ```

6. Run the following command to create the cnccdb:

   ```
   $ CREATE DATABASE IF NOT EXISTS <CNCC IAM Database>;
   ```

   For example:

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

7. Run the following command to grant permission to cncc-user:

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

   For example:

   ```
   $ GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, REFERENCES,
   INDEX, CREATE TEMPORARY TABLES, DELETE, UPDATE, EXECUTE ON cnccdb .*
   TO'cnccusr'@'%';
   ```

2.2.1.6.3 Configuring M-CNCC Core Database

This section explains how to create M-CNCC Core database (*mcncccommonconfig*) and grant permissions to the M-CNCC Core database user for relevant operations on the *mcncccommonconfig* Database.

> **Note**
>
> In this installation guide, the commands use "mcncccommonconfig" as sample db name. The sample db name "mcncccommonconfig" must be replaced to the name chosen as per naming conventions defined by this note.

1. Log in to the server or machine which has permission to access the SQL nodes of the NDB cluster.
2. Connect to the SQL node of the NDB cluster or connect to the cnDBTier.
   Run the following command to connect to the cnDBTier:

   ```
   $ kubectl -n <cndbtier_namespace> exec -it <cndbtier_sql_pod_name> -c
   <cndbtier_sql_container_name> -- bash
   ```

   Example:

   ```
   $  kubectl -n occne-cndbtier  exec -it ndbappmysqld-0 -c mysqlndbcluster
   -- bash
   ```

3. Log in to the MySQL prompt using root permission or as a user with permission to create new users (with permissions).

   ```
   $ mysql -h 127.0.0.1 -u root -p
   ```

   > **Note**
   >
   > After running the command mentioned above, user must enter MySQL password.

4. Run the following command to check if Database *mcncccommonconfig* exists:

   ```
   $ show databases;
   ```

5. Run the following command to create a mcncccommonconfig, if the mcncccommonconfig does not exist:

   ```
   $ CREATE DATABASE IF NOT EXISTS <M-CNCC Common Config Database>;
   ```

6. Run the following command to grant permission to cncc-user:

   ```
   $ GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE TEMPORARY
   TABLES, DELETE, UPDATE,
   EXECUTE ON <M-CNCC Core Common Config Database>.* TO'<CNCC User Name>'@'%';
   ```

Example to demonstrate mcncccommonconfig creation, and granting permissions to cncc user:

```
# Command to check if database exists:
$ show databases;
# Database creation for CNCC mcncccommonconfig if do not exists
$ CREATE DATABASE IF NOT EXISTS mcncccommonconfig;
# Granting permission to user:
$ GRANT SELECT, INSERT, CREATE, ALTER, DROP, LOCK TABLES, CREATE TEMPORARY
TABLES, DELETE, UPDATE, EXECUTE ON mcncccommonconfig .* TO'cnccusr'@'%';
```

2.2.1.7 Configuring Kubernetes Secret

This section explains how to configure Kubernetes secrets for accessing the database and the M-CNCC IAM default user.

2.2.1.7.1 Configuring Kubernetes Secret for Accessing Database

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

1. Run the following command to create the kubernetes secret:

```
kubectl create secret generic <database secret name> --from-
literal=dbUserNameKey=<CNCC MySQL database username> --from-
literal=dbPasswordKey='<CNCC MySQL database passsword>' -n <Namespace of
MySQL secret>
```

> **Note**
>
> You must use a strong non-predictable password consisting of complex strings of more than 10 mixed characters.

2. Verify the secret created using following command:

```
kubectl describe secret <database secret name> -n <Namespace of MYSQL
secret>
```

Example:

```
$ kubectl create secret generic cncc-db-secret --from-
literal=dbUserNameKey=cnccusr --from-literal=dbPasswordKey='<db password>'
-n cncc
$ kubectl describe secret cncc-db-secret -n cncc
```

2.2.1.7.2 Configuring Secret for the Admin User in M-CNCC IAM

> **Note**
>
> Not applicable for OCI Deployment.

To create and update Kubernetes secret for default (admin) user:

1. Run the following command to create the Kubernetes secret for admin user:

```
$ kubectl create secret generic <secret-name> --from-
literal=iamAdminPasswordKey='<password>'--namespace <namespace>
```

Example:

```
$ kubectl create secret generic cncc-iam-secret --from-
literal=iamAdminPasswordKey='password' --namespace cncc
```

> **Note**
>
> This Command is just for reference. You must use a strong non-predictable password consisting of complex strings of more than 10 mixed characters.

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

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

Example:

```
$ kubectl describe secret cncc-iam-secret -n cncc
```

2.2.1.7.3 Configuring OCI IAM Secret

> **Note**
>
> Applicable only for OCI deployment.

This section describes the procedure to configure OCI IAM Secret with clientId and clientSecret for M-CNCC Core and A-CNCC Core:

1. Run the following command to create Kubernetes secret for OCI IAM clientId and clientSecret:

```
$ kubectl create secret generic <secret-name> --from-
literal=clientId='<clientId>' --from-literal=clientSecret='<clientSecret>'
--namespace <namespace>
```

For example:

```
$ kubectl create secret generic oci-iam-secret --from-
literal=clientId='269d98xxxxbb5064'--from-
literal=clientSecret='6779exxxxx9602' --namespace cncc
```

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

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

For example:

```
$ kubectl describe secret oci-iam-secret -n cncc
```

> **Note**
>
> For getting **clientId** and **clientSecret** for OCI IAM, see the How to access ClientId and ClientSecret of OCI IAM section in the *Oracle Communications Cloud Native Configuration Console User Guide.*

2.2.1.7.4 Configuring OCI IAM Secret With Admin Username and Password

> **Note**
>
> - Applicable only for OCI deployment.
> - You need OCI IAM admin user credentials to create the oci-iam-admin-secret. For more information, see the Oracle Cloud Infrastructure Documentation.

Perform the following procedure to configure OCI IAM secet with admin username and password:

1. Run the following command to create the Kubernetes secret for OCI IAM admin username and password. Replace `<username>` with the admin username and `<password>` with the admin password:

   ```
   $ kubectl create secret generic oci-iam-admin-secret --from-
   literal=username='<username>' --from-literal=password='<password>' --
   namespace <namespace>
   ```

2. Run the following command to verify that the secret has been created:

   ```
   $ kubectl describe secret oci-iam-admin-secret -n <namespace>
   ```

   For example:

   ```
   $ kubectl describe secret oci-iam-admin-secret -n cncc
   ```

2.2.1.8 Configuring Secrets for Enabling HTTPS

Following files must be present prior to configuring secrets for CNC Console for HTTPs deployment:

1. The Root Certificate Authority (CA) (caroot.cer) and its associated private Key (caroot.key) are required.

> **Note**
>
> If the Root Certificate Authority (CA) and its associated private Key are not available from your organization, generate a Self-Signed Root CA and its Key.

a. If the initial algorithm is ES256, an ECDSA Root CA Certificate (ssl_ecdsa_certificate.crt) along with its private key (ssl_ecdsa_private_key.pem) are necessary.

b. If the initial algorithm is RSA256, an RSA Root CA Certificate (ssl_rsa_certificate.crt) along with its private key (ssl_rsa_private_key.pem) are necessary.

2. A CA Bundle (cabundle.cer) is needed in case multiple Root CA Certificates are involved.

```
-----BEGIN CERTIFICATE-----
MIID4TCC...
...
...jtUl/zQ==
-----END CERTIFICATE-----
--------
-----BEGIN CERTIFICATE-----
MIID4TCC...
...
...jtUl/zQ==
-----END CERTIFICATE-----
--------
-----BEGIN CERTIFICATE-----
MIID4TCC...
...
...jtUl/zQ==
-----END CERTIFICATE-----
```

3. Additionally, files containing passwords for the TrustStore (ssl_truststore.txt) and KeyStore (ssl_keystore.txt) are required.

> **Note**
>
> The creation process for private keys, CA Root Certificates, CA Bundle and passwords is left to the discretion of the user or operator. The CNC Console does not document these procedures.

2.2.1.8.1 Configuring Secret to Enable HTTPS in M-CNCC IAM

> **Note**
>
> Not applicable for OCI deployment.

This section describes how create and configure secrets to enable HTTPS. This section must be executed before configuring secret to enable HTTPS CNC Console Core Ingress Gateway.

Following files must be present prior to configure secrets for M-CNCC IAM for HTTPs deployment.

1. If the initial algorithm is ES256, an ECDSA Intermediate Certificate (ssl_ecdsa_certificate.crt) along with its private key (ssl_ecdsa_private_key.pem) signed by Root CA.
2. If the initial algorithm is RSA256, an RSA Root CA Certificate (ssl_rsa_certificate.crt) along with its private key (ssl_rsa_private_key.pem) signed by Root CA.

1. Run the following command to create secret:

```
$ kubectl create secret generic <secret-name> --from-
file=<ssl_ecdsa_private_key.pem>
      --from-file=<rsa_private_key_pkcs1.pem> --from-
file=<ssl_truststore.txt>
      --from-file=<ssl_keystore.txt> --from-file=<caroot.cer> --from-
file=<cabundle.cer>
      --from-file=<ssl_rsa_certificate.crt> --from-
file=<ssl_ecdsa_certificate.crt> -n <Namespace of CNCC
      IAM Ingress Gateway secret>
```

> **Note**
>
> Note down the command used during the creation of Kubernetes secret as this command is used for future updates.

For example:

```
$ kubectl create secret generic cncc-iam-ingress-secret
        --from-file=ssl_ecdsa_private_key.pem  --from-
file=rsa_private_key_pkcs1.pem
        --from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=caroot.cer
        --from-file=cabundle.cer --from-file=ssl_rsa_certificate.crt
        --from-file=ssl_ecdsa_certificate.crt -n cncc
```

> **Note**
>
> The names used in the above command must be as same as the names provided in the custom_values.yaml in CNC Console deployment.

2. On successfully running the above command, the following message is displayed:
   secret/cncc-iam-ingress-secret created
3. Run the following command to verify the secret creation:

```
$ kubectl describe secret cncc-iam-ingress-secret -n cncc
```

Perform the following procedure to update existing secrets to enable HTTPS, if they already exist:

1. Run the following command to create secret:

```
$ kubectl create secret generic <secret-name> --from-
file=<ssl_ecdsa_private_key.pem> --from-file=<rsa_private_key_pkcs1.pem> --
from-file=<ssl_truststore.txt> --from-file=<ssl_keystore.txt> --from-
```

```
file=<caroot.cer> --from-file=<ssl_rsa_certificate.crt> --from-
file=<ssl_ecdsa_certificate.crt> --dry-run -o yaml -n <Namespace of CNCC
IAM Ingress Gateway secret> | kubectl replace -f --n <Namespace of CNCC
IAM Ingress Gateway secret>
```

For xample:

```
$ kubectl create secret generic cncc-iam-ingress-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=caroot.cer --from-file=ssl_rsa_certificate.crt --from-
file=ssl_ecdsa_certificate.crt --dry-run -o yaml -n cncc | kubectl replace
-f --n cncc
```

2. On successfully running the above command, the following message is displayed:
   secret/cncc-iam-ingress-secret replaced

Dynamic Reloading of Certificates of M-CNCC IAM

Perform the following procedure for configuring CNC Console IAM to Support Dynamic Reloading of Certificates of M-CNCC IAM:

CNC Console supports Dynamic Reload of Certificates that are used to establish both TLS and mTLS connections.

To enable dynamic reloading of certificates, the following flags must be enabled in the *occncc_custom_values_<version>.yaml* file.

```
cncc-iam:
  global:
    ingressGwCertReloadEnabled: &iamIGwCertReloadEnabled true
```

> **Note**
>
> The new certificate must be created with the existing secret and certificate name.

The procedure for dynamic reloading of certificates as follows:

1. Delete the existing certificates with which existing secure connections were established.
2. Create the new certificate as per the requirement. The certificate must be created with the same name as the existing certificate.
3. The Ingress Gateway pods automatically pick up the new certificates and the changes will be reflected in the browser.

> **Note**
>
> **Naming Update of Certificates and Secrets**
> If the name of the secret or the certificate is changed then the corresponding changes must be made in the *occncc_custom_values_<version>.yaml* file, and either a reinstall or a helm upgrade must be done.

2.2.1.8.2 Configuring Secret to Enable HTTPS in M-CNCC Core

This section describes how to create secret configuration for enabling HTTPS. This section must be run before enabling HTTPS in CNC Console Core Ingress Gateway.

> **Note**
>
> **For OCI:**
>
> 1. Download OCI IAM Root CA Certificates
>   a. Obtain the Intermediate Root CA: **DigiCert TLS RSA SHA256 2020 CA1** from the specified URL: https://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt.pem.
>   b. Acquire the Root CA: **DigiCert Global Root CA** from the following link: https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem.
> 2. Create a CA Bundle with OCI IAM Root CA Certificates and CNC Console Root CA Certificates (Organization or Self-Signed).
> 3. Create M-CNCC Core secret with the CA Bundle.

> **Note**
>
> - For single cluster deployment, both M-CNCC Core and A-CNCC Core can use same configurations as both reside in same cluster namespace.
> - For multicluster deployment, configurations need to be created on both the clusters separately.

Prerequisite

Following files must be present prior to configuring secrets for M-CNCC Core for HTTPs deployment:

1. If the initial algorithm is ES256, an ECDSA Intermediate Certificate (ssl_ecdsa_certificate.crt) along with its private key (ssl_ecdsa_private_key.pem) signed by Root CA.
2. If the initial algorithm is RSA256, an RSA Root CA Certificate (ssl_rsa_certificate.crt) along with its private key (ssl_rsa_private_key.pem) signed by Root CA.

1. Run the following command to create secret:

```
$ kubectl create secret generic <secret-name> --from-
file=<ssl_ecdsa_private_key.pem> --from-file=<rsa_private_key_pkcs1.pem> --
from-file=<ssl_truststore.txt> --from-file=<ssl_keystore.txt> --from-
file=<caroot.cer> --from-file=<cabundle.cer>--from-
file=<ssl_rsa_certificate.crt> --from-file=<ssl
```

> **Note**
>
> Note down the command used during the creation of kubernetes secret, this command is used for updates in future.

For example:

```
kubectl create secret generic cncc-core-ingress-secret --from-
file=ssl_ecdsa_private_key.pem --from-file=rsa_private_key_pkcs1.pem --
from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=caroot.cer --from-file=ssl_rsa_certificate.crt --from-
file=ssl_ecdsa_certificate.crt -n cncc
```

On successfully running the above command, the following message will be displayed:
secret/cncc-core-ingress-secret created

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

```
$ kubectl describe secret cncc-core-ingress-secret -n cncc
```

Perform the following procedure to update existing secrets to enable HTTPS:

1. Run the following command to create secret:

```
$ kubectl create secret generic <secret-name> --from-
file=<ssl_ecdsa_private_key.pem> --from-file=<rsa_private_key_pkcs1.pem> --
from-file=<ssl_truststore.txt> --from-file=<ssl_keystore.txt> --from-
file=<caroot.cer> --from-file=<ssl_rsa_certificate.crt> --from-
file=<ssl_ecdsa_certificate.crt> --dry-run -o yaml -n <Namespace of M-CNCC
Core Ingress Gateway secret> | kubectl replace -f - -n <Namespace of CNC
Console Core Ingress Gateway secret>
```

For example:

```
$ kubectl create secret generic cncc-core-ingress-secret --from-
file=ssl_ecdsa_private_key.pem  --from-file=rsa_private_key_pkcs1.pem --
from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=caroot.cer --from-file=ssl_rsa_certificate.crt --from-
file=ssl_ecdsa_certificate.crt --dry-run -o yaml -n cncc | kubectl replace
-f - -n cncc
```

2. On successfully running the above command, the following message will be displayed:
secret/cncc-core-ingress-secret replaced

Dynamic Reloading of Certificates of M-CNCC Core

CNC Console supports dynamic reloading of certificates that are used to establish both TLS and mTLS connections. To enable dynamic reloading of certificates, the following flags must be enabled in the *occncc_custom_values_<version>.yaml* file.

```
mcncc-core:
  global:
```

```
ingressGwCertReloadEnabled: & mcoreIGwCertReloadEnabled true
```

> **Note**
>
> Here, the new certificate must be created with the existing secret and certificate name.

The procedure for dynamic reloading of certificates is as follows:

1. Delete the existing certificates with which existing secure connections were established.
2. Create the new certificate as per the requirement. The certificate must be created with the same name as the existing certificate.
3. The Ingress Gateway pods automatically pick up the new certificates and the changes are reflected in the browser.

> **Note**
>
> **Naming update of Certificates and Secrets**
>
> If the name of the secret or the certificate is changed, then the corresponding changes must be made in the *occncc_custom_values_<version>.yaml* file, and either a reinstall or a helm upgrade must be done.

2.2.1.8.3 Configuring Secret to Enable HTTPS in A-CNCC Core

This section describes how create and configure secrets to enable HTTPS. This section must be run before configuring secret to enable HTTPS CNC Console Core Ingress Gateway.

> **Note**
>
> **For OCI**
>
> 1. Download OCI IAM Root CA Certificates
>   a. Obtain the Intermediate Root CA: **DigiCert TLS RSA SHA256 2020 CA1** from the specified URL: https://cacerts.digicert.com/DigiCertTLSRSASHA2562020CA1-1.crt.pem.
>   b. Acquire the Root CA: **DigiCert Global Root CA** from the provided link: https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem.
> 2. Create a CA Bundle with OCI IAM Root CA Certificates and CNC Console Root CA Certificates (Organization or Self-Signed).
> 3. Create A-CNCC Core secret with the CA Bundle.

> **Note**
>
> - For single cluster deployment, both M-CNCC Core and A-CNCC Core can use same configurations as both reside in same cluster namespace.
> - For multicluster deployment configurations need to be created on both the clusters separately.

Prerequisite

Following files must be present prior to configuring secrets for A-CNCC Core for HTTPs deployment:

1. If the initial algorithm is ES256, an ECDSA Intermediate Certificate (ssl_ecdsa_certificate.crt) along with its private key (ssl_ecdsa_private_key.pem) signed by Root CA.
2. If the initial algorithm is RSA256, an RSA Root CA Certificate (ssl_rsa_certificate.crt) along with its private key (ssl_rsa_private_key.pem) signed by Root CA.

Procedure:

1. Run the following command to create secret:

```
$ kubectl create secret generic <secret-name> --from-
file=<ssl_ecdsa_private_key.pem>
        --from-file=<rsa_private_key_pkcs1.pem> --from-
file=<ssl_truststore.txt>
        --from-file=<ssl_keystore.txt> --from-file=<caroot.cer> --from-
file=<cabundle.cer>
        --from-file=<ssl_rsa_certificate.crt> --from-
file=<ssl_ecdsa_certificate.crt> -n <Namespace of
        CNCC Core Ingress Gateway secret>
```

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

For example:

The names used below are same as provided in custom values.yaml in CNC Console Core deployment

```
$ kubectl create secret generic cncc-core-ingress-secret
        --from-file=ssl_ecdsa_private_key.pem  --from-
file=rsa_private_key_pkcs1.pem
        --from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
file=caroot.cer
        --from-file=cabundle.cer --from-file=ssl_rsa_certificate.crt
        --from-file=ssl_ecdsa_certificate.crt -n cncc
```

On successfully running the above command, the following message will be displayed:
secret/cncc-core-ingress-secret created

2. Run the following command to verify the secret creation:
   ```
   $ kubectl describe secret cncc-core-ingress-secret -n cncc
   ```

Perform the following procedure to update existing secrets to enable HTTPS:

- Copy the exact command used in preveious section during creation of secret. Update the same command with string "--dry-run -o yaml" and "kubectl replace -f - -n <Namespace of CNCC Core Ingress Gateway secret>". The command will become:

  ```
  $ kubectl create secret generic <secret-name> --from-
  file=<ssl_ecdsa_private_key.pem>
          --from-file=<rsa_private_key_pkcs1.pem> --from-
  file=<ssl_truststore.txt>
          --from-file=<ssl_keystore.txt> --from-file=<caroot.cer> --from-
  file=<cabundle.cer>
          --from-file=<ssl_rsa_certificate.crt> --from-
  file=<ssl_ecdsa_certificate.crt> --dry-run -o yaml
          -n <Namespace of CNCC Core Ingress Gateway secret> | kubectl
  replace -f - -n <Namespace of CNCC
          Core Ingress Gateway secret>
  ```

  For example:

  ```
  $ kubectl create secret generic cncc-core-ingress-secret
          --from-file=ssl_ecdsa_private_key.pem  --from-
  file=rsa_private_key_pkcs1.pem
          --from-file=ssl_truststore.txt --from-file=ssl_keystore.txt --from-
  file=caroot.cer
          --from-file=cabundle.cer --from-file=ssl_rsa_certificate.crt
          --from-file=ssl_ecdsa_certificate.crt --dry-run -o yaml -n cncc |
  kubectl replace -f - -n
          cncc
  ```

  The names used here are the same as the ones given in the custom values.yaml in CNC Console Core deployment.

- The following message appears when you execute the above command:`secret/cncc-core-ingress-secret replaced`

Dynamic Reloading of Certificates of A-CNCC Core

CNC Console supports dynamic reloading of certificates that are used to establish both TLS and mTLS connections. To enable dynamic reloading of certificates, the following flags must be enabled in the *occncc_custom_values_<version>.yaml* file.

```
acncc-core:
  global:
     ingressGwCertReloadEnabled: &acoreIGwCertReloadEnabled true
```

Under this provision, we use the existing secret and the certificate name, but create a completely new certificate for the same name.

The procedure for dynamic reloading of certificates is as follows:

1. Delete the existing certificates with which existing secure connections were established.

2. Create the new certificate as per the requirement. The certificate must be created with the same name as the existing certificate.
3. The Ingress Gateway pods automatically pick up the new certificates and the changes are reflected in the browser.

> **Note**
>
> **Naming update of Certificates and Secrets**
>
> If the name of the secret or the certificate is changed, then the corresponding changes must be made in the *occncc_custom_values_<version>.yaml* file, and either a reinstall or a helm upgrade must be done.

2.2.1.9 Configuring CNC Console to support Aspen Service Mesh

> **Note**
>
> Not applicable for OCI deployment.

2.2.1.9.1 Introduction

CNC Console 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 cowork 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.x

For ASM installation and configuration, see the official Aspen Service Mesh website.

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 on 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. So, you need Envoy Filters to help in passing the headers from back-end services to use it as it is.

> **Note**
>
> For ASM installation and configuration, refer Official Aspen Service Mesh website for details.

2.2.1.9.2 Predeployment Configuration

Following are the prerequisites to install CNC Console with support for ASM:

Enabling Auto sidecar Injection for Namespace

This section explains how to enable auto sidecar injection for namespace.

1. Run the following command to enable auto sidecar injection to automatically add the sidecars in all of the pods spawned in CNC Console namespace:

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

   For example:

   ```
   $ kubectl label ns cncc istio-injection=enabled
   ```

Update Default Kyverno Policy Restriction to add CNC Console Namespace

> **Note**
>
> You need admin privileges to edit or patch the **clusterpolicies** that are mentioned in following steps.

From 23.2.0 CNE, we have support for Kyverno policies. The default Kyerno policy restrictions don't allow istio-proxy containers. To allow running of istio-proxy containers on CNC Console with ASM deployment, you must perform the following kubectl operation on the namespace where the CNC Console is installed.

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

For example,

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

Establish connectivity to services that are not part of Service Mesh Registry

> **Note**
>
> This is an optional step. Depending on the underlying Service Mesh deployment, Service Entry and Destination Rule may be required for CNC Console to connect to other kubernetes microservices that are not a part of Service Mesh Registry. The kubernetes microservices may be DB service, NF services, or Common services.

You can use the following sample service entry and destination rule template:

```
apiVersion: networking.istio.io/v1alpha3
kind: ServiceEntry
metadata:
  name: <Unique ServiceEntry Name for Service>
  namespace: <CNCC-NAMESPACE>
spec:
  exportTo:
  - "."
  hosts:
  - <Service-public-FQDN>
  ports:
  - number: <Service-public-PORT>
    name: <Service-PORTNAME>
    protocol: <Service-PROTOCOL>
  location: MESH_EXTERNAL
---
apiVersion: networking.istio.io/v1alpha3
```

```
kind: DestinationRule
metadata:
  name: <Unique DestinationRule Name for Service>
  namespace: <CNCC-NAMESPACE>
spec:
  exportTo:
  - "."
  host: <Service-public-FQDN>
  trafficPolicy:
    tls:
      mode: DISABLE
```

If Kubernetes services only have IP, and does not have public FQDN, then first create the necessary headless service, and then create Service Entry and Destination Rule. Here is a sample headless service template:

```
apiVersion: v1
kind: Endpoints
metadata:
  name: <Unique Endpoint Name for Service>
  namespace: <CNCC_NAMESPACE>
subsets:
- addresses:
  - ip: <Service-public-IP>
  ports:
  - port: <Service-public-PORT>
    protocol: <Service-PROTOCOL>
---
apiVersion: v1
kind: Service
metadata:
  name: <Unique Endpoint Name for Service>-headless
  namespace: <CNCC_NAMESPACE>
spec:
  clusterIP: None
  ports:
  - port: <Service-public-PORT>
    protocol: <Service-PROTOCOL>
    targetPort: <Service-public-PORT>
  sessionAffinity: None
  type: ClusterIP
```

Set the mTLS Connection from Client Browser to ASM

Prerequisites
Enable certificateCustomFields in ASM values.yaml

> **Note**
>
> Ensure that ASM is deployed with **certificateCustomFields** enabled.
>
> ```
> global:
>   certificateCustomFields: true
> ```

Using ASM self-signed CA (Default)

1. ASM creates *istio-ca* secrets (ca-certs, ca-key) in istio-namespace which contains CA public and private key.
   a. Run the following command to verify if the certificate is created:

      ```
      $ kubectl get secrets -n istio-system -o yaml istio-ca-secret
      ```

      > **Note**
      >
      > Export the ca-*cert.pem*, ca-*key.pem* from the secret **istio-ca-secret** to your local machine where browser is installed.
      >
      > ```
      > ca-cert.pem → Istio CA public
      >
      > ca-key.pem → CA private key
      > ```

   b. Run the following commands to get ASM Istio CA certificate with base64 decoded and copy the output to a file in you local machine:

      ```
      kubectl get secret istio-ca-secret -n istio-system -o go-
      template='{{ index .data "ca-cert.pem" | base64decode}}'
      kubectl get secret istio-ca-secret -n istio-system -o go-
      template='{{ index .data "ca-key.pem" | base64decode}}'
      ```

2. Create client certificate using Openssl commands using ca-cert.pem and ca-key.pem obtained in Step1, and import it to the browser. Refer to your browser specific documentation on how to import certificate and key.
3. Update the browser configuration to trust the CA certificate (ca-cert.pem) obtained from Step 1. Refer to your browser specific documentation on how to trust the CA certificate.

Existing Organization CA

1. Create client certificate using Openssl commands using Organization CA public and private key and import it to the browser. Refer to your browser specific documentation on how to import certificate and key.
2. Update the browser configuration to trust the Organization CA. Refer to your browser specific documentation on how to trust the CA certificate.

Create Service Account, Role and Role bindings with ASM annotations

While creating service account for M-CNCC IAM, M-CNCC Core, and A-CNCC Core, you need to provide following ASM annotations in the given format:

```
certificate.aspenmesh.io/customFields:'{"SAN":{"DNS":["<helm-release-name>-
ingress-gateway.<cncc_namespace>.svc.<cluster_domain>"]}}'
```

Sample ASM annotations for M-CNCC-IAM, M-CNCC, and A-CNCC

```
apiVersion: v1
kind: ServiceAccount
metadata:
  annotations:
    certificate.aspenmesh.io/customFields: '{ "SAN": { "DNS": [ "cncc-iam-
ingress-gateway.cncc.svc.cluster.local", "cncc-acore-ingress-
gateway.cncc.svc.cluster.local", "cncc-mcore-ingress-
gateway.cncc.svc.cluster.local"] } }'
```

Single Cluster Deployment

For single cluster deployment, where M-CNCC IAM, M-CNCC Core and A-CNCC Core are deployed in same cluster or site, can share same service account, role, and rolebinding.

Sample example for M-CNCC IAM, M-CNCC Core, and A-CNCC Core| cncc-sa-role-rolebinding.yaml

```
kubectl apply -n cncc -f - <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cncc-serviceaccount
  labels:
    app.kubernetes.io/component: internal
  annotations:
    sidecar.istio.io/inject: "false"
    "certificate.aspenmesh.io/customFields": '{ "SAN": { "DNS": [ "cncc-iam-
ingress-gateway.cncc.svc.cluster.local", "cncc-acore-ingress-
gateway.cncc.svc.cluster.local", "cncc-mcore-ingress-
gateway.cncc.svc.cluster.local"] } }'
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: cncc-role
  labels:
    app.kubernetes.io/component: internal
  annotations:
    sidecar.istio.io/inject: "false"
rules:
- apiGroups:
  - "" # "" indicates the core API group
  resources:
  - services
```

```
  - configmaps
  - pods
  - secrets
  - endpoints
  - persistentvolumeclaims
  verbs:
  - get
  - watch
  - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: cncc-rolebinding
  labels:
    app.kubernetes.io/component: internal
  annotations:
    sidecar.istio.io/inject: "false"
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: cncc-role
subjects:
- kind: ServiceAccount
  name: cncc-serviceaccount
---
EOF
```

Multi Cluster Deployment
For Multi cluster deployment,

1. Where M-CNCC IAM, M-CNCC Core and A-CNCC Core are deployed in same site/cluster can share same service account, role and rolebinding.
   See the above single cluster service account example.

   > **Note**
   >
   > In multicluster deployment, A-CNCC Core is an optional component in manager cluster. Ensure that you take out "cncc-ccore-ingress-gateway.cncc.svc.cluster.local" from "certificate.aspenmesh.io/customFields" in case A-CNCC Core is not deployed in manager cluster.

2. Where M-CNCC IAM and M-CNCC Core, which are in same cluster, can still share same service account, role and rolebinding and A-CNCC deployed in different cluster, a separate service account, role and rolebinding needs to be created.
   Example for M-CNCC IAM, M-CNCC Core | cncc-sa-role-rolebinding.yaml:

   ```
   kubectl apply -n cncc -f - <<EOF
   apiVersion: v1
   kind: ServiceAccount
   metadata:
     name: cncc-serviceaccount
     labels:
       app.kubernetes.io/component: internal
     annotations:
   ```

```
    sidecar.istio.io/inject: "false"
    "certificate.aspenmesh.io/customFields": '{ "SAN": { "DNS": [ "cncc-
iam-ingress-gateway.cncc.svc.cluster.local", "cncc-mcore-ingress-
gateway.cncc.svc.cluster.local"] } }'
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: cncc-role
  labels:
    app.kubernetes.io/component: internal
  annotations:
    sidecar.istio.io/inject: "false"
rules:
- apiGroups:
  - "" # "" indicates the core API group
  resources:
  - services
  - configmaps
  - pods
  - secrets
  - endpoints
  - persistentvolumeclaims
  verbs:
  - get
  - watch
  - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: cncc-rolebinding
  labels:
    app.kubernetes.io/component: internal
  annotations:
    sidecar.istio.io/inject: "false"
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: cncc-role
subjects:
- kind: ServiceAccount
  name: cncc-serviceaccount
---
EOF
```

Example for A-CNCC Core | cncc-sa-role-rolebinding.yaml

```
kubectl apply -n cncc -f - <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cncc-serviceaccount
  labels:
    app.kubernetes.io/component: internal
```

```
  annotations:
    sidecar.istio.io/inject: "false"
    "certificate.aspenmesh.io/customFields": '{ "SAN": { "DNS": [ "cncc-
acore-ingress-gateway.cncc.svc.cluster.local"] } }'
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: cncc-role
  labels:
    app.kubernetes.io/component: internal
  annotations:
    sidecar.istio.io/inject: "false"
rules:
- apiGroups:
  - "" # "" indicates the core API group
  resources:
  - services
  - configmaps
  - pods
  - secrets
  - endpoints
  - persistentvolumeclaims
  verbs:
  - get
  - watch
  - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: cncc-rolebinding
  labels:
    app.kubernetes.io/component: internal
  annotations:
    sidecar.istio.io/inject: "false"
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: cncc-role
subjects:
- kind: ServiceAccount
  name: cncc-serviceaccount
---
EOF
```

2.2.1.9.3 M-CNCC IAM, M-CNCC Core and A-CNCC Core configuration for ASM

This section explains about the CNC Console IAM deployment configuration for ASM.

Update *occncc_custom_values_<version>.yaml* as follows:

1. Add the following sidecar resource configuration annotations:

```
global:
  # ********  Sub-Section Start: Common Global Parameters *************
```

```
  # ********************************************************************

  customExtension:
    allResources:
      labels: {}
      annotations:
        sidecar.istio.io/proxyMemory: "1Gi"
        sidecar.istio.io/proxyMemoryLimit: "1Gi"
        sidecar.istio.io/proxyCPU: "1"
        sidecar.istio.io/proxyCPULimit: "1"

  # ********  Sub-Section End: Common Global Parameters ******************
  # ********************************************************************
```

2. Add rewriteAppHTTPProbers annotation to make health checks on services with mTLS enforcement on work:

```
global:
  # ********  Sub-Section Start: Common Global Parameters *************
  # ********************************************************************

    nonlbStatefulSets:
      labels: {}
      annotations:
        sidecar.istio.io/rewriteAppHTTPProbers: "true"

  # ********  Sub-Section End: Common Global Parameters ******************
  # ********************************************************************
```

3. Provide the service account name:

```
global:
  # *****  Sub-Section Start: Ingress Gateway Global Parameters *****
  serviceAccountName: &serviceAccountName <cncc-serviceaccount-name>
```

4. Enable Service Mesh Flag:

```
global:
  # Mandatory: This flag needs to set it "true" if Service Mesh would be
present where CNC Console will be deployed
  serviceMeshCheck: true
```

5. If ASM is deployed with mTLS disabled, then set **serviceMeshHttpsEnabled** flag to *false*:

```
global:
  serviceMeshHttpsEnabled: false
```

2.2.1.9.4 M-CNCC IAM, M-CNCC Core, and A-CNCC Core Configuration for OSO

Add Annotation **oracle.com/cnc: "true"** under *global.customExtention.lbDeployments.annotations* section in

occncc_custom_values_<version>*.yaml* file to indicate OSO to scrape metrics from ingress pod.

```
global:
  # ****  Sub-Section Start: Common Global Parameters *****


  customExtension:
    lbDeployments:
      labels: {}
      annotations:
        oracle.com/cnc: "true"

  # ****  Sub-Section End: Common Global Parameters *******
```

2.2.1.10 Configuring Network Policies

> **Note**
>
> Not applicable for OCI deployment.

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

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

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

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

Configuring Network Policies

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

Installing Network Policies

Prerequisite

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

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

1. Open the *occncc_network_policy_custom_values_<version>.yaml* file provided in the release package zip file. For downloading the file, see Downloading CNC Console Package and Pushing the Images to Customer Docker Registry.
2. The file is provided with the default network policies. If required, update the *occncc_network_policy_custom_values_<version>.yaml* file. For more information on the parameters, see the Configuration Parameters for network policy parameter table.
3. Run the following command to install the network policies:

   ```
   helm install <release_name> -f
   <occncc_network_policy_custom_values_<version>.yaml> --namespace
   <namespace> <chartpath>./<chart>.tgz
   ```

   For example:

   ```
   helm install occncc-network-policy -f
   occncc_network_policy_custom_values_24.1.1.yaml --namespace cncc occncc-
   network-policy-24.1.1.tgz
   ```

   Where,

   - `helm-release-name`: occncc-network-policy helm release name.
   - `custom-value-file`: occncc-network-policy custom value file.
   - `namespace`: CNC Console namespace.
   - `network-policy`: network-policy package.

> **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.

Upgrading Network Policies

1. Modify the *occncc_network_policy_custom_values_<version>.yaml* file to update, add, or delete the network policy.

2. Run the following command to upgrade the network policies:

```
helm upgrade <release_name> -f
occncc_network_policy_custom_values_<version>.yaml --namespace <namespace>
<chartpath>./<chart>.tgz
```

For example:

```
helm upgrade occncc-network-policy -f
occncc_network_policy_custom_values_24.1.1.yaml --namespace cncc occncc-
network-policy-24.1.1.tgz
```

Verifying Network Policies

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

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

For example:

```
kubectl get networkpolicy -n cncc
```

Uninstalling Network Policies

Run the following command to uninstall the network policies:

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

For example:

```
$ helm uninstall occncc-network-policy --namespace cncc
```

> **Note**
>
> Uninstalling removes all the network policies.

Configuration Parameters for Network Policies

Table 2-13 Configuration Parameters for Network Policies

Parameter	Description	Details
apiVersion	This is a mandatory parameter. This indicates 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

Table 2-13 (Cont.) Configuration Parameters for Network Policies

Parameter	Description	Details
kind	This is a mandatory parameter. This represents the REST resource this object represents.**Note:**This is a read-only parameter.	**Data Type:** String **Default Value:** NetworkPolicy

Supported parameters for Configuring Network Policies

Table 2-14 Supported parameters for Configuring Network Policies

Parameter	Description	Details
metadata.name	This is a mandatory parameter. Specifies a unique name for the network policy.	{{ .metadata.name }}
spec.{}	This is a mandatory parameter. This consists of all the information needed to define a particular network policy in the given namespace.	NA

For more information about this functionality, see Network Policies in the *Oracle Communications Cloud Native Configuration Console User Guide*.

2.2.1.11 Global Configurations

CNC Console Deployment Configurations

This section explains about the CNC Console global configurations which are common for M-CNCC and A-CNCC deployment.

Table 2-15 Non OCI

Deployment	isMultiClusterDeployment enabled	oci-iam enabled	cncc-iam enabled	mcncc-core enabled	acncc-core enabled
Single Cluster	false	false	true	true	true
Multi Cluster(manager only)	true	false	true	true	false
Multi Cluster(managing local NF's)	true	false	true	true	true
Multi cluster(agent only)	true	false	false	false	true

Example: Configuration in *occncc_custom_values_<version>.yaml* file.

In case of single cluster deployment (*global.isMultiClusterDeployment: false*) the user must configure cncc-iam, mcncc-core and acncc-core flag to true and oci-iam flag to false.

```
global:

  isMultiClusterDeployment: false

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true
```

OCI

> **Note**
>
> For OCI deployment, only Single cluster is supported.

Table 2-16 OCI

Deployment	isMultiClusterDeployment enabled	cncc-iam enabled	mcncc-core enabled	acncc-core enabled
Single Cluster	false	false	true	true

Example: Configuration in *occncc_custom_values_<version>.yaml*

In case of single cluster deployment(*global.isMultiClusterDeployment: false*) the user must configure oci-iam, mcncc-core and acncc-core flag to true and cncc-iam flag to false.

```
global:

  isMultiClusterDeployment: false

  oci-iam:
```

```
    enabled: true
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true
```

2.2.1.11.1 M-CNCC IAM Predeployment Configuration

The following are the predeployment configuration procedures of M-CNCC IAM:

> **Note**
>
> Not applicable for OCI deploymemnt.

2.2.1.11.1.1 Configuring LDAPS in M-CNCC IAM

This section explains the procedure to enable LDAPS in M-CNCC IAM.

When you configure a secured connection URL to your LDAP store (Example: `ldaps://myhost.com:636'), CNC Console IAM uses SSL for communication with the LDAP server. The truststore must be properly configured on the CNC Console IAM server side; otherwise CNC Console IAM cannot trust the SSL connection to LDAP.

For enabling LDAPS update kc section of *occncc_custom_values_<version>.yaml* as below:

```
cncc-iam
  kc:
    ldaps:
      enabled: true
```

M-CNCC IAM Secret configuration for enabling LDAPS

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

To create Kubernetes secret for LDAPS, following files are required:

- TrustStore password file
- CA certificate or CA Bundle

Creating CA Bundle

When combining multiple CA certificates into a single certificate, add a delimiter after each certificate.

Delimiter: "--------"

Sample CA Bundle

```
-----BEGIN CERTIFICATE-----
MIID4TCC...
...
...jtUl/zQ==
-----END CERTIFICATE-----
--------
-----BEGIN CERTIFICATE-----
MIID4TCC...
...
...jtUl/zQ==
-----END CERTIFICATE-----
```

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

Perform the following procedure to create the secrets to enable LDAPS after required certificates and password files are generated and update details in kc section:

> **Note**
>
> The value of *ssl_truststore.txt* and *ssl_truststore-password-key* value must be same.

1. Run the following command to create secret:

   ```
   kubectl create secret generic <secret-name> --from-file=<caroot.cer> --
   from-file=ssl_truststore.txt --from-literal=ssl_truststore-password-
   key=<password> --namespace cncc
   ```

   > **Note**
   >
   > Note down the command used during the creation of Kubernetes secret as this command is used for future updates.

   For example:

   ```
   $ kubectl create secret generic cncc-iam-kc-root-ca --from-file=caroot.cer
   --from-file=ssl_truststore.txt --from-literal=ssl_truststore-password-
   key=<password> --namespace cncc
   ```

   Run the following to display the sample ssl_truststore.txt:

   ```
   echo <password> > ssl_truststore.txt
   ```

2. On successfully running the above command, the following message is displayed:
   secret/cncc-iam-kc-root-ca created

3. Run the following command to verify the secret creation:

```
$ kubectl describe secret cncc-iam-kc-root-ca -n cncc
```

M-CNCC IAM Service Account configuration for enabling LDAPS

This section describes the customizations that you should make in custom-value.yaml file to configure Kubernetes service account. M-CNCC IAM provides option to configure custom service account.

> **Note**
>
> Skip this section if service account is already configured as part of HTTPS or ASM configuration.

Configure service account for ingress-gateway and keycloak in *custom-cncc_values_<version>.yaml* as follows:

1. For ingress-gateway provide custom service account under *global.serviceAccountName.*

```
global:

  serviceAccountName: &serviceAccountName cncc-sa

cncc-iam:
  kc:
    keycloak:
      serviceAccount:
        # The name of the service account to use.
        name: *serviceAccountName
```

For CNC Console IAM LDAP related configurations, see *Integrating CNC Console LDAP Server with CNC Console IAM* section in Oracle Communications Cloud Native Core Console User Guide.

Sample Service account section in *custom-cncc_values_<version>.yaml*:

```
## Service account yaml file for cncc-sa
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cncc-sa
  namespace: cncc
  annotations: {}
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: cncc-role
  namespace: cncc
rules:
- apiGroups:
  - "" # "" indicates the core API group
  resources:
```

```
  - services
  - configmaps
  - pods
  - secrets
  - endpoints
  - persistentvolumeclaims
  verbs:
  - get
  - watch
  - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: cncc-rolebinding
  namespace: cncc
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: cncc-role
subjects:
- kind: ServiceAccount
  name: cncc-sa
  namespace: cncc
```

M-CNCC IAM LOG LEVEL Configuration

By default the log level of keycloak is set to **WARN**. To set the log level set the **enable** flag under **log** to **true**

In the **level** label, set the log level. Follow the below instruction about the options available to set log level

- **Log level**
  - TRACE.
  - DEBUG.
  - INFO.
  - WARN.
  - ERROR.
  - FATAL.
- **level: INFO**
  INFO, WARN, ERROR, FATAL will be covered for logs of all packages in KC
- **level: INFO, DEBUG**
  In this case it will take the last one as log level, here DEBUG
- **level: INFO, package-group: WARN**
  What does this mean?

  INFO level logs for all, but log level will be WARN only for that particular package. For example:

  ```
  level: INFO,org.keycloak:WARN,org.infinispan:WARN,org.jgroups:TRACE
  ```

level: OFF

No logs will appear

level: ALL

logs of all the level will appear in the logs

- Sample KC log configuration:

```
kc:
  preferIpv6Stack:
    enabled: false
  log:
    enabled: true
    level: DEBUG
```

2.2.1.11.2 A-CNCC Core Predeployment Configuration

Following are the predeployment configuration procedures:

2.2.1.11.2.1 Configuring A-CNCC Core mTLS

This section describes the A-CNCC Core Configuration for enabling mTLS.

> **Note**
>
> Not supported for OCI deployment.

mTLS Configuration at A-CNCC Core

mTLS must be enabled at the ingress-gateway SSL configuration section of the A-CNCC Core *occncc_custom_values_<version>.yaml* file. The parameter **scheme** must be set to https in the *occncc_custom_values_<version>.yaml* file.

Sample TLS Configuration section of A-CNCC Core:

```
acncc-core:
  global
    # CNCC https enabled
    httpsEnabled: &httpsEnabled true
    # Server Configuration for http and https support
    enableIncomingHttp: &enableIncomingHttp false
    enableIncomingHttps: &enableIncomingHttps true
    # Enables server with MTLS
    needClientAuth: &needClientAuth true
```

> **Note**
>
> While enabling mTLS, **needClientAuth** flag must be set to true.

2.2.1.11.2.2 Configuring M-CNCC IAM to Enable Additional Setting

CNC Console provides an option to enable additional settings in M-CNCC IAM by setting below mentioned flag to true in the `occncc_custom_values_<version>.yaml` file

The additional settings include some of the configuration settings such as authentication settings to configure password policies.

```
cncc-iam:
  global:
    iamSettingEnabled: false
```

2.2.2 Installation Tasks

This section explains how to install CNC Console. To install CNC Console using CDCS, see *Oracle Communications Cloud Native Core CD Control Server User Guide.*

> **Note**
>
> - Before installing CNC Console, you must complete the Prerequisites and Preinstallation Tasks.
> - In a georedundant deployment, perform the steps explained in this section on all georedundant sites.

This section describes the prerequisites and installation procedure for the CNC Console.

CNC Console helm chart is a common helm chart to be used for deploying Manager CNC Console IAM (M-CNCC IAM), Manager CNC Console Core (M-CNCC Core), and Agent CNCC Core (A-CNCC Core).

The scripts directory present in the `occncc_csar_<marketing-release-number>.zip` consists of `occncc_custom_values_<version>.yaml` file and can be used for deployment of M-CNCC IAM, M-CNCC Core and A-CNCC Core.

This section covers installation instructions for M-CNCC IAM, M-CNCC Core and A-CNCC Core deployment.

> **Note**
>
> - For a single cluster deployment, both Manager (M-CNCC) and Agent (A-CNCC) must deployed on the same cluster.
> - For a multicluster deployment,
>   - If the manager cluster has a local NF deployment, both M-CNCC and A-CNCC should be deployed on the same cluster
>   - If the manager cluster does not have a local NF deployment, only M-CNCC should be deployed. A-CNCC should be deployed on a cluster where NFs are present
> - The Manager manages CNE or OSO common service if present in a cluster.
>   - Manager in a cluster is preferred over Agent in the same cluster to manage the CNE common services.
>   - Agent in a cluster can manage CNE common service in absence of a Manager in the same cluster.
> - Agent is needed only when NFs are present on the cluster.

2.2.2.1 Installing CNC Console Package

This section provides the installation procedure to install CNC Console using Command Line Interface (CLI). To install CNC Console using CDCS, see *Oracle Communications Cloud Native Core CD Control Server User Guide.*

Perform the following procedure to deploy CNC Console:

1. Run the following command to check the version of the helm chart installation:

   ```
   helm search repo <release_name> -l
   ```

   For example:

   ```
   helm search repo cncc -l
   ```

   ```
   NAME             CHART VERSION  APP VERSION  DESCRIPTION
   ocspf-helm-repo/cncc      24.1.1         24.1.1     A Helm chart for CNC
   Console
   ```

2. Customize the `occncc_custom_values_<version>.yaml` file with the required deployment parameters. For customizing custom-cncc_values.yaml file, see CNC Console Configuration Parameters section.

   > **Note**
   >
   > **For Single or Dual Stack IP Configuration**
   > For IPv4 or IPv6 configurations, see Support for IPv4 or IPV6 Configuration for CNC Console.

Note

Assigning LoadBalancer IPs in CNE:

The annotation *metallb.universe.tf/address-pool: signaling/oam* is required in global section if MetalLB in CNE 1.8.x onwards is used.

```
customExtension:
  lbServices:
    labels: {}
    annotations:
     # The annotation metallb.universe.tf/address-pool:
signaling/oam is required if MetalLB in CNE 1.8.x is used
      metallb.universe.tf/address-pool: oam
      service.beta.kubernetes.io/oci-load-balancer-internal: "true"
```

Note

For HTTPs deployment in CNE:

The annotation `oracle.com.cnc/app-protocols: '{"http-tls":"TCP"}'` is required in the global section of *occncc_custom_values_<version>.yaml* file when CNC Console is deployed with HTTPs enabled in CNE.

```
customExtension:
  lbServices:
    labels: {}
    annotations:
      oracle.com.cnc/app-protocols: '{"http-tls":"TCP"}'
```

Note

For LDAP/LDAPS deployment:

The annotation `oracle.com.cnc/egress-network:` oam is required under the global section if Ldap or Ldaps is integrated with console.

```
nonlbStatefulSets:
  labels: {}
    annotations:
      oracle.com.cnc/egress-network: oam
```

Note

For MultiCluster deployment:

The annotation `oracle.com.cnc/egress-network: oam` is required under the global section if isMultiClusterDeployment flag is enabled for CNC Console.

```
customExtension:
    lbDeployments:
      labels: {}
      annotations:
        oracle.com.cnc/egress-network: oam
```

CNC Console IAM deployment has the following Pod Security context and Container Security context:
Pod Security context: `PSC: map[fsGroup:1000]`

Container Security context: `runAsUser:1000 runAsNonRoot:true`

> **Note**
>
> **For OCI:**
>
> - The following annotations musr be used to assign Network Load Balancer IP to the CNC Console Services in OCI environment. <subnet-OCID> is the OCID of the public subnet (nf_lb_subnet).
>
>   ```
>   customExtension:
>     lbServices:
>       labels: {}
>       annotations:
>         oci.oraclecloud.com/load-balancer-type: "nlb"
>         oci-network-load-balancer.oraclecloud.com/subnet: "<subnet-
>   OCID>"
>         oci-network-load-balancer.oraclecloud.com/security-list-
>   management-mode: All
>   ```
>
>   For example:
>
>   ```
>   customExtension:
>     lbServices:
>       labels: {}
>       annotations:
>         oci.oraclecloud.com/load-balancer-type: "nlb"
>         oci-network-load-balancer.oraclecloud.com/subnet:
>   "ocid1.subnet.oc1..aaaaaa....vdfw"
>         oci-network-load-balancer.oraclecloud.com/security-list-
>   management-mode: All
>   ```
>
>   For accessing subnet OCID, see the Getting Subnet's Details section in Oracle Cloud Infrastructure Documentation.
> - CNC Console must be deployed with HTTPs only in OCI. Non-HTTPs deployment of CNC Console is not supported in OCI.

Following configurations are needed in *occncc_custom_values_<version>.yaml* file. This includes configuring the following based on the deployment:

a. Update unique CNCC ID per cluster (global.self.cnccId).
b. Provide the details of M-CNCC IAMs or OCI-IAMs based on deployment (mCnccIams).
c. Provide the details of A-CNCC (aCnccs).
d. Provide the details of Agent Instances (instances).
e. In case of M-CNCC Core, provide the details of M-CNCC Cores and M-CNCC Instances (instances).

> **Note**
>
> - For instances configuration details, see the CNC Console Instances Configurations section and the CNC Console Instances Configuration Options section.
> - There are multiple M-CNCC, A-CNCC, NF Instances, and OCCNE Instances. You must be cautious while updating *occncc_custom_values_<version>.yaml* file.
> - In case of M-CNCC Core, *cmservice.envSystemName* in *occncc_custom_values_<version>.yaml* file can be used to display cluster name.
>   For example: envSystemName: CNCC - Site Name.
> - Route creation happens automatically. There is no need to provide routes in the Ingress Gateway section. Only instances details must be provided in the global section.
>
>   A-CNCC and M-CNCC Core use the same CNC Console helm chart, and only deployment configurations may differ.
> - See CNC Console Deployment Configuration Workflow section for details on deployment specific configuration updates.

3. The following are the Sample configuration section for CNC Console:

> **Note**
>
> **For OCI:**
> For deployment of CNC Console on OCI, in all the following sample configurations for different deployments, you must set **cncc-iam.enabled** flag to *false* and **oci-iam.enabled** flag to *true*:
>
> ```
> global:
>   oci-iam:
>     enabled: true
>   cncc-iam:
>     enabled: false
> ```
>
> For OCI, only single cluster configuration is applicable.

   a. **Single Cluster Deployment**
   Sample configuration section for CNC Console in case of single cluster deployment:

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
```

```
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.bumblebee
      port: 80
  instances:
    - id: Cluster1-grafana
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-grafana.occne-infra.svc.bumblebee
      apiPrefix: /bumblebee/grafana
    - id: Cluster1-kibana
      type: CS
      owner: Cluster1
      fqdn: occne-kibana.occne-infra.svc.bumblebee
      apiPrefix: /bumblebee/kibana
    - id: Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.scp.svc.bumblebee
      port: 80
```

> **Note**
>
> CNC Console only supports prometheus apiprefix and not promxy.

b. **Multicluster Deployment**
Sample configuration section for manager only deployment set cncc-iam, mcncc-core to "true" and acncc-core to "false":

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: false

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
```

```
    self:
      cnccId: Cluster1
    mCnccIams:
      - id: Cluster1
        ip: 10.xx.xx.xx
    mCnccCores:
      - id: Cluster1
    aCnccs:
      - id: Cluster2
        role: Cluster2
        ip: 10.xx.xx.xx
        port: 80
    instances:
      - id: Cluster1-grafana
        type: CS
        owner: Cluster1
        fqdn: occne-kube-prom-stack-grafana.occne-infra.svc.bumblebee
        apiPrefix: /bumblebee/grafana
      - id: Cluster1-kibana
        type: CS
        owner: Cluster1
        fqdn: occne-kibana.occne-infra.svc.bumblebee
        apiPrefix: /bumblebee/kibana
      - id: Cluster2-kibana
        type: CS
        owner: Cluster2
        fqdn: occne-kibana.occne-infra.svc.jazz
        apiPrefix: /jazz/kibana
      - id: Cluster2-scp-instance2
        type: SCP
        owner: Cluster2
        fqdn: ocscp-scpc-configuration.scp.svc.jazz
        port: 80
```

Sample configuration section for manager managing local NFs. User must configure cncc-iam, mcncc-core and acncc-core flag to "true".

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
```

```
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.bumblebee
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id: Cluster1-grafana
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-grafana.occne-infra.svc.bumblebee
      apiPrefix: /bumblebee/grafana
    - id: Cluster1-kibana
      type: CS
      owner: Cluster1
      fqdn: occne-kibana.occne-infra.svc.bumblebee
      apiPrefix: /bumblebee/kibana
    - id: Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.scp.svc.bumblebee
      port: 80
    - id: Cluster2-scp-instance2
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp.svc.jazz
      port: 80
```

Sample configuration section for agent only deployment. User must configure cncc-iam and mcncc-core to "false" and acncc-core to "true".

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
```

```
aCnccs:
  - id: Cluster2
    role: Cluster2
instances:
  - id: Cluster2-kibana
    type: CS
    owner: Cluster2
    fqdn: occne-kibana.occne-infra.svc.jazz
    apiPrefix: /jazz/kibana
  - id: Cluster2-scp-instance2
    type: SCP
    owner: Cluster2
    fqdn: ocscp-scpc-configuration.scp.svc.jazz
    port: 80
```

Note

- In the above examples, mCnccIams port is assumed as "80". The mCnccIams port configuration must be added only if port value is other than 80 or 443.
- Instance id must be globally unique as it will be used for routing, here is the recommendation for id naming
- `id: <owner>-<instance name>`
  For example:

  `id: Cluster2-scp-instance2`
- `aCnccs.id`:
  - is mandatory as its needed for site authorization.
  - `aCnccs.id` value must be same as `self.cnccId`.
  - `aCnccs.role` and `mCnccCores.role` are optional, which can be used for overriding site role name.
- For HTTPS enabled deployment scheme, port must be updated to "https" and "https port value" in `mCnccIams` and `aCnccs`. For sample configuration, see CNC Console Core Instances configuration examples listed in the appendix.

4. Deploy M-CNCC IAM using repository and helm tar.

Caution

CNC Console helm install command appears hung for a while because Kubernetes job run by Install helm hook. Helm deployment status is shown as **DONE** after the applicable hook is run.

> **⚠ Caution**
>
> Pod restarts may be observed at M-CNCC Core Ingress Gateway during fresh installation, upgrade, or rollback. This is because M-CNCC Core Ingress Gateway internally checks if CNC Console IAM KC pod is up or not using CNC Console IAM Ingress Gateway. Once CNC Console IAM KC pod is up, you should see M-CNCC Core Ingress Gateway in running state.

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

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

For example:

```
kubectl get pods -n cncc -w
```

The pod status gets updated at regular intervals. When helm install command is run, and it exits with the status, you may stop watching the status of Kubernetes pods.

> **ⓘ Note**
>
> If helm purge does not clean the deployment and Kubernetes objects completely, then follow CNC Console IAM Clean up section.

Update DB details in *occncc_custom_values_<version>.yaml* file.

```
dbVendor: mysql
dbName: cnccdb
dbHost: mysql-sds.default.svc.cluster.local
dbPort: 3306
```

> **ⓘ Note**
>
> Database must be created first and that Database name must be mentioned as dbName.

a. Run the following command for installation using helm repository:

```
helm install <release_name> <helm-repo> -f
<occncc_custom_values_<version>.yaml> --namespace
      <namespace_name> --version <helm_version>
```

Where:

helm-repo: repository name where the helm images, charts are stored

values: helm configuration file which needs to be updated based on the docker registry

release_name and **namespace_name**: depends on user configuration

For example:

```
helm install cncc ocscp-helm-repo/cncc -f
occncc_custom_values_24.1.1.yaml --namespace cncc --version 24.1.1
```

b. Run the following command for installation using helm tar:

```
helm install <release_name> -f <occncc_custom_values_<version>.yaml> --
namespace <namespace>
      <chartpath>./<chart>.tgz
```

For example:

```
helm install cncc -f occncc_custom_values_24.1.1.yaml --namespace cncc
occncc-24.1.1.tgz
```

5. Run the following commands to upgrade the CNC Console Configuration:

> **Note**
>
> For details about CNC Console Deployment Configuration workflow, see the CNC Console Deployment Configuration Workflow section.

To upgrade:

- Prepare the *occncc_custom_values_<version>.yaml* file for upgrade.
- Upgrade CNC Console.

a. Run the following command for upgrading using helm repository:

```
$ helm upgrade <release_name> <helm_chart> -f
<occncc_custom_values_<version>.yaml> --namespace <namespace-name>
```

For example:

```
$ helm upgrade cncc ocspf-helm-repo/cncc -f
occncc_custom_values_24.1.1.yaml --namespace cncc
```

b. Run the following command for upgrading using helm tar:

```
helm upgrade <release_name> -f occncc_custom_values_<version>.yaml --
namespace <namespace>
      <chartpath>./<chart>.tgz
```

For example:

```
helm  upgrade cncc -f occncc_custom_values_24.1.1.yaml --namespace cncc
occncc-24.1.1.tgz
```

6. Run the following command to check the deployment status:

```
helm status <release_name>
```

7. Run the following command to check if all the services are deployed and running:
For Non OCI:

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

Sample output:

```
$ kubectl -n cncc get services
```

For example:

```
NAME                          TYPE           CLUSTER-IP      EXTERNAL-
IP      PORT(S)                        AGE
cncc-acore-igw-cache          ClusterIP      None
<none>           8000/TCP                      24h
cncc-acore-ingress-gateway    ClusterIP      10.233.47.246
<none>           80/TCP                        24h
cncc-iam-igw-cache            ClusterIP      None
<none>           8000/TCP                      24h
cncc-iam-ingress-gateway      LoadBalancer   10.233.3.123
10.75.224.188    80:30185/TCP                  24h
cncc-iam-kc-headless          ClusterIP      None
<none>           8285/TCP                      24h
cncc-iam-kc-http              ClusterIP      10.233.42.16
<none>           8285/TCP,8443/TCP,9990/TCP    24h
cncc-mcore-cmservice          ClusterIP      10.233.9.144
<none>           8442/TCP                      24h
cncc-mcore-igw-cache          ClusterIP      None
<none>           8000/TCP                      24h
cncc-mcore-ingress-gateway    LoadBalancer   10.233.44.167
10.75.224.189    80:30175/TCP                  24h
```

For OCI

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

For example:

```
kubectl -n cncc get services
NAME                          TYPE           CLUSTER-IP      EXTERNAL-
IP                    PORT(S)         AGE
cncc-acore-igw-cache          ClusterIP      None
<none>                         8000/TCP        34m
cncc-acore-ingress-gateway    ClusterIP      10.96.171.188
<none>                         443/TCP         34m
cncc-mcore-cmservice          ClusterIP      10.96.100.237
<none>                         8442/TCP        34m
cncc-mcore-igw-cache          ClusterIP      None
<none>                         8000/TCP        34m
```

```
cncc-mcore-ingress-gateway   LoadBalancer   10.96.64.105
10.0.20.117,129.213.159.165   443:31114/TCP   34m
```

8. Run the following command to check if all the pods are up and running:
   Non OCI:

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

   For example:

   ```
   $ kubectl -n cncc get pods
   ```

   ```
   NAME                                          READY   STATUS
   RESTARTS        AGE
   cncc-acore-ingress-gateway-c685bf678-bgmdf    1/1     Running
   0               24h
   cncc-iam-ingress-gateway-6776df55cd-xzx2m     1/1     Running
   0               24h
   cncc-iam-kc-0                                 2/2     Running
   0               24h
   cncc-mcore-cmservice-587749d58d-8lnd7         1/1     Running
   0               24h
   cncc-mcore-ingress-gateway-59758876b-zc7d7    1/1     Running
   0               24h
   ```

   OCI:

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

   For example:

   ```
   $ kubectl -n cncc get pods
   ```

   ```
   NAME                                          READY   STATUS    RESTARTS   AGE
   cncc-acore-ingress-gateway-84c99d6f86-lcxln   2/2     Running   0          23m
   cncc-mcore-cmservice-df5b8b885-nxwpv          2/2     Running   0          23m
   cncc-mcore-ingress-gateway-8666dcbc4f-4b2cf   2/2     Running   0          23m
   ```

> ⚠ **Caution**
>
> Do not exit from the helm install command manually. After running the helm install command, it will take a while to install all the services. Do not press "ctrl+c" to exit from helm install command. It may lead to anomalous behavior.

> **Note**
>
> **Tmeout duration (optional)**: If not specified, the default value will be 5m (5 minutes) in helm.This specifies the time to wait for any individual Kubernetes operation (like Jobs for hooks). The default value is 5m0s. If the helm install command fails at any point to create a Kubernetes object, it will internally call the purge to delete after timeout value (default: 300s). Here, timeout value is for automatic purge on installation failure, and not for overall installation.

2.2.3 Postinstallation Tasks

This section explains the postinstallation tasks for CNC Console.

For Non OCI postinstallation steps, see CNC Console IAM Postinstallation Steps.

For OCI postinstallation steps, see Postinstallation Steps for OCI IAM.

For IPv4 or IPv6 configurations, see Support for IPv4 or IPV6 Configuration for CNC Console.

2.2.3.1 Verifying CNC Console Installation

This section describes how to verify if CNC Console is installed successfully.

> **Note**
>
> - M-CNCC IAM helm install command will appear hung for a while because Kubernetes job will get executed by install helm hook. Helm deployment will be shown as DONE after the applicable hook is executed.
> - Pod restarts maybe observed at M-CNCC Core Ingress Gateway during fresh installation, upgrade, or rollback. This is because M-CNCC Core Ingress Gateway internally checks if CNC Console IAM KC pod is up or not using CNC Console IAM Ingress Gateway. Once CNC Console IAM KC pod is up, you should see M-CNCC Core iIngress Gateway in running state.

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

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

   For example:

   ```
   occncc -n cncc
   ```

   Status should be `deployed`
2. Run the following command to verify if the pods are up and active:

   ```
   kubectl get jobs,pods -n release_namespace
   ```

For example:

```
kubectl get pod -n cncc
```

If the deployment is successful, the status for all pods changes to **Running** and **Ready**.

3. Run the following command to verify if the services are deployed and active:

```
kubectl get services -n release_namespace
```

For example:

```
kubectl get services -n cncc
```

> **Note**
>
> Take a backup of the following files, which are required during fault recovery:
>
> - Current custom-values.yaml file from which you are upgrading.
> - Updated *occncc_custom_values_<version>.yaml* file.
> - Updated Helm charts.
> - Secrets, certificates, and keys that are used during installation.

> **Note**
>
> - If the installation is not successful or you do not see the status as Running for all the pods, perform the troubleshooting steps provided in *Oracle Communications Cloud Native Configuration ConsoleTroubleshooting Guide.*
> - For information on validation-hook errors, see CNC Console Validation-hook Error Codes.

2.2.3.2 Performing Helm Test

Helm Test is a feature which validates the successful installation of CNCC along with readiness (Readiness probe URL configured will be checked for success) of all the pods. The pods to be checked will be based on the namespace and label selector configured for the helm test configurations.

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

To perform Helm test, perform the following steps:

1. Configure the helm test configurations which are under global sections in *occncc_custom_values_<version>.yaml* file. Refer the following configurations :

CNCC Helm Test

```
global:
  # Helm test related configurations
  test:
    nfName: cncc
    image:
      name: occncc/nf_test
      tag: 24.1.1
      imagePullPolicy: IfNotPresent
    config:
      logLevel: WARN
      timeout: 240
```

2. Run the following command to perform the Helm test:

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

Where,

<release_name> is the release name.
<namspace> is the deployment namespace where CNCC is installed.

Example:

```
E.g. [root@master cncc]# helm test cncc -n cncc
Pod cncc-test pending
Pod cncc-test pending
Pod cncc-test pending
Pod cncc-test pending
Pod cncc-test running
Pod cncc-test succeeded
NAME: cncc
LAST DEPLOYED: Tue Jun  7 06:47:14 2022
NAMESPACE: cncc
STATUS: deployed
REVISION: 1
TEST SUITE:     cncc-test
Last Started:   Wed Jun  8 06:01:10 2022
Last Completed: Wed Jun  8 06:01:44 2022
Phase:          Succeeded
NOTES:
# Copyright 2020 (C), Oracle and/or its affiliates. All rights reserved.
Thank you for installing cncc. Your release is named cncc , Release
Revision: 1.
To learn more about the release, try:

  $ helm status cncc
  $ helm get cncc
```

3. Wait for the helm test to complete. Check for the output to see if the test job is successful.

If the Helm test fails, see the *Oracle Communications Cloud Native Configuration Console Troubleshooting Guide.*

2.2.3.2.1 Helm Test Kubernetes Resources Logging

The Helm test logging enhancement for Kubernetes resources lists the following details of Kubernetes resources:

1. Versions of Kubernetes resource available in OCCNE.
2. Preferred version for that Kubernetes resource on the OCCNE.
3. For each micro service, it list the version of Kubernetes resource used.

This information can be used in the following cases:

1. In case of CNE upgrade for customer, helm test shall list the Kubernetes resource versions used by NFs. The operator can use this information to run a pre-upgrade compatibility test to see if the Kubernetes resource versions are available on target CNE.
2. After CNE upgrade, there might be certain resources for which a newer version is available on CNE which is also supported by Console charts. If the output of helm test indicates failure of compliance for certain resource, then upgrade the Console to use the latest version of Kubernetes resource for which failure was indicated.
3. List all available versions on CNE. Console can use this detail as an input for apiVersion to be used in latest NF charts to which upgrade will be performed.

Note that this feature is tested and compatible with CNE version 1.10 and above.

To use this feature, set global.test.compliance flag to true.

Separate helm test service account can be created and set at global.helmTestserviceAccountName, see Helm Test Service Account Configuration section.

> **Note**
>
> For helm test execution preference goes to global.helmTestserviceAccountName first, if this is not available then global.serviceAccountName will be referred. If both of these are missing then default service account will be created and used.

```
# Custom service account for Helm test execution
helmTestserviceAccountName: ""

# Helm test related configurations
test:
  nfName: cncc
  image:
    name: occncc/nf_test
    tag: 24.1.1
    imagePullPolicy: IfNotPresent
  config:
    logLevel: WARN
    timeout: 240 #Beyond this duration helm test will be considered failure
  resources:
  - horizontalpodautoscalers/v1
  - deployments/v1
  - configmaps/v1
  - prometheusrules/v1
  - serviceaccounts/v1
```

```
  - poddisruptionbudgets/v1
  - roles/v1
  - statefulsets/v1
  - persistentvolumeclaims/v1
  - services/v1
  - rolebindings/v1
 complianceEnable: true
```

Run the following command to check the helm test logs:

```
helm test <releaseName> --logs -n <namespace>
```

Example:

```
helm test cncc --logs -n cncc
```

The output lists:

1. The versions of the Kubernetes resources used by Console, which helps in running pre upgrade compatibility test before CNE upgrade.
2. Compliance check for each Kubernetes resource, if compliance check is false we need to upgrade the Console charts as latest version is supported both by charts and available in new CNE.
3. Available Kubernetes resource versions on CNE.

Log Example:

```
{
  "horizontalpodautoscalers" : {
    "availableVersionOnCne" : [ "v1", "v2beta1", "v2beta2" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "deployments" : {
    "availableVersionOnCne" : [ "v1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "configmaps" : {
    "availableVersionOnCne" : [ "v1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "serviceaccounts" : {
    "availableVersionOnCne" : [ "v1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
```

```
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "poddisruptionbudgets" : {
    "availableVersionOnCne" : [ "v1beta1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1beta1",
    "maxNFVersion" : "v1"
  },
  "roles" : {
    "availableVersionOnCne" : [ "v1", "v1beta1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "statefulsets" : {
    "availableVersionOnCne" : [ "v1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "persistentvolumeclaims" : {
    "availableVersionOnCne" : [ "v1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "services" : {
    "availableVersionOnCne" : [ "v1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  },
  "rolebindings" : {
    "availableVersionOnCne" : [ "v1", "v1beta1" ],
    "avaliableOnDeployment" : [ ],
    "compliant" : true,
    "prefferedVersionOnCne" : "v1",
    "maxNFVersion" : "v1"
  }
}
```

2.2.3.2.2 Helm Test Cleanup

After running the helm test, the pod moves to completed state, to remove the pod manually, run the following command:

```
kubectl delete pod release_name -test -n <namespace_name>
```

Example:

```
kubectl delete pod cncc-test -n cncc
```

2.2.3.3 CNC Console IAM Postinstallation Steps

This section explains the postinstallation steps such as Configuring CNC Console redirection URL, creating the User, and assigning the roles.

> **Note**
>
> CNC Console multicluster deployment supports cluster specific roles. The user can create cluster roles in CNC Console IAM and assign cluster specific roles to the user similar to NF roles.
>
> Operators must ensure that the cluster role name matches with the role name given in helm configuration.
>
> - For M-CNCC cluster role creation in M-CNCC IAM, the value of global.mCnccCores.id or global.mCnccCores.role name must be used.
> - For A-CNCC cluster role creation in M-CNCC IAM, the value of global.aCnccs.id or global.aCnccs.role name must be used.
>
> > **Note**
> >
> > Cluster role names are case sensitive.

Prerequisites

The CNC Console IAM and CNC Console Core must be deployed.

Admin must perform following tasks once CNC Console IAM is deployed:

- Set the CNC Console redirection URL.
- Create the user and assign roles (applicable if not integrated with LDAP).

Steps for configuring CNC Console redirection URL, creating user, and assigning the roles:

1. Log in to CNC Console IAM Console using admin credentials provided during installation of CNC Console IAM.
   Format:

   ```
   <scheme>://<cncc-iam-ingress IP/FQDN>:<cncc-iam-ingress Port>
   ```

   Node-IP and NodePort
   Example:

   ```
   http://10.75.xx.xx:30085/*
   ```

   DNS Resolvable FQDN and NodePort

Example:

```
http://cncc-iam-ingress-gateway.cncc.svc.cluster.local:30085/*
```

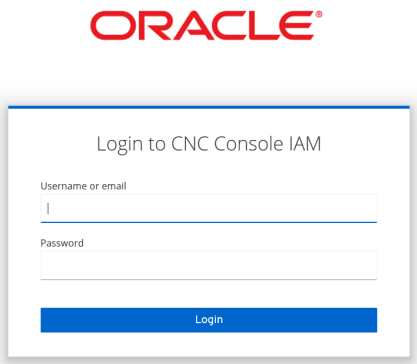
External LB-IP and ServicePort
Example:

```
http://10.75.xx.xx:8080/*
```

DNS Resolvable FQDN and ServicePort
Example:

```
http://cncc-iam-ingress-gateway.cncc.svc.cluster.local:8080/*
```

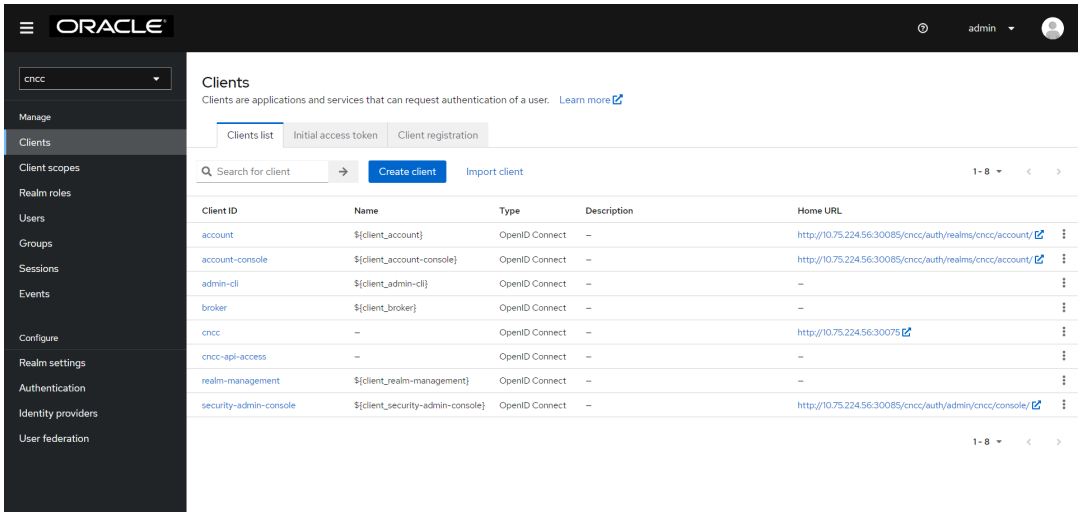
Figure 2-10 Login



> **Note**
>
> You must select CNCC from the Realm drop down on the left pane after logging in to CNC Console IAM.

1. Go to **Clients** option and click **cncc**.

Figure 2-11 Clients Tab

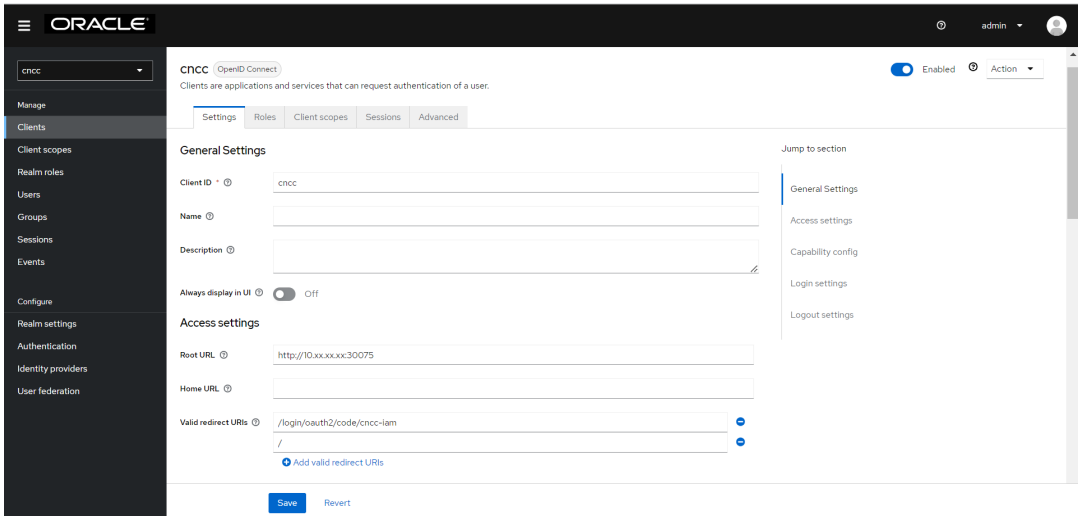


2. Enter CNC Console Core Ingress URI in the **Root URIs** field and **Save.**

```
<scheme>://<cncc-mcore-ingress IP/FQDN>:<cncc-mcore-ingress Port>
```

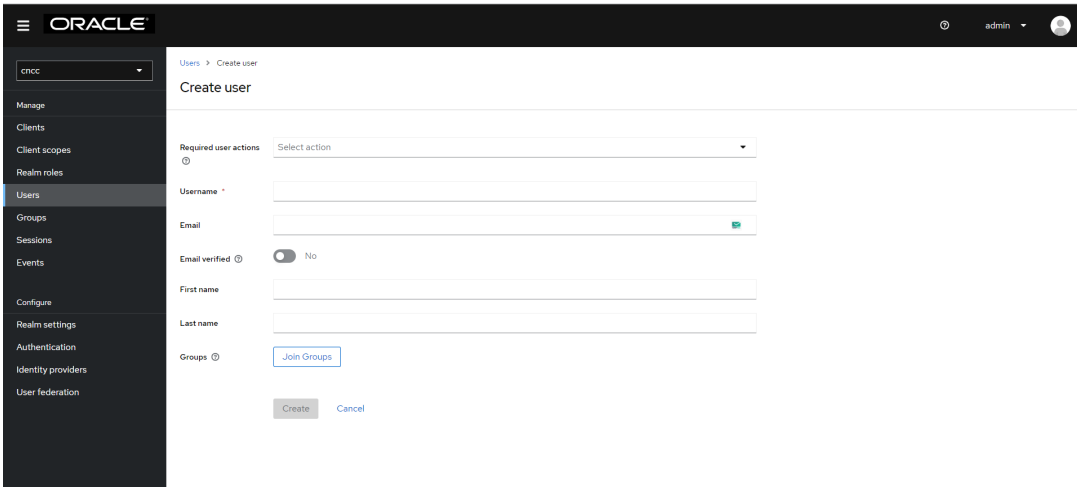
> **Note**
>
> **Redirection URL** is prepopulated, only root URL needs to be configured as part of postinstallation procedure.

Figure 2-12 General Settings



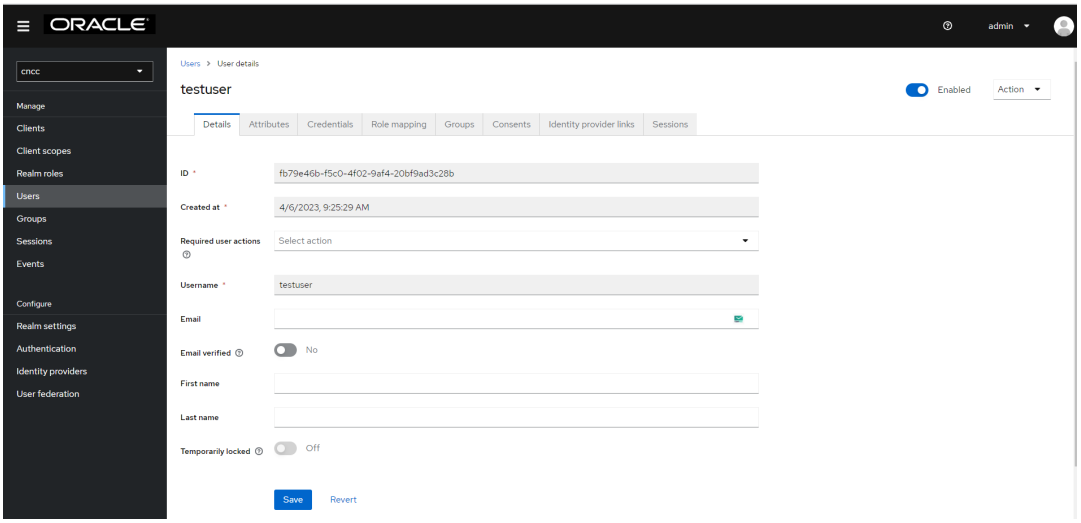
3. Click **Manage**, click **Users,** and click **Add user** on the right pane.

Figure 2-13 Add User



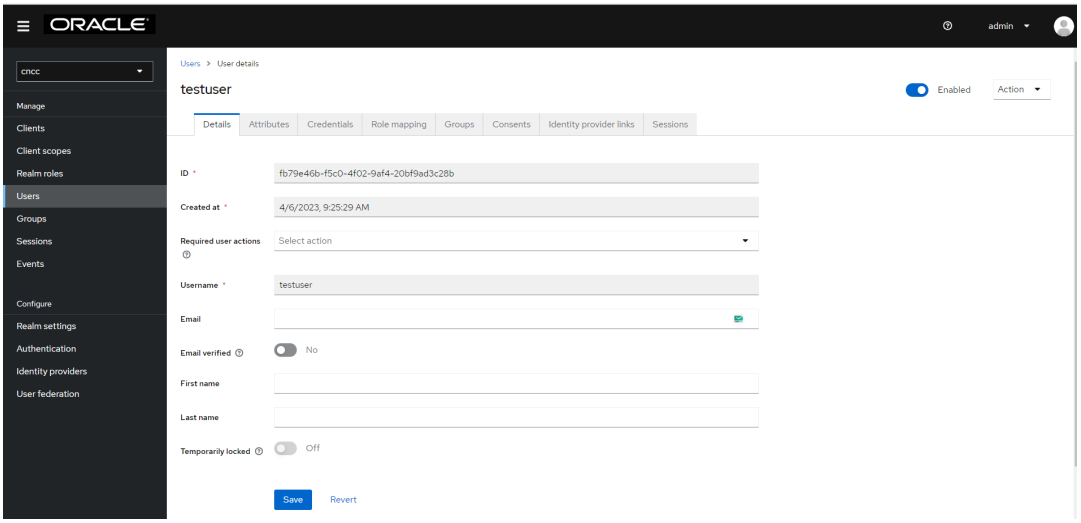
4. **Add user** screen appears. Add the user details and click **Save**.

Figure 2-14 Save User



5. The user has been created and the user details screen appears.

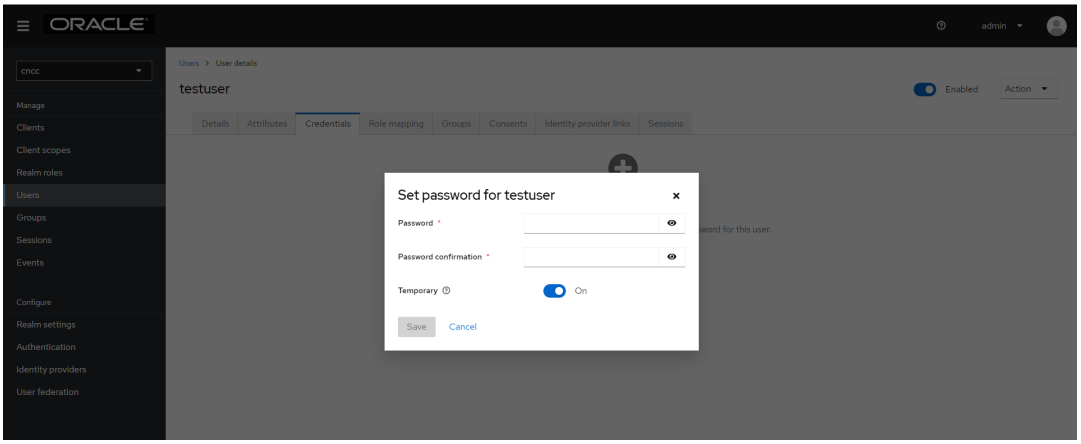
Figure 2-15 User Details



6. For setting the password for the user, click the **Credentials** tab and set the password for that user.

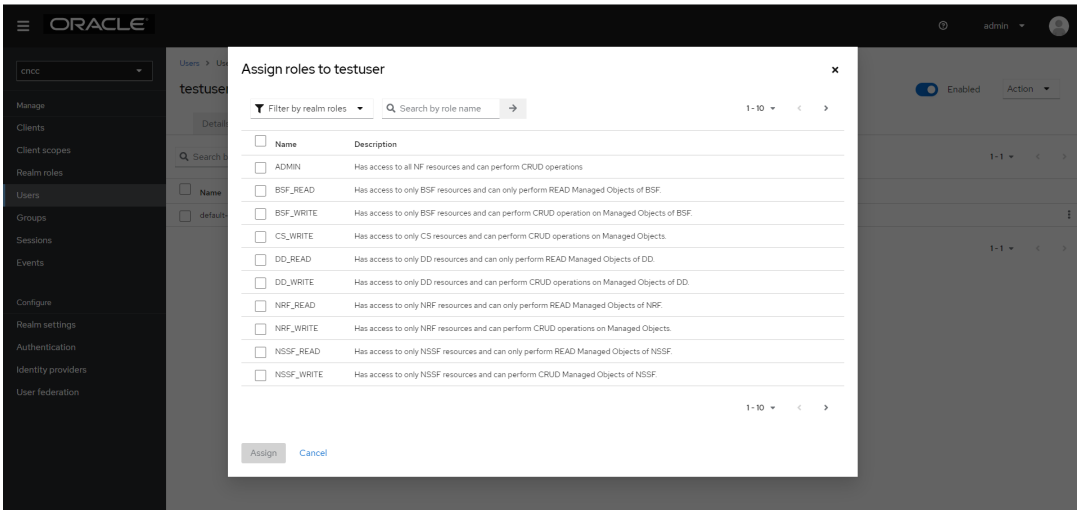
> **Note**
>
> Setting **Temporary flag** to **ON** prompts the user to change the password when logging in to the CNC Console Core GUI for the first time.

Figure 2-16 Set Password



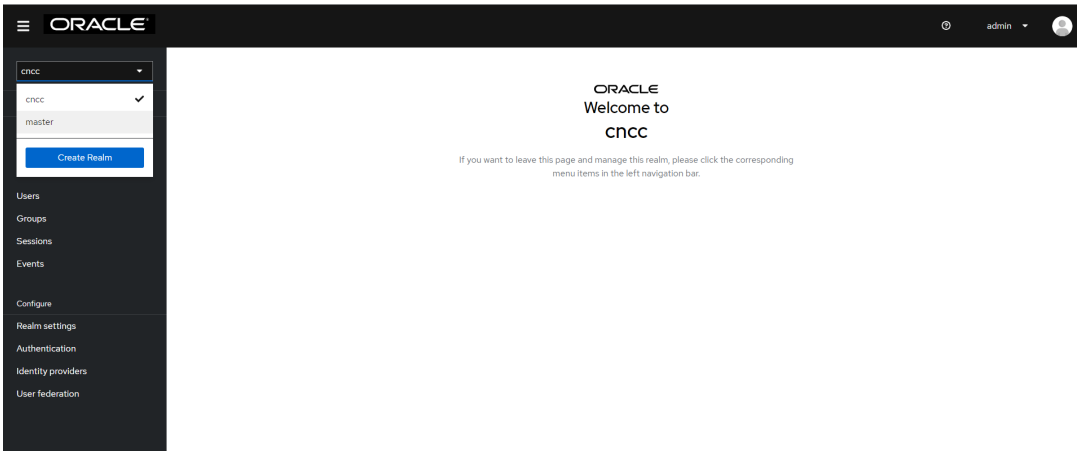
7. Navigate to the **Role Mappings** tab and assign roles to the user.

Figure 2-17 Role Mappings



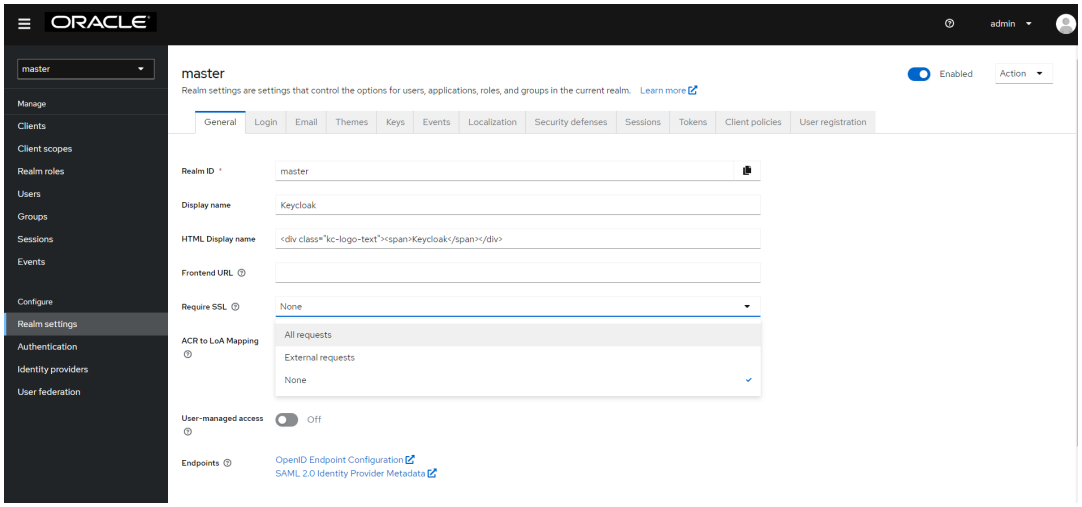
8. Select **Master Realm** from the Realm drop down list.

Figure 2-18 Master Realm



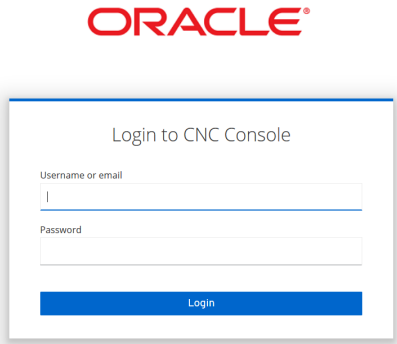
9. From the **Realm Settingw** tab, navigate to the **General** tab. Set Require SSL to **All Requests** and click **Save**.

Figure 2-19 Realm Settings



10. Log in to CNC Console Core using the credentials of the user created earlier.

Figure 2-20 CNC Console Core login



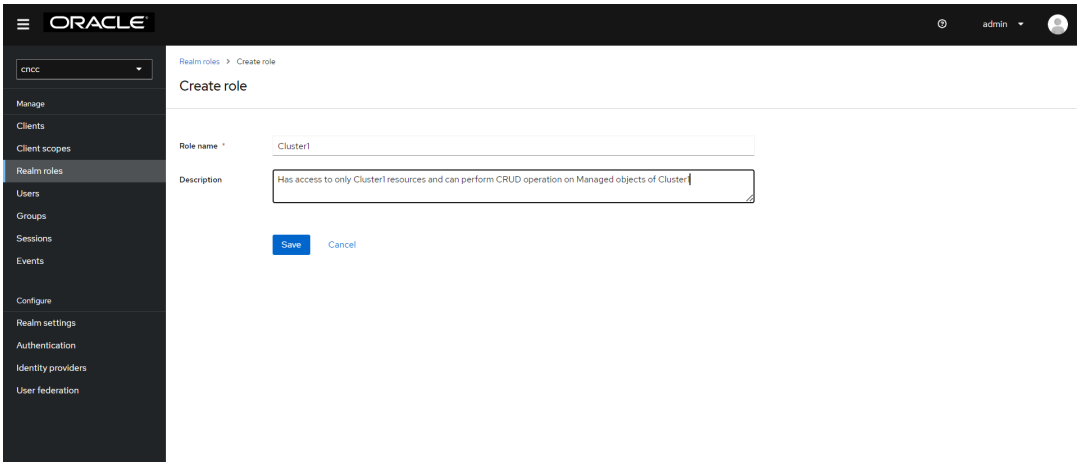
2.2.3.3.1 CNC Console Multicluster Deployment Roles

CNC Console multicluster feature needs additional cluster specific roles to be created in M-CNCC IAM.

This section explains the steps to create the roles.

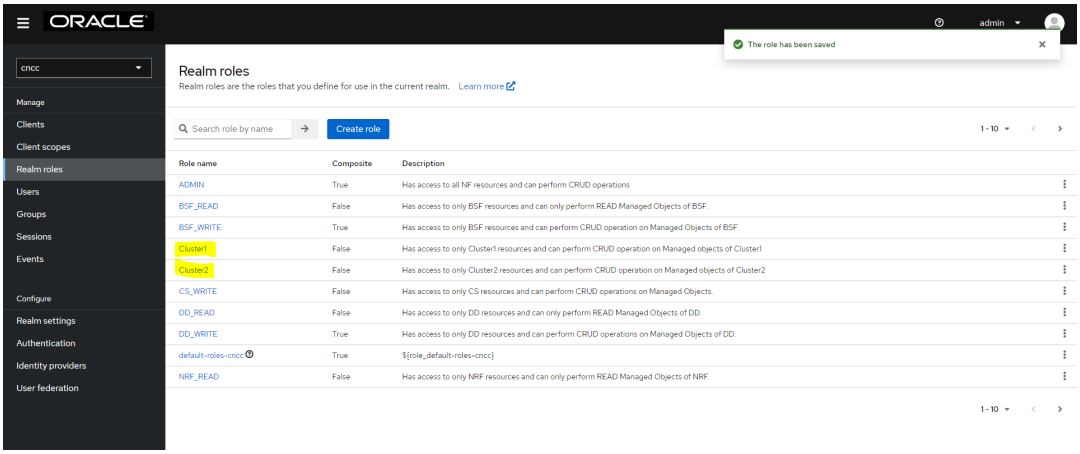
1. Log in to M-CNCC IAM and click **Realm Roles** present on the left pane. The roles defined in the realm is displayed on the right pane.

Figure 2-21 Realm Roles



2. Click **Create Role**.The **Create Role** screen appears. Add the **Role Name** and click **Save**.

Figure 2-22 Create Role



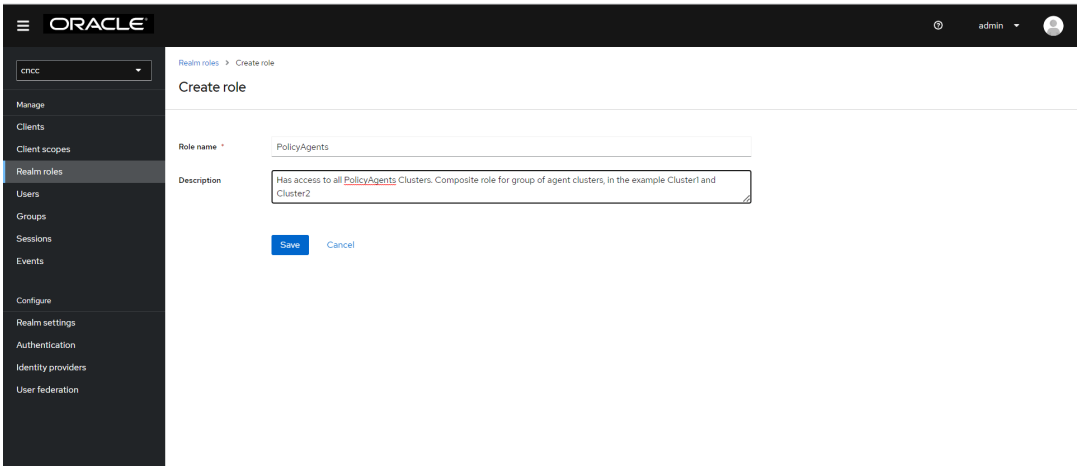
> **Note**
>
> The user must ensure that the cluster role name matches the role name given in helm configuration.
>
> - For M-CNCC cluster role creation in M-CNCC IAM, the value of `global.mCnccCores.id` or `global.mCnccCores.role name` must be used.
> - For A-CNCC cluster role creation in M-CNCC IAM, value of `global.aCnccs.id` or `global.aCnccs.role name` must be used.
> - Cluster roles are case sensitive.

Composite Role Creation

CNC Console IAM provides an option to create composite (group) the roles. This section explains the steps to create the composite roles.

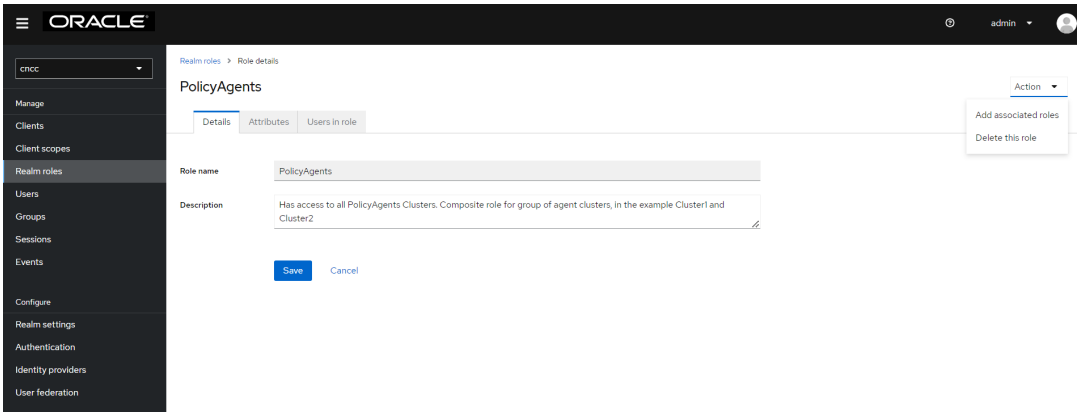
1. Click **Create Role**. The **Create Role** screen appears. Add the **Role Name** and click **Save**.

Figure 2-23 Add Role Name



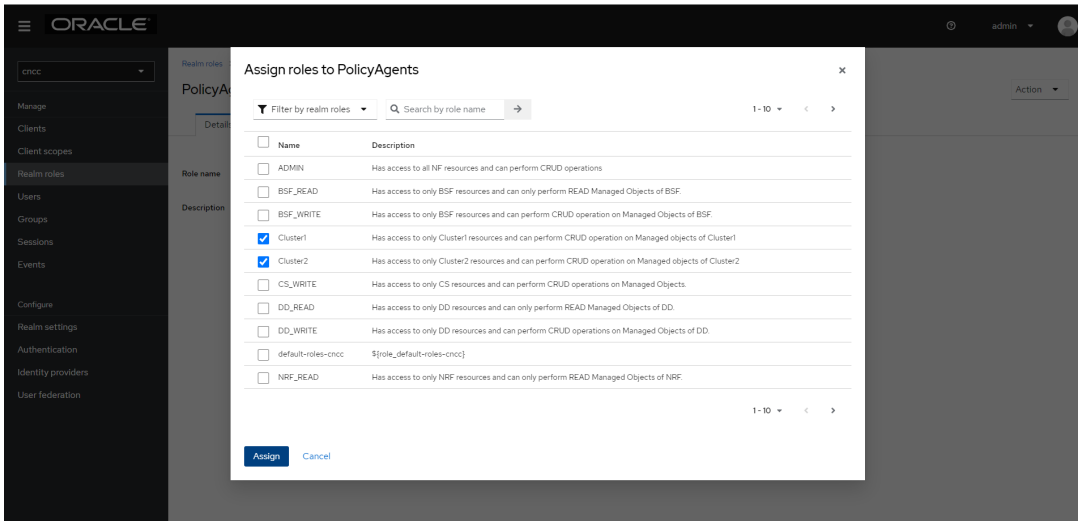
2. From the **Action** drop-down, select **Add associated roles.**

Figure 2-24 Assign Role



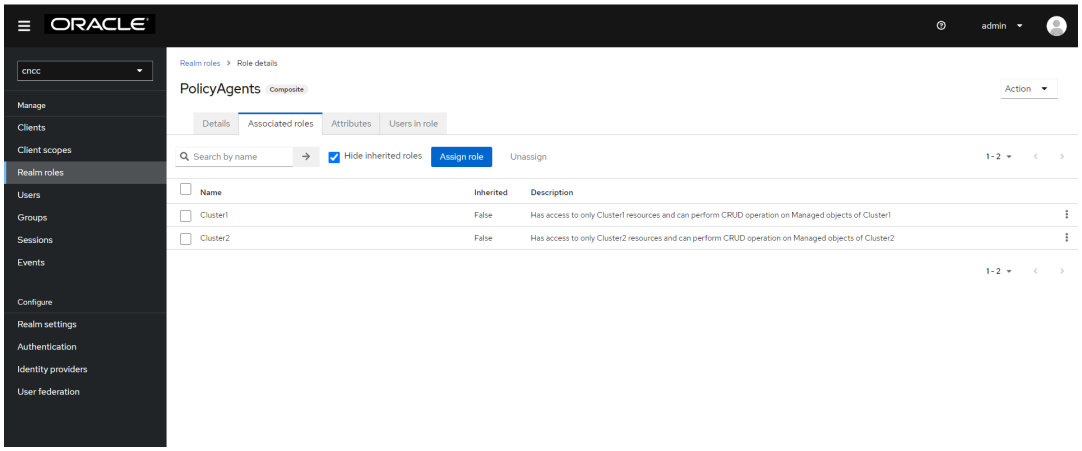
3. This enables the **Composite Roles** functionality, and the **Assign roles** screen appears.
4. Select the required roles from **Realm Roles**, and click **Assign**.

Figure 2-25 Assign Roles



5. The **Associated roles** tab appears in the **Role details** screen.

Figure 2-26 Associates Roles



> **Note**
>
> Here, the name "PolicyAgents" is used for composite role, that can be read as "PolicyAgentCnccs".

> **Note**
>
> For more information about the Roles, see the **Role Based Access Control in CNC Console** section in *Oracle Communications Cloud Native Configuration Console User Guide*.

2.2.3.3.2 CNC Console Password Reset

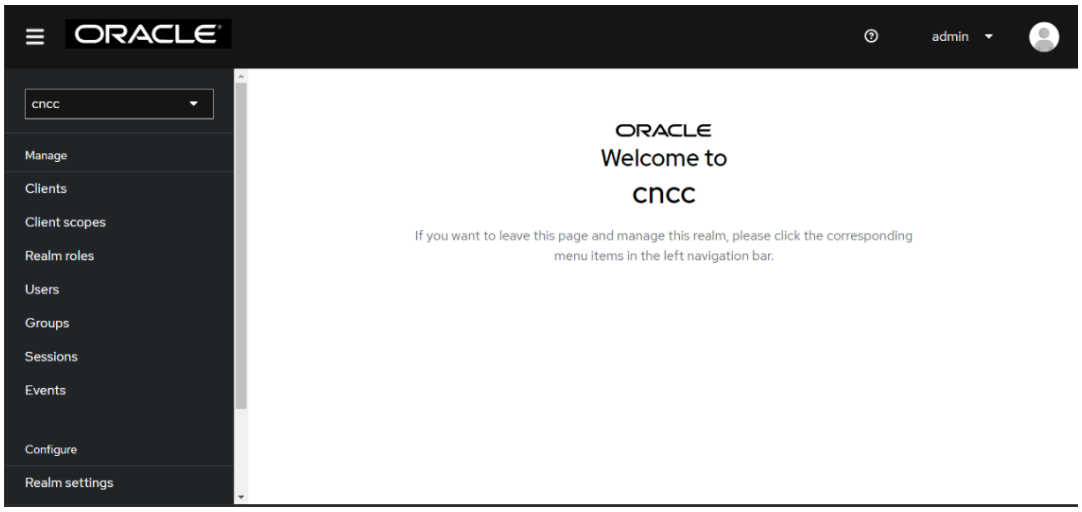
CNC Console admin Password Reset (optional)

> **Warning**
>
> You are recommended to continue using the default admin password because a forgotten admin password can't be recovered. For more information, see *Oracle Communications Cloud Native Configuration Console Troubleshooting Guide.*

CNC Console provides support to change the password of CNC Console IAM:

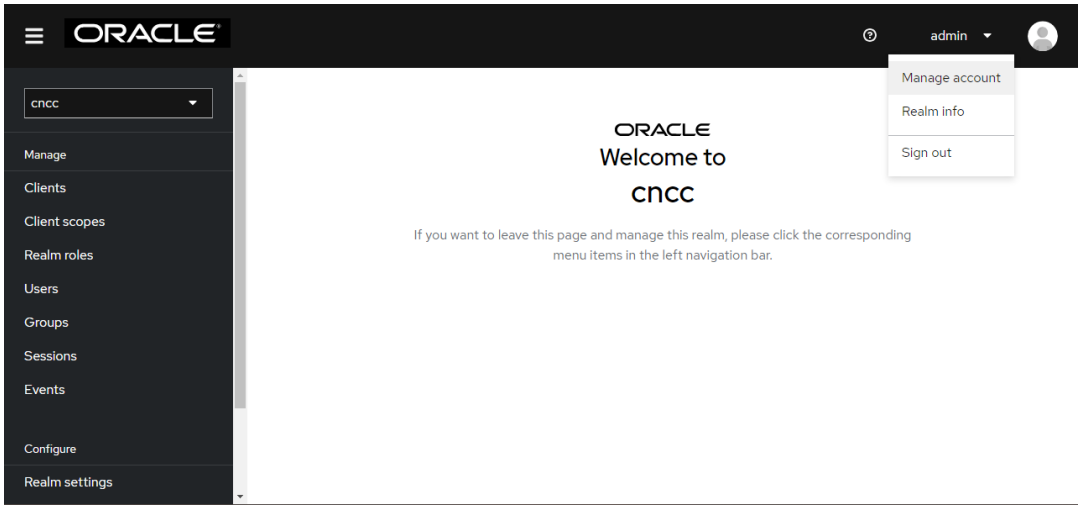
1. Log in to CNC Console IAM and click **Admin** present on the top right of the screen.

Figure 2-27 Log in to CNC Console IAM



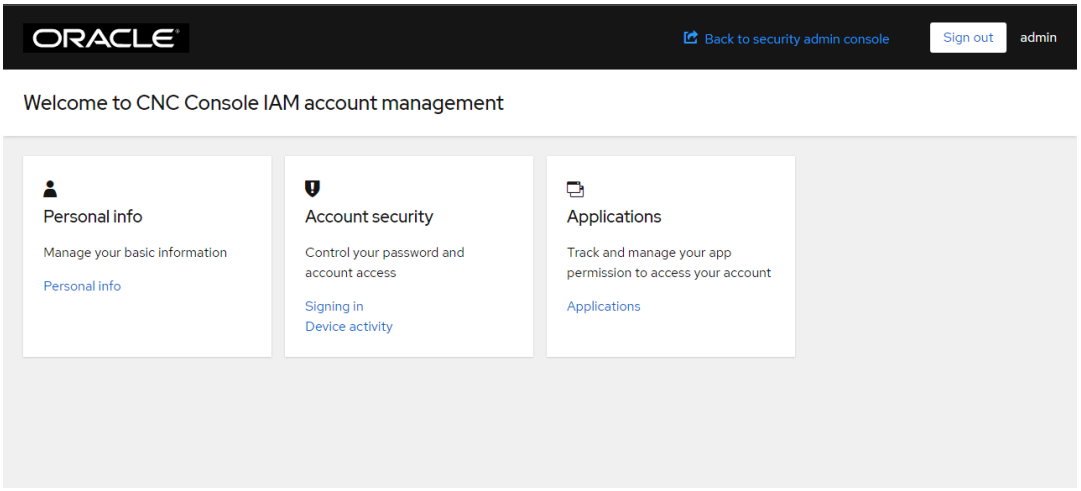
2. Click **Manage Account**.

Figure 2-28 Manage account



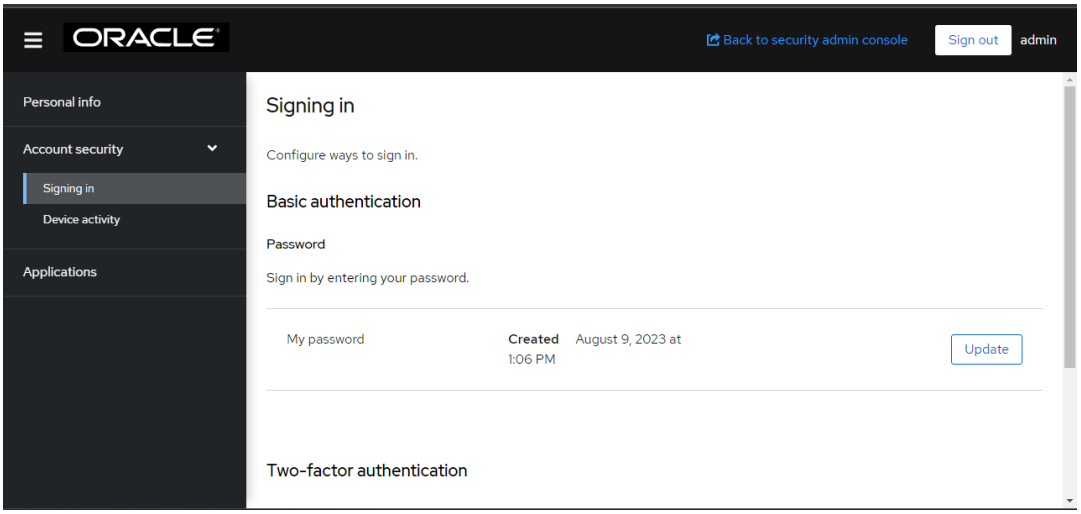
3. Click **Signing** in Account security.

Figure 2-29 Account Security



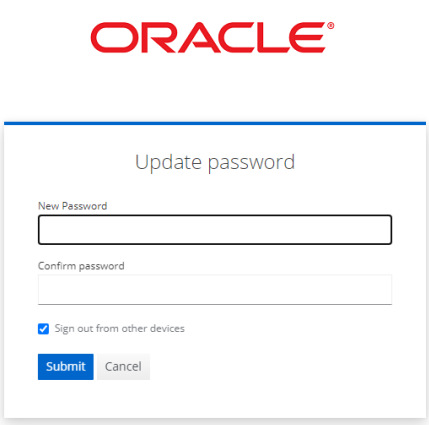
4. Click **Update.**

Figure 2-30 Update



5. Update your password.

Figure 2-31 Update Password



6. Click **Submit.**

CNC Console User Password Reset

> **Note**
>
> Only CNC Console admin can update the user password.

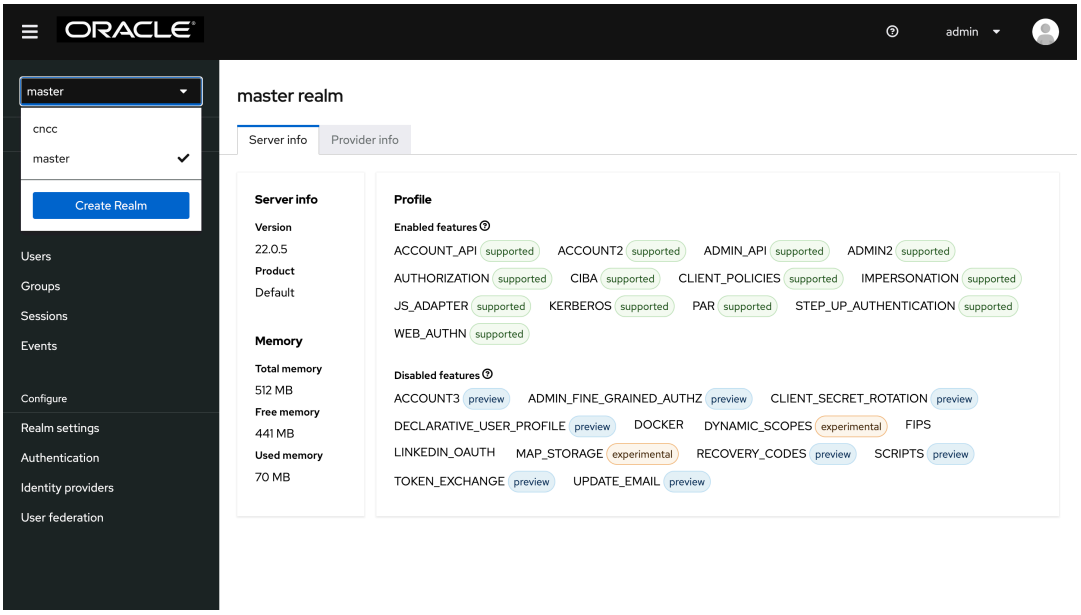
To reset CNC Console user password:

1. Log in to CNC Console IAM.

Figure 2-32 CNC Console IAM

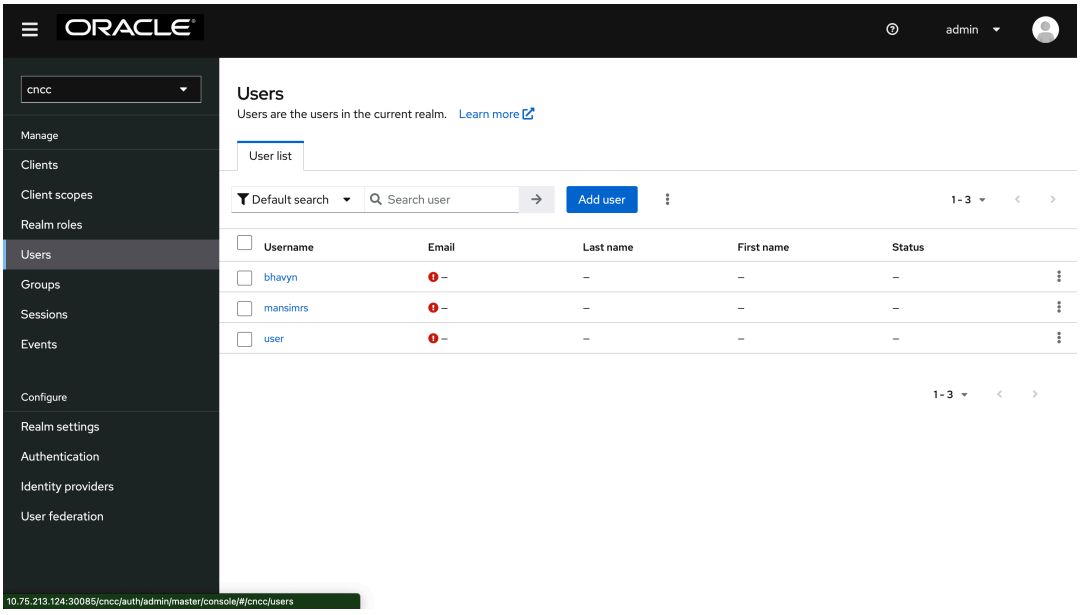
2. Select cncc realm.

Figure 2-33 cncc Realm



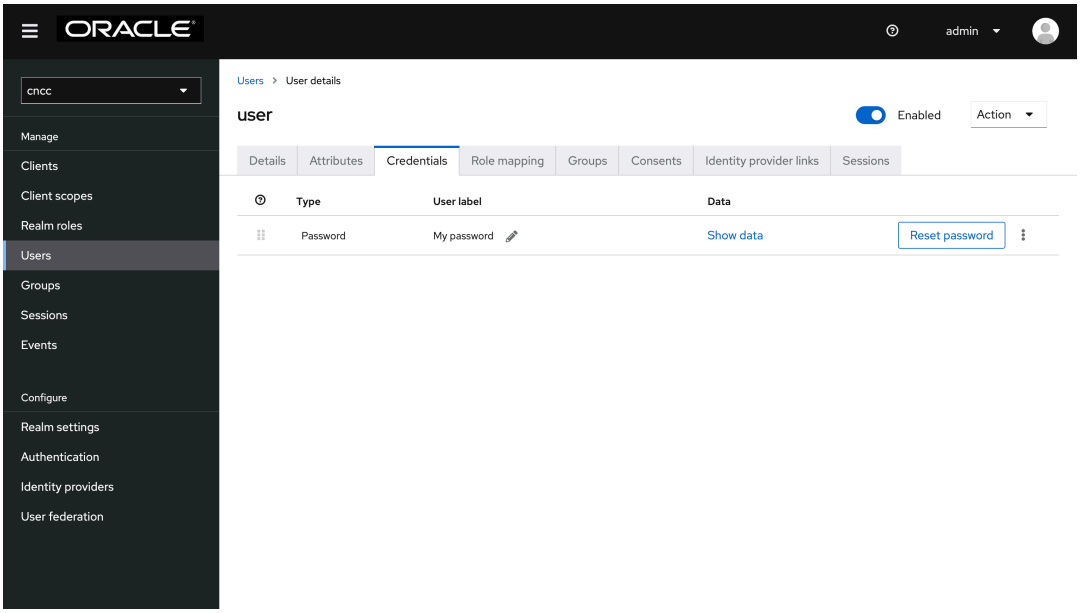
3. Select **Users** from menu on left.

Figure 2-34 Users



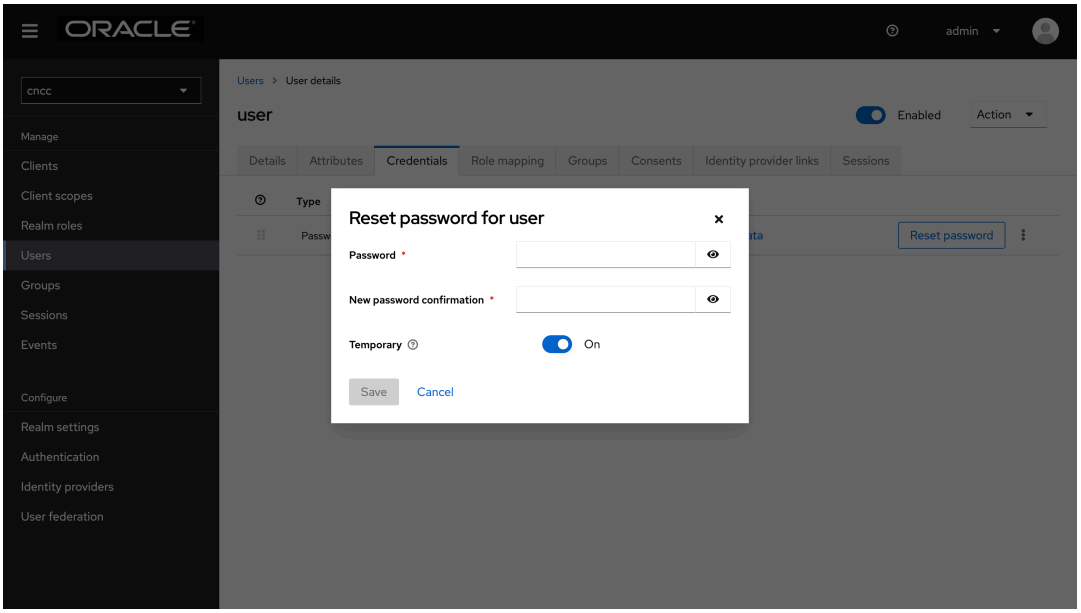
4. Click your desired user, and select **credentials**.

Figure 2-35 Credentials



5. Click **reset password**, enter your password, and then click **Save**.

Figure 2-36 Reset Password



2.2.3.4 Postinstallation Steps for OCI IAM

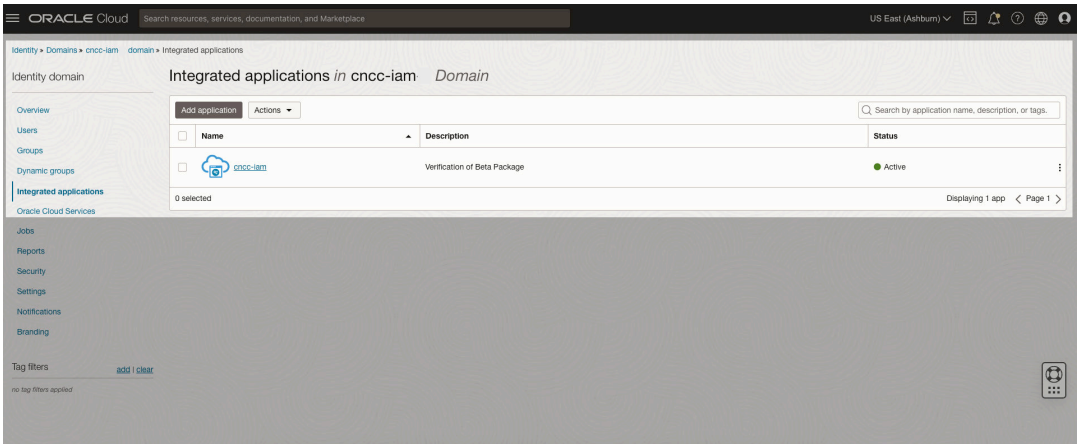
2.2.3.4.1 Configure CNC Console Redirect URLs in OCI IAM

Once the CNC Console application is deployed in the OKE cluster you must configure the **Redirect URL** and **Post-logout redirect URL** in OCI IAM.

1. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.

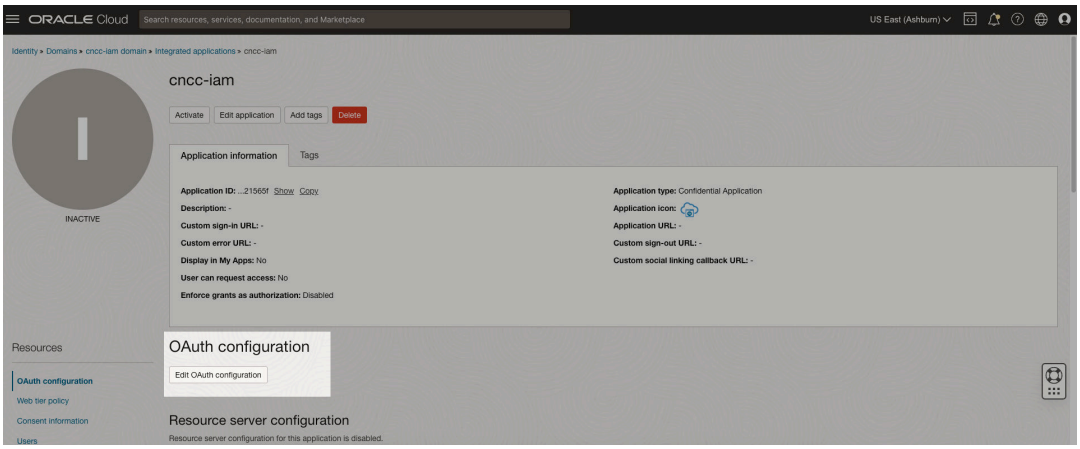
2. Click the name of the identity domain that you want to work in. You might need to change the compartment to find the domain that you want. Then, click **Integrated applications**.

Figure 2-37 Integrated Applications



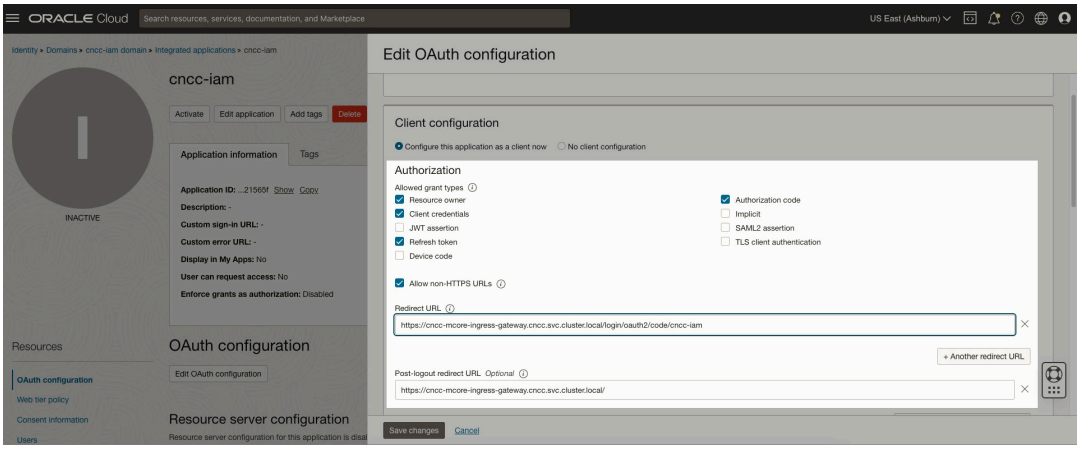
3. Click the application that you want to modify (for example: **cncc-iam**).
4. Click **Edit OAuth Configuration**.

Figure 2-38 Edit OAuth



5. Expand the **Client configuration** node.
6. Update the following fields:

Figure 2-39 Authorization



a. **Authorization Types:** select thev**Resource owner, Client Credentials**, **Refresh token**, and **Authorization code** checkboxes.

b. **Redirect URL:** Application URL where the user is redirected after authentication. This field is mandatory.

- Configure the following for CNC Console:

  ```
  /login/oauth2/code/cncc-iam
  ```

- Template for redirect URL:
  For LoadBalancer IP and Port:

  ```
  https://<cncc-mcore-igw-lb-ip>:<port>/login/oauth2/code/cncc-iam
  ```

  For DNS resolvable FQDN and port:

  ```
  https://<cncc-mcore-igw-dns-resolvable-fqdn>:<port>/login/oauth2/
  code/cncc-iam
  ```

- Example if port 80 or 443:
  For LoadBalancer IP and port:

  ```
  https://xxx.xxx.xx.xxx/login/oauth2/code/cncc-iam
  ```

  For DNS resolvable FQDN and port:

  ```
  https://cncc-mcore-ingress-gateway.cncc.svc.cluster.local/login/
  oauth2/code/cncc-iam
  ```

- Example if port is other than 80/443:
  For LoadBalancer IP and port:

  ```
  https://xxx.xxx.xx.xxx:8443/login/oauth2/code/cncc-iam
  ```

For DNS resolvable FQDN and port:

```
https://cncc-mcore-ingress-gateway.cncc.svc.cluster.local:8443/
login/oauth2/code/cncc-iam
```

c. Post logout redirect URL: Enter the URL where you want to redirect the user after logging out of the application.

- Template for Post-logout redirect URL:

  For LoadBalancer IP and port:

  ```
  https://<cncc-mcore-igw-lb-ip>:<port>/
  ```

  For DNS resolvable FQDN and port:

  ```
  https://<cncc-mcore-igw-dns-resolvable-fqdn>:<port>/
  ```

- Example if port is 80 or 443

  For LoadBalancer IP and port

  ```
  https://xxx.1xx.xx.xxx/
  ```

  For DNS resolvable FQDN and port:

  ```
  https://cncc-mcore-ingress-gateway.cncc.svc.cluster.local/
  ```

- Example if port is other than 80 or 443:

  For LoadBalancer IP and port:

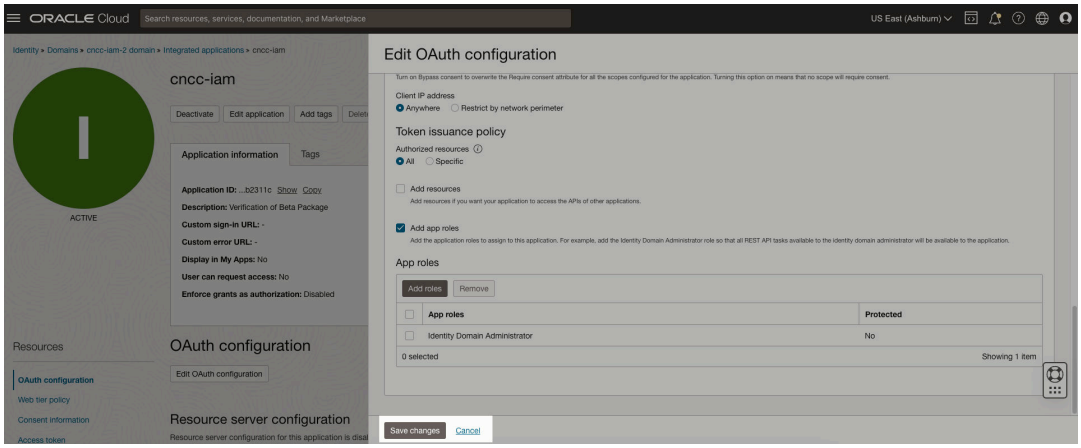
  ```
  https://xxx.1xx.xx.xxx:8443/
  ```

  For DNS resolvable FQDN and port:

  ```
  https://cncc-mcore-ingress-gateway.cncc.svc.cluster.local:8443/
  ```

7. Click **Save Changes**.

Figure 2-40 Save



8. If the application is not activated, , click **Activate** at the top of the page, to the right of the application name.
9. In the **Activate application** dialog box, click **Activate application**.

2.2.3.4.2 Configure Password Policies in OCI IAM

You can choose the default password policies that OCI IAM provides, or create custom password policies based on your own requirement.

See OCI Password Policies in the *Oracle Communications Cloud Native Configuration Console User Guide* for customizing password policies.

2.2.3.4.3 Configure Groups in OCI IAM

> **Note**
>
> In OCI deployment, CNC Console roles are called groups.

Create CNC Console Groups

You can create groups by:

- (Recommended) Importing groups using CSV file. For more details, see the Importing Groups section in *Oracle Communications Cloud Native Configuration Console User Guide*.
- Manually creating CNC Console groups. For more details, see the Create a Group section in *Oracle Communications Cloud Native Configuration Console User Guide*.

Verify Created or Imported Groups

To view all groups, see the Create a Group section in the *Oracle Communications Cloud Native Configuration Console User Guide*.

2.2.3.4.4 Configure Users in OCI IAM

Create Users

You can create users using following options:

- Importing users via CSV file. For more details, see the Importing Users section in the *Oracle Communications Cloud Native Configuration Console User Guide*.
- Manually creating users. For more details, see the Create a User section in the *Oracle Communications Cloud Native Configuration Console User Guide*.

Assign Users to Groups
To assign users to groups, see the Add a User to a Group section in *Oracle Communications Cloud Native Configuration Console User Guide*.

Verify Created or Imported Users
To view all users, see the View Users section in the *Oracle Communications Cloud Native Configuration Console User Guide.*

2.2.3.4.5 Verify CNC Console GUI Access

To verify the CNC Console GUI access, see the Logging into CNC Console GUI section in the *Oracle Communications, Cloud Native Configuration Console User Guide*.

3
Customizing CNC Console

This chapter provides information about customizing CNC Console.

The CNC Console deployment is customized by overriding the default values of various configurable parameters in the `occncc_custom_values_<version>.yaml` file.

To customize the custom yaml files, perform the following steps:

1. Unzip the CNC Console package file: Unzip the CNC Console package file to the specific repository:
   `unzip occncc_csar_<marketing-release-number>.zip`

   The package consists of following files and folders:

   a. **Files**: CNC Console Docker images file and CNC Console Helm Charts

   b. **Scripts**: Custom values and alert files:

      - CNC Console custom values file: `occncc_custom_values_<version>.yaml`
      - CNC Console cnDBTier custom values file: `occncc_dbtier_<cndbtier_version>_custom_values_<version>.yaml`
      - CNC Console network policy custom values file: `occncc_network_policy_custom_values_<version>.yaml`
      - CNC Console IAM Schema file for rollback to previous version: `occncc_rollback_iam_schema_<version>.sql`
      - CNC Console Metric Dashboard file: `occncc_metric_dashboard_<version>.json`
      - CNC Console Metric Dashboard file for CNE supporting Prometheus HA (CNE 1.9.x onwards): `occncc_metric_dashboard_promha_<version>.json`
      - CNC Console Metric Dashboard file for OCI deployment: `occncc_oci_metric_dashboard_<version>.zip`
      - CNC Console Alert Rules file: `occncc_alertrules_<version>.yaml`
      - CNC Console Alert Rules file for CNE supporting Prometheus HA (CNE 1.9.x onwards): `occncc_metric_dashboard_promha_<version>.json`
      - CNC Console Alert Rules file for OCI deployment: `occncc_oci_alertrules_<version>.zip`
      - CNC Console MIB files: `occncc_mib_<version>.mib`, `occncc_mib_tc_<version>.mib`
      - CNC Console Groups CSV files having roles definition for OCI deployment: `occncc_oci_groups_<version>.csv`
      - CNC Top level mib file: `toplevel.mib`

   c. **Definitions**: Definitions folder contains the CNE Compatibility and definition files.

      - `occncc_cne_compatibility.yaml`
      - `occncc.yaml`

   d. TOSCA-Metadata: `TOSCA.meta`

e. The package folder structure is as follows:

```
Definitions
       occncc_cne_compatibility.yaml
       occncc.yaml
Files
    apigw-common-config-hook-24.1.10.tar
    apigw-configurationinit-24.1.10.tar
    ChangeLog.txt
    cncc-apigateway-24.1.10.tar
    cncc-cmservice-24.1.1.tar
    cncc-core-validationhook-24.1.1.tar
    cncc-iam-24.1.1.tar
    cncc-iam-healthcheck-24.1.1.tar
    cncc-iam-hook-24.1.1.tar
    Helm
        occncc-24.1.1.tgz
        occncc-network-policy-24.1.1.tgz
    Licenses
    nf_test-24.1.2.tar
    ocdebug-tools-24.1.3.tar
    Oracle.cert
    Tests
occncc.mf
Scripts
    occncc_alerting_rules_promha_24.1.1.yaml
    occncc_alertrules_24.1.1.yaml
    occncc_custom_values_24.1.1.yaml
    occncc_dbtier_24.1.1_custom_values_24.1.1.yaml
    occncc_metric_dashboard_24.1.1.json
    occncc_metric_dashboard_promha_24.1.1.json
    occncc_mib_24.1.1.mib
    occncc_mib_tc_24.1.1.mib
    occncc_network_policy_custom_values_24.1.1.yaml
    occncc_rollback_iam_schema_24.1.1.sql
    occncc_oci_metric_dashboard_24.1.1.zip
    occncc_oci_alertrules_24.1.1.zip
    occncc_oci_groups_24.1.1.csv
    toplevel.mib
TOSCA-Metadata
    TOSCA.meta

Example: unzip occncc_csar_24_1_1_0_0.zip
Archive: occncc_csar_24_1_1_0_0.zip
creating: Definitions/
inflating: Definitions/occncc_cne_compatibility.yaml
inflating: Definitions/occncc.yaml
creating: Files/
creating: Files/Tests/
creating: Files/Helm/
inflating: Files/Helm/occncc-24.1.1.tgz
extracting: Files/Helm/occncc-network-policy-24.1.1.tgz
creating: Files/Licenses/
inflating: Files/apigw-configurationinit-24.1.10.tar
inflating: Files/apigw-common-config-hook-24.1.10.tar
inflating: Files/ocdebug-tools-24.1.3.tar
```

```
inflating: Files/cncc-apigateway-24.1.10.tar
inflating: Files/cncc-iam-24.1.1.tar
inflating: Files/cncc-iam-hook-24.1.1.tar
inflating: Files/cncc-iam-healthcheck-24.1.1.tar
inflating: Files/nf_test-24.1.2.tar
inflating: Files/cncc-core-validationhook-24.1.1.tar
inflating: Files/cncc-cmservice-24.1.1.tar
inflating: Files/ChangeLog.txt
extracting: Files/Oracle.cert
creating: Scripts/
inflating: Scripts/occncc_custom_values_24.1.1.yaml
inflating: Scripts/occncc_network_policy_custom_values_24.1.1.yaml
inflating: Scripts/occncc_mib_tc_24.1.1.mib
inflating: Scripts/occncc_mib_24.1.1.mib
inflating: Scripts/toplevel.mib
inflating: Scripts/occncc_metric_dashboard_24.1.1.json
inflating: Scripts/occncc_metric_dashboard_promha_24.1.1.json
inflating: Scripts/occncc_alertrules_24.1.1.yaml
inflating: Scripts/occncc_alerting_rules_promha_24.1.1.yaml
inflating: Scripts/occncc_rollback_iam_schema_24.1.1.sql
inflating: Scripts/occncc_dbtier_24.1.1_custom_values_24.1.1.yaml
inflating: Scripts/occncc_oci_metric_dashboard_24.1.1.zip
inflating: Scripts/occncc_oci_alertrules_24.1.1.zip
inflating: Scripts/occncc_oci_groups_24.1.1.csv
creating: TOSCA-Metadata/
inflating: TOSCA-Metadata/TOSCA.meta
inflating: occncc.mf
```

```
occncc_oci_metric_dashboard_<version>.zip file contains the metric
dashboard files for OCI deployment.
occncc_oci_metric_dashboard_<version>.json  covers overall metrics
including all the supported NF flows.
occncc_oci_<NF>_metric_dashboard_<version>.json covers NF flow specific
metrics.

Example:
unzip occncc_oci_metric_dashboard_24.1.1.zip
Archive:  occncc_oci_metric_dashboard_24.1.1.zip
   creating: occncc_oci_metric_dashboard/
  inflating: occncc_oci_metric_dashboard/
occncc_oci_bsf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_dd_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nef_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nrf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nssf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_nwdaf_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_occm_metric_dashboard_24.1.1.json
```

```
  inflating: occncc_oci_metric_dashboard/
occncc_oci_policy_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_provgw_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_scp_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_sepp_metric_dashboard_24.1.1.json
  inflating: occncc_oci_metric_dashboard/
occncc_oci_udr_metric_dashboard_24.1.1.json

occncc_oci_alertrules_<version>.zip file contains the alarm terraform
directory for OCI deployment.
occncc_oci directory contains CNC Console feature specific alarms.
occncc_oci_resources directory contains CNC Console pod/container
memory alarms.

Example:
unzip occncc_oci_alertrules_24.1.1.zip
Archive:  occncc_oci_alertrules_24.1.1.zip
   creating: occncc_oci_alertrules/
   creating: occncc_oci_alertrules/occncc_oci_resources/
  inflating: occncc_oci_alertrules/occncc_oci_resources/
notifications.tf
  inflating: occncc_oci_alertrules/occncc_oci_resources/alarms.tf
  inflating: occncc_oci_alertrules/occncc_oci_resources/variables.tf
  inflating: occncc_oci_alertrules/occncc_oci_resources/schema.yaml
   creating: occncc_oci_alertrules/occncc_oci/
  inflating: occncc_oci_alertrules/occncc_oci/notifications.tf
  inflating: occncc_oci_alertrules/occncc_oci/alarms.tf
  inflating: occncc_oci_alertrules/occncc_oci/variables.tf
  inflating: occncc_oci_alertrules/occncc_oci/schema.yaml
```

2. Customize the appropriate files.
3. Save the updated files.

3.1 Global Configuration Options

This section includes information about the configuration parameters of the Global Configuration section of CNC Console Core:

Table 3-1 Global Configuration Options

Parameter	Description	Details
`global.dockerRegistry`	This is a mandatory parameter. Here user provides the registry that contains CNC Console images. It comprises of the following: <registry-url> Ex: cgbu-occncc-dev-docker.dockerhub-phx.oci.oraclecorp.com	**DataType:** String **Range:** It may contain lowercase letters, digits, and separators. A separator is defined as a period, one or two underscores, or one or more dashes. **Default Value:** ocspf-registry.us.oracle.com:5000

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.clusterDomain`	This is a mandatory parameter. Cluster Domain where cncc-core will be deployed. example: cluster.local Note: To check cluster domain use the following command: `kubectl -n kube-system get configmap kubeadm-config -o yaml | grep -i dnsDomain`	**DataType:** String **Range:** It may contain lowercase letters, digits, and separators. A separator is defined as a period, one or two underscores, or one or more dashes.
`global.serviceAccountName`	This is an optional parameter. Name of service account. If this field is kept empty, then a default service account 'cncc-core-service-account' is created. If any value is provided, then a service account has to be created manually. `kubectl create serviceaccount <name> -n <namespace>`	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters.
`global.customExtension.allResources.labels`	This is an optional parameter. This can be used to add custom label(s) to all Kubernetes resources that will be created by Ingress Gateway helm chart.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources
`global.customExtension.allResources.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all Kubernetes resources that will be created by Ingress Gateway helm chart.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.customExtension.nonlbStatefulsets.labels`	This is an optional parameter. This can be used to add custom label(s) to all Statefulsets that will be created by Ingress Gateway helm chart which are associated to a service which is of Load Balancer Type.	**DataType:** String **Range:** Custom Annotations that need to be added to Ingress Gateway deployments that are associated to a Service which is of Load Balancer type.

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.customExtension.nonlbStatefulsets.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all Statefulsets that will be created by Ingress Gateway helm chart which are associated to a service which is of Load Balancer Type.	**DataType:** String **Range:** Custom Annotations that need to be added to Ingress Gateway deployments that are associated to a Service which is of Load Balancer type.
`global.customExtension.lbServices.labels`	This is an optional parameter. This can be used to add custom label(s) to all Load Balancer Type Services that will be created by Ingress Gateway helm chart.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.customExtension.lbServices.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all Load Balancer Type Services that will be created by Ingress Gateway helm chart.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.customExtension.lbDeployments.labels`	This is an optional parameter. This can be used to add custom label(s) to all deployments that will be created by Ingress Gateway helm chart which are associated to a service which is of Load Balancer Type.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.customExtension.lbDeployments.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all deployments that will be created by Ingress Gateway helm chart which are associated to a service which is of Load Balancer Type.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.customExtension.nonlbServices.labels`	This is an optional parameter. This can be used to add custom label(s) to all non-Load Balancer Type services that will be created by Ingress Gateway helm chart.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.customExtension.nonlbServices.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all non-Load Balancer Type services that will be created by Ingress Gateway helm chart.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.customExtension.nonlbDeployments.labels`	This can be used to add custom label(s) to all deployments that will be created by Ingress Gateway helm chart which are associated to a service which is not of Load Balancer Type.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.customExtension.nonlbDeployments.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all Deployments that will be created by Ingress Gateway helm chart which are associated to a service which is not of Load Balancer Type.	**DataType:** String **Range:** Custom Labels that need to be added to all the Ingress Gateway Kubernetes resources.
`global.helmTestServiceAccountName`	This is an optional parameter. For helm test execution, preference goes to global.helmTestserviceAccountName first. If this is not available, then global.serviceAccountName will be referred. If both of these are missing then default service account will be created and used.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters.
`global.test.nfName`	This is a mandatory parameter. Name of deployment for which helm test is done.	**DataType:** String **Range:** NF Name
`global.test.image.name`	This is a mandatory parameter. Image name for the helm test container image.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:**
`global.test.image.tag`	This is a mandatory parameter. Image version tag for helm test.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters.
`global.test.image.imagePullPolicy`	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:** String **Range:** IfNotPresent, Always, Never **Default Value:** IfNotPresent
`global.test.config.logLevel`	This is a mandatory parameter. Log level for helm test pod.	**DataType:** String **Range:** WARN, DEBUG, INFO

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.test.config.timeout`	This is a mandatory parameter. Timeout value for the helm test operation. If exceeded helm test will be considered as failure. Unit:seconds	**DataType:** String **Range:** 1-300
`global.test.resources`	This is a mandatory parameter. Which ever kubernetes resource are mentioned, will be logged in helm test.	**DataType:** <List[String]> **Range:** It takes resources and its version in the form of <resource_name>/<max_version_supportedbyNF> - horizontalpodautoscalers/v1 - deployments/v1 - configmaps/v1 - prometheusrules/v1 - serviceaccounts/v1 - poddisruptionbudgets/v1 - roles/v1 - statefulsets/v1 - persistentvolumeclaims/v1 - services/v1 - rolebindings/v1
`global.test.complianceEnable`	This is a mandatory parameter. It will enable or disable helm test resource logging.	**DataType:** Boolean **Range:** True or False **Default Value:** True
`global.validationHook.image.name`	This is a mandatory parameter. Image name for validation hook.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters.
`global.validationHook.image.tag`	This is a mandatory parameter. Image version tag for validation hook.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods and dashes. An image name may not start with a period, or a dash and may contain a maximum of 128 characters.
`global.validationHook.image.imagePullPolicy`	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:** String **Range:** IfNotPresent, Always, Never **Default Value:** IfNotPresent
`global.validationHook.config.logLevel.root`	This is a mandatory parameter. Log level for validation hook pod.	**DataType:** String **Range:** WARN, DEBUG, INFO, etc.

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.ephemeralStorage.requests.containersLogStorage`	This is a mandatory parameter. Set value for Ephemeral Storage Requests.	**DataType:** Integer **Range:** It can take values in integer and that values are used in MBs.
`global.ephemeralStorage.requests.containersCriticalStorage`	This is a mandatory parameter. Set value for Ephemeral Storage Requests.	**DataType:** Integer **Range:** It can take values in integer and that values are used in MBs. **Default Value:**
`global.ephemeralStorage.limits.containersLogStorage`	This is a mandatory parameter. Set value for Ephemeral Storage Limits.	**DataType:** Integer **Range:** It can take values in integer and that values are used in MBs.
`global.ephemeralStorage.limits.containersCriticalStorage`	Set value for Ephemeral Storage Limits.	**DataType:** Integer **Range:** It can take values in integer and that values are used in MBs.
`global.hookJobResources.limits.cpu`	This is a mandatory parameter. It limits the number of CPUs to be used by the helm test pod.	**DataType:** String **Range:** Valid floating point value between 0 and 1.
`global.hookJobResources.limits.memory`	This is a mandatory parameter. It limits the number of memory to be used by the helm test pod.	**DataType:** Integer **Range:** Valid Integer value followed by Mi/Gi etc.
`global.hookJobResources.limits.logStorage`	This is a mandatory parameter. It limits the logStorage (ephemeral storage) to be used by the helm test pod.	**DataType:** Integer **Range:** Values will be set by global.ephemeralStorage.limits.containers LogStorage. **Default Value:**
`global.hookJobResources.limits.criticalStorage`	This is a mandatory parameter. It limits the criticalStorage (ephemeral storage) to be used by the helm test pod.	**DataType:** Integer **Range:** Values will be set by global.ephemeralStorage.limits.containers CrititcalStorage.
`global.hookJobResources.requests.cpu`	This is a mandatory parameter. The minimum amount of CPUs required.	**DataType:** String **Range:**Valid floating point value between 0 and 1.
`global.hookJobResources.requests.memory`	This is a mandatory parameter. The minimum amount of CPUs required.	**DataType:** Integer **Range:** Valid Integer value followed by Mi/Gi etc.
`global.hookJobResources.requests.logStorage`	This is a mandatory parameter. The minimum amount of logStorage (ephemeral storage).	**DataType:** Integer **Range:** Values will be set by global.ephemeralStorage.requests.containerLogStorage. **Default Value:**

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.hookJobResources.requests.criticalStorage`	This is a mandatory parameter. The minimum amount of criticalStorage (ephemeral storage).	**DataType:** Integer **Range:** Values will be set by global.ephemeralStorage.requests.containerCrititcalStorage. **Default Value:**
`global.k8sResource.container.prefix`	This is an optional parameter. This value will be used to prefix to all the container names of Ingress Gateway.	**DataType:** Integer **Range:** Value that will be prefixed to all the container names of Ingress Gateway. **Default Value:**
`global.k8sResource.container.suffix`	This is an optional parameter. This value will be used to suffix to all the container names of Ingress Gateway.	**DataType:** Integer **Range:** Value that will be prefixed to all the container names of Ingress Gateway. **Default Value:**
`global.k8sResources.pdb.supportedVersions`	This is an optional parameter. List of supported Kubernetes apiVersion for PodDisruptionBudget out of which the priority is given to the latest.	**DataType:** List String **Range:**It takes resources and its version in the form of <resource_name>/<max_version_supportedbyNF> **Default Value:** policy/v1
`global.extraContainers`	This is a mandatory parameter. To enable or disable the debug tools container.	**DataType:** enum **Range:** DISABLED, ENABLED **Default Value:**
`global.debugToolContainerMemoryLimit`	This is a mandatory parameter This field describes the memory size (request and limit) and emptyDir volume size for the Debug-tool container.	**DataType:** String **Range:** Valid Integer value followed by Mi/Gi **Default Value:** 4Gi
`global.extraContainersVolumesTpl.name`	This is a mandatory parameter Name of the emptyDir volume.	**DataType:** String **Range:** May contain lowercase letters, digits, and separators. A separator is defined as a period, one or two underscores, or one or more dashes. **Default Value:** debug-tools-dir
`global.extraContainersVolumesTpl.emptyDir.medium`	This is a mandatory parameter Describes where emptyDir volumes are stored.	**DataType:** String **Range:** **Default Value:** Memory
`global.extraContainersVolumesTpl.emptyDir.sizeLimit`	This is a mandatory parameter The size of the emptyDir volume.	**DataType:** String **Range:** Valid Integer value followed by Mi/Gi. **Default Value:** 4Gi

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details

`global.extraContainersTpl.command`	This is a mandatory parameter.
	String array used for container command.
		DataType: List[String]
		Range:
		Example:
		`drop:`
		`-/bin/sleep`
		`-infinity`

`global.extraContainersTpl.image`	This is a mandatory parameter. Docker image name	**DataType:** String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters.
`global.extraContainersTpl.imagePullPolicy`	This is a mandatory parameter. Image Pull Policy	**DataType:** String **Range:** IfNotPresent, Always, Never **Default Value:** IfNotPresent
`global.extraContainersTpl.name`	This is a mandatory parameter. Name of the container	**DataType:** String **Range:** It may contain lowercase letters, digits, and separators. A separator is defined as a period, one or two underscores, or one or more dashes.
`global.extraContainersTpl.resources.limits.ephemeral-storage`	This is a mandatory parameter. The maximum amount of Ephemeral Storage allowed.	**DataType:** Integer **Range:** Valid Integer value followed by Mi/Gi etc. **Default Value:**512Mi
`global.extraContainersTpl.resources.limits.cpu`	The maximum amount of cpu allowed.	**DataType:** String **Range:** Valid floating point value between 0 and 1. **Default Value:**0.5
`global.extraContainersTpl.resources.limits.memory`	This is a mandatory parameter. The maximum amount of memory allowed.	**DataType:** String **Range:** Valid Integer value followed by Mi/Gi etc. Values will be set by global.debugToolContainerMemoryLimit. **Default Value:**4Gi
`global.extraContainersTpl.resources.requests.ephemeral-storage`	This is a mandatory parameter. The minimum amount of Ephemeral Storage required.	**DataType:** Integer **Range:** Valid Integer value followed by Mi/Gi etc. **Default Value:** 512Mi
`global.extraContainersTpl.resources.requests.cpu`	This is a mandatory parameter. The minimum amount of cpu limits required.	**DataType:** String **Range:** Valid floating point value between 0 and 1. **Default Value:**

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.extraContainersTpl.resources.requests.memory`	This is a mandatory parameter. The minimum amount of memory required.	**DataType:** Integer **Range:** Valid Integer value followed by Mi/Gi etc. Values will be set by global.debugToolContainerMemoryLimit. **Default Value:**4Gi
`global.extraContainersTpl.securityContext.allowPrivilegeEscalation`	This is a mandatory parameter. AllowPrivilegeEscalation controls whether a process can gain more privileges than its parent process. This bool directly controls if the no_new_privs flag will be set on the container process.	**DataType:** Boolean **Range:**True or False **Default Value:** True

`global.extraContainersTpl.securityContext.capabilities.drop`	This is a mandatory parameter.
	Removed capabilities.
		DataType: List[String]
		Range:
		Example:
		`drop:`
		`-ALL`
		Default Value:

`global.extraContainersTpl.securityContext.capabilities.add`	This is a mandatory parameter.
	Added capabilities.
		DataType: List[String]
		Range:
		Example:
		`add:`
		`- NET_RAW`
		`- NET_ADMIN`
		Default Value:

`global.extraContainersTpl.securityContext.runAsUser`	This is an optional parameter. The UID to run the entrypoint of the container process.	**DataType:** Integer **Range:**Integer Value
`global.extraContainersTpl.volumeMounts.mountPath`	This is a mandatory parameter. Path where the emptyDir volume has to be mounted inside the debug-tool container.	**DataType:** String **Range:**Valid path **Default Value:** /tmp/tools
`global.extraContainersTpl.volumeMounts.name`	This is a mandatory parameter.	**DataType:** String **Range:**It may contain lowercase letters, digits, and separators. A separator is defined as a period, one or two underscores, or one or more dashes. **Default Value:** debug-tools-dir

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.serviceMeshCheck`	This is an optional parameter. This flag needs to set it "true" if Service Mesh would be present where CNC Console will be deployed.	**DataType:** Boolean **Range:**True or False **Default Value:** False
`global.serviceMeshHttpsEnabled`	This is an optional parameter. If Service Mesh is deployed with TLS/MTLS disabled then set this flag to false.	**DataType:** Boolean **Range:** True or False **Default Value:** True
`global.istioSidecarQuitUrl`	This is an optional parameter. This needs to be set with correct url format http://127.0.0.1:<Istio sidecar proxy admin port>/quitquitquit" if Service Mesh would be present where CNC Console will be deloyed.	**DataType:** String **Range:** Valid url
`global.istioSidecarReadyUrl`	This is an optional parameter. This needs to be set with correct url format http://127.0.0.1:<Istio sidecar proxy admin port>/ready" if Service Mesh would be present where CNC Console will be deloyed.	**DataType:** String **Range:** Valid url **Default Value:**
`global.dbHost`	This is a mandatory parameter. It the hostname for persistence db. Example: mysql.default.svc.cluster.local	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:**
`global.dbPort`	This is a mandatory parameter. It is the db port for CNC Console Core. Example: 3306	**DataType:**Integer **Range:**0-65535. **Default Value:**
`global.secretName`	It specifies an existing secret to be used for mysql username and password. Example: secretName: &mySqlSecretNameRef cncc-db-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:**

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.useClusterIpForLbServices`	This is an optional parameter. Set this flag to true to assign ClusterIP service type for LoadBalancer (LB) services. This flag is required for deployment, that manages their LB services as ClusterIP alternatively. LoadBalancer in such cases is generally rely on service annotation to discover LB services.	**DataType:**Boolean **Range:** True or False **Default Value:** False
`global.cmServiceHttpPort`	This is a mandatory parameter. It specifies the port number which makes cmservice visible to other services running within the same Kubernetes cluster and the also used by common config client for db creation.	**DataType:** Integer **Range:** 0-65535. **Default Value:**
`global.iamUserName`	This is a mandatory parameter. It is the name of cncc-iam user as given by a user. Example: admin	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. **Default Value:** Admin
`global.isMultiClusterDeployment`	This is an optional parameter. This flag indicates single cluster deployment or multicluster deployment. By default single cluster deployment is configured, flag must be set to true for multicluster deployment.	**DataType:** Boolean **Range:** True or False **Default Value:** False
`global.oci-iam.enabled`	This is a mandatory parameter. This flag indicates that OCI IAM is used for Identity and Access Management instead of CNC Console IAM. **Note:** This flag needs to be set to true if CNC Console is being deployed in OCI environment. **Note:** For a given deployment either **global.oci-iam.enabled** or **global.cncc-iam.enabled** can be true, both cannot be false/true.	**DataType:** Boolean **Range:** True or False **Default Value:** False

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.oci-iam.existingSecret`	This is a mandatory parameter. It specifies an existing secret name to be used for the OCI IAM clientId and clientSecret configuration. Example: oci-iam-secret	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** oci-iam-secret
`global.oci-iam.existingSecretClientIdKey`	This is a mandatory parameter. Applicable only if global.oci-iam.existingSecret is provided. It is the key in the existing secret that stores the clientId. Example: clientId	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** clientId
`global.oci-iam.existingSecretClientSecretKey`	This is a mandatory parameter. Applicable only if global.oci-iam.existingSecret is provided. It is the key in the existing secret that stores the clientSecret. Example: clientSecret	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** clientSecret
`global.cncc-iam.enabled`	This is a mandatory parameter. This flag indicates manager IAM installation. By default it is set to true for single cluster deployment.	**DataType:** Boolean **Range:** True or False **Default Value:**
`global.mcncc-core.enabled`	This is a mandatory parameter. This flag indicates manger core installation. By default it is set to true for single cluster deployment. **Note**: Set this flag to false while installing agent core in case of multicluster deployment.	**DataType:** Boolean **Range:** True or False **Default Value:** True
`global.acncc-core.enabled`	This is a mandatory parameter. This flag indicates agent core installation. By default it is set to true for single cluster deployment. **Note**: Set this flag to false while installing manager core in case of multicluster deployment.	**DataType:** Boolean **Range:** True or False **Default Value:** True

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.self.cnccId`	This is a mandatory parameter. It is the ID of deployment in multicluster Multi Instance Cluster.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:**

`global.mCnccIams[]`	This is a mandatory parameter.
	It is the list of Manager CNC Console IAMs. For further Information, see CNC Console Multi Cluster and Multi Instance Configurations.
		DataType: List[String]
		Range:
		Example:
		`drop:`
		`-all`
		Default Value:

`global.mCnccCores[]`	This is a mandatory parameter. It is the list of Manager CNC Console Cores. For more information see, CNC Console Multi Cluster and Multi Instance Configurations. Note: This parameter is not applicable for A-CNCC Core deployment.	**DataType:** <List> **Range:** **Default Value:**
`global.aCnccs[]`	This is a mandatory parameter. For more information see, CNC Console Multi Cluster and Multi Instance Configurations.	**DataType:** <List> **Range:** Example: **Default Value:**
`global.instances[]`	This is a mandatory parameter. It is the list of NF Instances and Common Services added on various Agents and Managers. For more information see, CNC Console Multi cluster and Multi Instance Configurations.	**DataType:** Integer **Range:** 0-65535. **Default Value:** 60
`global.publicHttpSignalingPort`	This is an optional parameter. It is the port on which Ingress Gateway service is exposed. If httpsEnabled is false, this Port would be HTTP/2.0 Port (unsecured). publicHttpSignalingPort: 80	**DataType:** Integer **Range:** 0-65535. **Default Value:**

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.publicHttpsSignallingPort`	This is an optional parameter. It is the port on which Ingress Gateway service is exposed If httpsEnabled is true, this Port would be HTTPS/2.0 Port (secured SSL)	**DataType:** Integer **Range:** 0-65535 **Default Value:**
`global.metalLbIpAllocationEnabled`	This is an optional parameter. This field enables or disables IP Address allocation from Metallb Pool.	**DataType:** Boolean **Range:** True or False **Default Value:** True
`global.metalLbIpAllocationAnnotation`	It is the address Pool Annotation for Metallb.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** metallb.universe.tf/address-pool: signaling"
`global.staticIpAddressEnabled`	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress else random IP will be assigned by the metalLB from its IP Pool.	**DataType:** Boolean **Range:** True or False **Default Value:** False
`global.staticIpAddress`	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress else random IP will be assigned by the metalLB from its IP Pool	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters.
`global.nodeSelector.nodeKey`	This is an optional parameter. Global node selector key	**DataType:** String
`global.nodeSelector.nodeValue`	This is an optional parameter. Global node value key	**DataType:** String
`global.logStorage`	This is a mandatory parameter. Set value for Ephemeral Storage Limits for logStorage.	**DataType:** Integer **Range:** It can take values in integer and those values are used in MBs. **Default Value:**
`global.criticalStorage`	This is a mandatory parameter. Set value for Ephemeral Storage Limits for criticalStorage.	**DataType:** Integer **Range:** It can take values in integer and those values are used in MBs. **Default Value:**

Table 3-1 (Cont.) Global Configuration Options

Parameter	Description	Details
`global.ephemeralStorageLimit`	This is a mandatory parameter. Limits value for Ephemeral Storage.	**DataType:** Integer **Range:** It can take values in integer and those values are used in MBs. **Default Value:**

3.2 CNC Console IAM Configuration Parameters

This section includes information about the configuration parameters of the CNC Console IAM.

> **Note**
>
> Not applicable for OCI deployment.

3.2.1 Global Parameters

This section includes information about the global parameters of the CNC Console IAM:

Table 3-2 Global Parameters

Parameter	Description	Details
`cncc-iam.global.iamServiceHttpPort`	This is a mandatory parameter. This should be same as kc.keycloak.service.httpPort.	**DataType:**Integer **Range**: 0-65535 **Default Value:**
`cncc-iam.global.iamSettingEnabled`	This is an optional parameter. It enables additional settings for M-CNCC IAM.	**DataType:**Boolean **Range**: True or False **Default Value:** False
`cncc-iam.global.hook.image.name`	This is a mandatory parameter. Image name for the helm hook.	**DataType:**String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** cncc/cncc-iam/hook
`cncc-iam.global.hook.image.tag`	This is a mandatory parameter. Image version tag for helm hook.	**DataType:**String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:**<current version>

Table 3-2 (Cont.) Global Parameters

Parameter	Description	Details
cncc-iam.global.hook.image.imagePullPolicy	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:** IfNotPresent, Always, Never **Default Value:**IfNotPresent
cncc-iam.global.hook.config.logLevel.root	This is a mandatory parameter. Root log level for helm hook pod.	**DataType:**String **Range:**It can take values like: WARN, DEBUG, INFO, etc. **Default Value:** INFO
cncc-iam.global.publicHttpSignalingPort	This is a mandatory parameter. If https is enabled, this Port would be HTTP/1.0 Port (unsecured). If https is disabled, this Port would be HTTPS/1.0 Port (secured SSL).	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** 8080
cncc-iam.global.publicHttpsSignallingPort	This is a mandatory parameter. If https is enabled, this Port would be HTTP/1.0 Port (unsecured). If https is disabled, this Port would be HTTPS/1.0 Port (secured SSL).	**DataType:**String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** 8443
cncc-iam.global.staticIpAddressEnabled	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress. Else random IP will be assigned by the metalLB from its IP Pool.	**DataType:**boolean **Range:** true or false **Default Value:** false
cncc-iam.global.staticIpAddress	This is an optional parameter. It is Static Ip and applicable only when ingress-gateway.cncc-iam.global.staticNodePortEnabled is true.	**DataType:**String **Range:** Valid IP address **Default Value:**10.75.212.60
cncc-iam.global.dbName	This is a mandatory parameter. It is the name of the database used for CNC Console IAM. User should create DB with the same name as provided here before deploying CNC Console IAM.	**DataType:**String **Range:**Valid String **Default Value:**

Table 3-2 (Cont.) Global Parameters

Parameter	Description	Details
`cncc-iam.global.httpsEnabled`	This is a mandatory parameter. To enable or disable https support.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`cncc-iam.global.enableIncomingHttp`	This is a mandatory parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`cncc-iam.global.enableIncomingHttps`	This is a mandatory parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`cncc-iam.global.ingressGwCertReloadEnabled`	This is a mandatory parameter. If enabled, certificates can be updated during run-time without restarting the application.	**DataType:**Boolean **Range:**True or False **Default Value:** True
`cncc-iam.ingress-gateway.nodeSelector.nodeKey`	This is an optional parameter Node selector key specific to chart (note this will be looked first and then if not present global node key will be picked).	**DataType:**String **Range:**NA **Default Value:** NA
`cncc-iam.ingress-gateway.nodeSelector.nodeValue`	This is an optional parameter Node selector value specific to chart (note this will be looked first and then if not present global node key will be picked).	**DataType:**String **Range:**NA **Default Value:** NA

3.2.2 IAM Backend Parameters

This section includes information about the IAM backend parameters of the CNC Console IAM:

Table 3-3 IAM Backend Parameters

Parameter	Description	Details
`cncc-iam.kc.preferIpv6Stack.enabled`	This is an optional parameter. The flag to enable or disable CNC Console deployment on an IPv6 setup.	**DataType:**Boolean **Range:**True or False **Default Value:** False
cncc-iam.kc.log.level	It defines the log level for the iam-kc.	**DataType:**String **Range:**TRACE,DEBUG,INFO,WARN,ERROR,FATAL,ALL,OFF

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
`cncc-iam.kc.ldaps.enabled`	This is a mandatory parameter. The flag to enable or disable LDAPS feature. .	**DataType:**Boolean **Range:**True or False **Default Value:** False
`cncc-iam.kc.ldaps.initContainersImage.name`	This is a mandatory parameter. Image name to be used for LDAPS.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:**cncc/apigw-configurationinit
`cncc-iam.kc.ldaps.initContainersImage.tag`	This is a mandatory parameter. Image version tag for LDAPS.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:**<Current Version>
`cncc-iam.kc.ldaps.initContainersImage.pullPolicy`	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent
`cncc-iam.kc.ldaps.service.customExtension.labels`	This is an optional parameter. This can be used to add custom label(s) that are specific to service and will be created by CNC Console IAM helm chart.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:**NA
`cncc-iam.kc.ldaps.service.customExtension.annotations`	This is an optional parameter. This can be used to add custom label(s) that are specific to service and will be created by CNC Console IAM helm chart.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:**NA
`cncc-iam.kc.ldaps.service.ssl.tlsVersion`	This is a mandatory parameter. TLS Version.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** TLSv1.2

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
cncc-iam.kc.ldaps.service.ssl.caBundle.k8SecretName	This is a mandatory parameter. Name of the caBundle secret. Example: cncc-iam-kc-root-ca	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**cncc-iam-kc-root-ca
cncc-iam.kc.ldaps.service.ssl.caBundle.k8NameSpace	This is a mandatory parameter. Namespace of caBundle. Example: cncc.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**cncc
cncc-iam.kc.ldaps.service.ssl.caBundle.fileName	This is a mandatory parameter. rsa caBundle file name. Example: caroot.cer	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**caroot.cer
cncc-iam.kc.ldaps.service.ssl.trustStorePassword.k8SecretName	This is a mandatory parameter. Name of the caBundle secret. Example: cncc-iam-kc-root-ca	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**cncc-iam-kc-root-ca
cncc-iam.kc.ldaps.service.ssl.trustStorePassword.k8NameSpace	This is a mandatory parameter. Namespace of caBundle. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**cncc
cncc-iam.kc.ldaps.service.ssl.trustStorePassword.fileName	This is a mandatory parameter. rsa caBundle file name. Example: ssl_truststore.txt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**ssl_truststore.txt
cncc-iam.kc.ldaps.service.ssl.initialAlgorithm	This is a mandatory parameter. Name of the initial algorithm.	**DataType:**String **Range:** **Default Value:**RS256
cncc-iam.kc.ldaps.resources.limits.initServiceCpu	This is a mandatory parameter. Init Container CPU Limit.	**DataType:**String **Range:** **Default Value:**1Gi

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
cncc-iam.kc.ldaps.resources.limits.initServiceMemory	This is a mandatory parameter. Init Container Memory Limit.	**DataType:**String **Range:** **Default Value:**1Gi
cncc-iam.kc.ldaps.resources.requests.initServiceCpu	This is a mandatory parameter. Init Container CPU Limit.	**DataType:**String **Range:** **Default Value:**0.5Gi
cncc-iam.kc.ldaps.resources.requests.initServiceMemory	This is a mandatory parameter. Init Container Memory Limit.	**DataType:**String **Range:** **Default Value:**0.5Gi
cncc-iam.kc.ldaps.ports.containerPort	This is a mandatory parameter. ContainerPort represents a network port in a single container.	**DataType:**String **Range:** 0-65535. **Default Value:**8086
cncc-iam.kc.ldaps.logLevel.initContainer	This is a mandatory parameter. Log level for initContainer logs.	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE **Default Value:**INFO
cncc-iam.kc.extraContainers	This is a mandatory parameter. To enable or disable debug tools container.	**DataType:**enum **Range:**DISABLED, ENABLED, USE_GLOBAL_VALUE **Default Value:**
cncc-iam.kc.healthcheck.image.name	This is a mandatory parameter. Image name for the helm healthcheck.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** cncc/cncc-iam/healthcheck
cncc-iam.kc.healthcheck.image.tag	This is a mandatory parameter. Image version tag for helm healthcheck.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** <Current Version>
cncc-iam.kc.healthcheck.image.pullpolicy	This is a mandatory parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent
cncc-iam.kc.healthcheck.logLevel.root	This is a mandatory parameter. Root log level for helm healthcheck container.	**DataType:**String **Range:**WARN, DEBUG, INFO, etc. **Default Value:** INFO

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
cncc-iam.kc.healthcheck.resources.limits.cpu	This is a mandatory parameter. It limits the number of CPUs to be used by the helm test container.	**DataType:**String **Range:**Valid floating point value between 0 and 1 **Default Value:** 0.5
cncc-iam.kc.healthcheck.resources.limits.memory	This is a mandatory parameter. It limits the number of memory to be used by the helm test container.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc. **Default Value:** 0.5Gi
cncc-iam.kc.healthcheck.limits.logStorage	This is a mandatory parameter. It limits the logStorage (Ephemeral storage).	**DataType:**Integer **Range:**Valid Integer value **Default Value:**
cncc-iam.kc.healthcheck.limits.criticalStorage	This is a mandatory parameter. It limits the criticalStorage (Ephemeral storage)	**DataType:**Integer **Range:**Valid Integer value **Default Value:**
cncc-iam.kc.healthcheck.resources.requests.cpu	This is a mandatory parameter. The minimum amount of CPUs required.	**DataType:**String **Range:**Valid floating point value between 0 and 1 **Default Value:** 0.3
cncc-iam.kc.healthcheck.resources.requests.memory	This is a mandatory parameter. The minimum amount of memory required.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc. **Default Value:** 0.3Gi
cncc-iam.kc.healthcheck.limits.logStorage	This is a mandatory parameter. Minimum memory for logStorage (Ephemeral storage).	**DataType:**Integer **Range:**Valid Integer value **Default Value:**
cncc-iam.kc.healthcheck.limits.criticalStorage	This is a mandatory parameter. Minimum memory for criticalStorage (Ephemeral storage).	**DataType:**Integer **Range:**Valid Integer value **Default Value:**
cncc-iam.kc.service.customExtension.labels	This is an optional parameter. This can be used to add custom label(s) that are specific to service and will be created by CNC Console IAM helm chart.	**DataType:**String **Range:** **Default Value:** NA
cncc-iam.kc.service.customExtension.annotations	This is an optional parameter. This can be used to add custom annotations that are specific to service and will be created by CNC Console IAM helm chart.	**DataType:**String **Range:** **Default Value:** NA

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
`cncc-iam.kc.keycloak.image.name`	This is a mandatory parameter. Image Name to be used for CNC Console IAM microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** cncc/cncc-iam
`cncc-iam.kc.keycloak.image.tag`	This is a mandatory parameter. Image Tag to be used for CNC Console IAM microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** <Current Version>
`cncc-iam.kc.keycloak.image.pullpolicy`	This is a mandatory parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent
`cncc-iam.kc.keycloak.serviceAccount.create`	This is an optional parameter. Flag for creating service account.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`cncc-iam.kc.keycloak.serviceAccount.name`	This is an optional parameter. The name of service account. Applicable only if keycloak.serviceAccount.create is set to 'true'. If keycloak.serviceAccount.name is kept empty, a default service account with name 'cncc-iam' is created by CNC Console, otherwise user has to create the service account and provide its name here. `kubectl create serviceaccount <name> -n <namespace>`	**DataType:**String **Range:** values will be set by global.serviceAccountName **Default Value:**
`cncc-iam.kc.keycloak.username`	This is a mandatory parameter. .It is the name of CNC Console IAM user as given by the user. Example: admin	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. **Default Value:**admin

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
`cncc-iam.kc.keycloak.existingSecret`	This is a mandatory parameter. It specifies an existing secret name to be used for the admin password. Example: cncc-iam-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** cncc-iam-secret
`cncc-iam.kc.keycloak.existingSecretKey`	This is a mandatory parameter. Applicable only if keycloak.existingSecret is provided. It is the key in the existing secret that stores the password. Example: iamAdminPasswordKey	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** iamAdminPasswordKey
`cncc-iam.kc.keycloak.service.httpPort`	This is an optional parameter. It is the port number which makes CNC Console IAM service visible to other services running within the same kubernetes cluster.	**DataType:**String **Range:** Values will be set by global.iamServiceHttpPort **Default Value:** 8285
`cncc-iam.kc.keycloak.resources.limits.cpu`	This is a mandatory parameter. It limits the number of CPUs to be used by the helm test container.	**DataType:**String **Range:**Valid floating point value between 0 and 1 **Default Value:**
`cncc-iam.kc.keycloak.resources.limits.memory`	This is a mandatory parameter. It limits the number of memory to be used by the helm test container.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc. **Default Value:**
`cncc-iam.kc.keycloak.resources.requests.cpu`	This is a mandatory parameter. The minimum amount of CPUs required.	**DataType:**String **Range:**Valid floating point value between 0 and 1. **Default Value:**
`cncc-iam.kc.keycloak.resources.requests.memory`	This is a mandatory parameter. The minimum amount of memory required.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc. **Default Value:**
`cncc-iam.kc.keycloak.persistence.dbVendor`	This is a mandatory parameter. It is the database vendor name. Example: mysql	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. **Default Value:** mysql

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
`cncc-iam.kc.keycloak.persistence.dbName`	This is a mandatory parameter. It is the name of the database used for CNC Console IAM. User should create DB with the same name as provided here before deploying CNC Console IAM Example: cnccdb	**DataType:**String **Range:** Values will be set by global.dbName **Default Value:** This values gets read from global variable *mySqlDbRef, no changes needed here.
`cncc-iam.kc.keycloak.persistence.dbHost`	This is a mandatory parameter. It the hostname for persistence db. Example: mysql-sds.default.svc.cluster.local.	**DataType:**String **Range:** Values will be set by global.dbHost **Default Value:** This values gets read from global variable *mySqlHostRef, no changes needed here.
`cncc-iam.kc.keycloak.persistence.dbPort`	This is a mandatory parameter. It is the db port for CNC Console IAM. Example: 3306	**DataType:**Integer **Range:** Values will be set by global.dbPort **Default Value:** This values gets read from global variable *mySqlPortRef, no changes needed here.
`cncc-iam.kc.keycloak.persistence.existingSecret`	This is a mandatory parameter. It specifies an existing secret to be used for mysql username and password. Example: cncc-db-secret	**DataType:**String **Range:** Values will be set by global.secretName **Default Value:** This values gets read from global variable *mySqlSecretNameRef, no changes needed here.
`cncc-iam.kc.keycloak.persistence.existingSecretPasswordKey`	This is a mandatory parameter. It is the key in the existing secret that stores the password. Example: dbPasswordKey	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** dbPasswordKey
`cncc-iam.kc.keycloak.persistence.existingSecretUsernameKey`	This is an optional parameter. It is the key in the existing secret that stores the username. Example: `dbUserNameKey`	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** dbUserNameKey

Table 3-3 (Cont.) IAM Backend Parameters

Parameter	Description	Details
`cncc-iam.kc.keycloak.nodeSelector.nodeKey`	This is an optional parameter. Node selector key specific to chart (note this will be looked first and then if not present global node key will be picked).	**DataType:**String **Range:** **Default Value:** NA
`cncc-iam.kc.keycloak.nodeSelector.nodeValue`	This is an optional parameter. Node selector value specific to chart (note this will be looked first and then if not present global node key will be picked).	**DataType:**String **Range:** **Default Value:** NA

3.2.3 Ingress Gateway Parameters

This section includes information about the Ingress Gateway parameters of the CNC Console IAM:

Table 3-4 Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.extraContainers`	This is a mandatory parameter. To enable or disable debug tools container.	**DataType:**enum **Range:**DISABLED, ENABLED, USE_GLOBAL_VALUE **Default Value:** USE_GLOBAL_VALUE
`cncc-iam.ingress-gateway.prefix`	This is a mandatory parameter. Metrics Instance Identifier to uniquely identify both Manager CNC Console Core and Agent CNC Console IAM metrics.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods and dashes. An image name may not start with a period, or a dash and may contain a maximum of 128 characters **Default Value:**'cncc-iam'
`cncc-iam.ingress-gateway.image.name`	This is a mandatory parameter. Image Name to be used for "cncc-iam.ingress-gateway" microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods and dashes. An image name may not start with a period, or a dash and may contain a maximum of 128 characters. **Default Value:** cncc/cncc-apigateway
`cncc-iam.ingress-gateway.image.tag`	This is a mandatory parameter. Image Tag to be used for "cncc-iam.ingress-gateway" microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** <Current Version>

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.image.pullPolicy`	This is a mandatory parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:**IfNotPresent
`cncc-iam.ingress-gateway.initContainersImage.name`	This is a mandatory parameter. Image Name to be used for init container.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods and dashes. An image name may not start with a period, or a dash and may contain a maximum of 128 characters. **Default Value:** cncc/apigw-configurationinit
`cncc-iam.ingress-gateway.initContainersImage.tag`	This is a mandatory parameter. Image tag to be used for init container.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods and dashes. A tag name may not start with a period, or a dash and may contain a maximum of 128 characters. **Default Value:**<Current Version>
`cncc-iam.ingress-gateway.initContainersImage.pullPolicy`	This is a mandatory parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent
`cncc-iam.ingress-gateway.service.ssl.tlsVersion`	This is a mandatory parameter. TLS Version	**DataType:**String **Range:** **Default Value:** TLSv1.2
`cncc-iam.ingress-gateway.service.ssl.privateKey.k8SecretName`	This is a mandatory parameter. Name of the privatekey secret. Example: cncc-iam-cncc-iam.ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc-iam-cncc-iam.ingress-secret
`cncc-iam.ingress-gateway.service.ssl.privateKey.k8NameSpace`	This is a mandatory parameter. Namespace of privatekey. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**CNC Console

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.service.ssl.privateKey.rsa.fileName`	This is a mandatory parameter. rsa private key file name. Example: rsa_private_key_pkcs1.pem	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** rsa_private_key_pkcs1.pem
`cncc-iam.ingress-gateway.service.ssl.privateKey.ecdsa.fileName`	This is a mandatory parameter. ecdsa private key file name. Example: ssl_ecdsa_private_key.pem	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_ecdsa_private_key.pem
`cncc-iam.ingress-gateway.service.ssl.certificate.k8SecretName`	This is a mandatory parameter. Name of the certificate secret. Example: cncc-iam-cncc-iam.ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, period, and dashes. A name component may not start or end with a separator. **Default Value:** cncc-iam-cncc-iam.ingress-secret
`cncc-iam.ingress-gateway.service.ssl.certificate.k8NameSpace`	This is a mandatory parameter. Namespace of certificate. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, period, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
`cncc-iam.ingress-gateway.service.ssl.certificate.rsa.fileName`	This is a mandatory parameter. rsa certificate file name. Example: ssl_rsa_certificate.crt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_rsa_certificate.crt
`cncc-iam.ingress-gateway.service.ssl.certificate.ecdsa.fileName`	This is a mandatory parameter. ecdsa certificate file name. Example: ssl_ecdsa_certificate.crt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_ecdsa_certificate.crt

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.service.ssl.caBundle.k8SecretName`	This is a mandatory parameter. Name of the caBundle secret. Example: cncc-iam-cncc-iam.ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ncc-iam-cncc-iam.ingress-secret
`cncc-iam.ingress-gateway.service.ssl.caBundle.k8NameSpace`	This is a mandatory parameter. Namespace of caBundle. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
`cncc-iam.ingress-gateway.service.ssl.caBundle.fileName`	This is a mandatory parameter. rsa caBundle file name. Example: caroot.cer	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:**caroot.cer
`cncc-iam.ingress-gateway.service.ssl.initialAlgorithm`	This is a mandatory parameter. This is initial Algorithm. Example: RSA256	**DataType:**String **Range:** **Default Value:** RS256
`cncc-iam.ingress-gateway.service.customExtension.labels`	This is an optional parameter. This can be used to add custom label(s) to cncc-iam.ingress-gateway Service.	**DataType:**String **Range:**Custom Labels that needs to be added to cncc-iam.ingress-gateway specific Service. **Default Value:**{}
`cncc-iam.ingress-gateway.service.customExtension.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to cncc-iam.ingress-gateway service.	**DataType:**String **Range:**Custom Annotations that needs to be added to cncc-iam.ingress-gateway specific Services. **Default Value:**{}
`cncc-iam.ingress-gateway.deployment.customExtension.labels`	This is an optional parameter. This can be used to add custom label(s) to cncc-iam.ingress-gateway deployment.	**DataType:**String **Range:**Custom Labels that needs to be added to cncc-iam.ingress-gateway specific deployment. **Default Value:** {}
`cncc-iam.ingress-gateway.deployment.customExtension.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to cncc-iam.ingress-gateway deployment.	**DataType:**String **Range:**Custom Annotations that needs to be added to cncc-iam.ingress-gateway specific deployment. **Default Value:**{}

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.ports.containerPort`	This is a mandatory parameter. ContainerPort represents a network port in a single container.	**DataType:**String **Range:**0-65535. **Default Value:**8081
`cncc-iam.ingress-gateway.ports.containersslPort`	This is a mandatory parameter. This is container ssl port.	**DataType:**String **Range:** **Default Value:**8443
`cncc-iam.ingress-gateway.ports.actuatorPort`	This is a mandatory parameter. This is actuator Port.	**DataType:**String **Range:** **Default Value:** 9090
`cncc-iam.ingress-gateway.log.level.root`	This is a mandatory parameter. It is the level at which user wants to see the logs. E.g. WARN	**DataType:**String **Range:** WARN, DEBUG, INFO, TRACE etc. **Default Value:** WARN
`cncc-iam.ingress-gateway.log.level.cncc-iam.ingress`	This is a mandatory parameter. Log level for cncc-iam.ingress logs.	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
`cncc-iam.ingress-gateway.log.level.cncc.security`	This is a mandatory parameter. Log level for cncc security logs.	**DataType:**String **Range:** WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
`cncc-iam.ingress-gateway.log.level.cncc.root`	This is a mandatory parameter. Log level for CNC Console root logs.	**DataType:**String **Range:** WARN, DEBUG, INFO, TRACE etc. **Default Value:**WARN
`cncc-iam.ingress-gateway.readinessProbe.initialDelaySeconds`	This is a mandatory parameter. It tells the kubelet that it should wait the mentioned seconds before performing the first probe.	**DataType:**String **Range:**0-65535 **Default Value:** 30
`cncc-iam.ingress-gateway.readinessProbe.timeoutSeconds`	This is a mandatory parameter. It is the number of seconds after which the probe times out.	**DataType:**String **Range:**0-65535 **Default Value:**3
`cncc-iam.ingress-gateway.readinessProbe.periodSeconds`	This is a mandatory parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**String **Range:** 0-65535 **Default Value:** 10

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.readinessProbe.successThreshold`	This is a mandatory parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**String **Range:**0-65535. **Default Value:** 1
`cncc-iam.ingress-gateway.readinessProbe.failureThreshold`	This is a mandatory parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**String **Range:**0-65535. **Default Value:** 3
`cncc-iam.ingress-gateway.livenessProbe.initialDelaySeconds`	This is a mandatory parameter. It tells the kubelet that it should wait the mentioned seconds before performing the first probe.	**DataType:**String **Range:**0-65535. **Default Value:** 30
`cncc-iam.ingress-gateway.livenessProbe.timeoutSeconds`	This is a mandatory parameter. It is the number of seconds after which the probe times out.	**DataType:**String **Range:**0-65535. **Default Value:** 3
`cncc-iam.ingress-gateway.livenessProbe.periodSeconds`	This is a mandatory parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**String **Range:**0-65535. **Default Value:** 15
`cncc-iam.ingress-gateway.livenessProbe.successThreshold`	This is a mandatory parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**String **Range:**0-65535. **Default Value:** 1
`cncc-iam.ingress-gateway.livenessProbe.failureThreshold`	This is a mandatory parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**String **Range:**0-65535. **Default Value:** 3
`cncc-iam.ingress-gateway.resources.limits.cpu`	This is a mandatory parameter. It limits the number of CPUs to be used by the microservice.	**DataType:**String **Range:**Valid floating point value between 0 and 1 **Default Value:**
`cncc-iam.ingress-gateway.resources.limits.initServiceCpu`	This is a mandatory parameter. Init Container CPU Limit.	**DataType:**String **Range:** **Default Value:** 1

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.resources.limits.memory`	This is a mandatory parameter. It limits the memory utilization by the "cncc-cmservice" microservice. By default, it is set to '2'.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc **Default Value:** 2Gi
`cncc-iam.ingress-gateway.resources.limits.initServiceMemory`	This is a mandatory parameter. Init Container Memory Limit.	**DataType:**String **Range:** **Default Value:** 1Gi
`cncc-iam.ingress-gateway.resources.requests.cpu`	This is a mandatory parameter. It limits the number of CPUs to be used by the "cncc-cmservice" microservice. By default, it is set to '2'.	**DataType:**String **Range:**Valid floating point value between 0 and 1 **Default Value:** 1
`cncc-iam.ingress-gateway.resources.requests.initServiceCpu`	This is a mandatory parameter. Init Container CPU Limit.	**DataType:**String **Range:** **Default Value:** 1
`cncc-iam.ingress-gateway.resources.requests.memory`	This is a mandatory parameter. It limits the memory utilization by the "cncc-cmservice" microservice. By default, it is set to '2'.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc. **Default Value:** 1Gi
`cncc-iam.ingress-gateway.resources.requests.initServiceMemory`	This is a mandatory parameter. Init Container Memory for requests.	**DataType:**String **Range:** **Default Value:** 1Gi
`cncc-iam.ingress-gateway.resources.target.averageCpuUtil`	This is a mandatory parameter. It gives the average CPU utilization percentage.	**DataType:**String **Range:**A value in between 0-100 **Default Value:**80
`cncc-iam.ingress-gateway.service.ssl.keyStorePassword.k8SecretName`	This is a mandatory parameter. Name of the keyStorePassword secret. Example: cncc-iam-cncc-iam.ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc-iam-cncc-iam.ingress-secret
`cncc-iam.ingress-gateway.service.ssl.keyStorePassword.k8NameSpace`	This is a mandatory parameter. Namespace of keyStorePassword. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.service.ssl.keyStorePassword.fileName`	This is a mandatory parameter. File name that has password for keyStore. Example: ssl_keystore.txt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**ssl_keystore.txt
`cncc-iam.ingress-gateway.service.ssl.trustStorePassword.k8SecretName`	This is a mandatory parameter. Name of the trustStorePassword secret. Example: cncc-iam-cncc-iam.ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**cncc-iam-cncc-iam.ingress-secret
`cncc-iam.ingress-gateway.service.ssl.trustStorePassword.k8NameSpace`	This is a mandatory parameter. Namespace of trustStorePassword. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc
`cncc-iam.ingress-gateway.service.ssl.trustStorePassword.fileName`	This is a mandatory parameter. File name that has password for trustStore. Example: ssl_truststore.txt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** ssl_truststore.txt
`cncc-iam.ingress-gateway.cipherSuites`	This is a mandatory parameter (if cncc-iam.ingressgateway.enableIncomingHttps is true). Allowed CipherSuites for TLS1.2	**DataType:**List[String] **Range:** TLS_ECDHE_ ECDSA_WIT H_AES_256_ GCM_SHA38 4 TLS_ECDHE_ RSA_WITH_ AES_256_GC M_SHA384 TLS_ECDHE_ RSA_WITH_ CHACHA20_ POLY1305_S HA256 TLS_ECDHE_ ECDSA_WIT H_AES_128_ GCM_SHA25 6 TLS_ECDHE_ RSA_WITH_ AES_128_GC M_SHA256 **Default Value:**
`cncc-iam.ingress-gateway.initssl`	This is a mandatory parameter. To Initialize SSL related infrastructure in init container.	**DataType:**String **Range:** Values will be set by global.httpsEnabled **Default Value:** NA

Table 3-4 (Cont.) Ingress Gateway Parameters

Parameter	Description	Details
`cncc-iam.ingress-gateway.enableIncomingHttp`	This is a mandatory parameter. Server Configuration for http and https support.	**DataType:**String **Range:** Values will be set by global.enableIncomingHttp **Default Value:**
`cncc-iam.ingress-gateway.enableIncomingHttps`	This is a mandatory parameter. Server Configuration for http and https support.	**DataType:**String **Range:** Values will be set by global.enableIncomingHttps **Default Value:**
`cncc-iam.ingress-gateway.needClientAuth`	This is a mandatory parameter. This must be true if client certificate identity is required in the header x-custom-cncc-iam.ingress-client-identity. **Note**: This parameter will be set to true only in case of ACNCC-CORE deployment.	**DataType:**Boolean **Range:** Values will be set by global.needClientAuth **Default Value:**
`cncc-iam.ingress-gateway.cncc-iam.ingressGwCertReloadEnabled`	This is a mandatory parameter. If enabled, then certificates can be updated during run-time without restarting the application.	**DataType:**Boolean **Range:** True or False **Default Value:** Values will be set by global.cncc-iam.ingressGwCertReloadEnabled
`cncc-iam.ingress-gateway.clusterDomain`	This is a mandatory parameter. Cluster Domain where CNC Console will be deployed.	**DataType:**string **Range:** **Default Value:** Values will be set by global.clusterDomain
`cncc-iam.ingress-gateway.cncc.securitylogEnabled`	This is a mandatory parameter. This flag is to enable or disable security logs for CNC Console.	**DataType:**Boolean **Range:** True or False **Default Value:** True
`cncc-iam.ingress-gateway.cncc.iam.port`	This is a mandatory parameter. This should be same as kc.keycloak.service.httpPort	**DataType:**Integer **Range:** Values will be set by global.iamServiceHttpPort **Default Value:**

3.3 M-CNCC Core Configuration Options

This section includes information about the configuration parameters of M-CNCC Core.

> **Note**
>
> The options mentioned in the following tables can be read as *mcncc-core.<field Name>*.
>
> Example: The *global.dbName* can be read as *mcncc-core.global.dbName* or *acncc-core.global.dbName*.

3.3.1 Global Parameters

This section includes information about the global parameters of the CNC Console Core:

Table 3-5 Global Parameters

Parameter	Description	Details
`global.publicHttpSignalingPort`	This is an optional parameter. It is the port on which Ingress Gateway service is exposed. If httpsEnabled is false, this Port would be HTTP/2.0 Port (unsecured). publicHttpSignalingPort: 80	**DataType:**Integer **Range:**0-65535. **Default Value:**80
`global.publicHttpsSignallingPort`	This is an optional parameter. It is the port on which Ingress Gateway service is exposed. If httpsEnabled is true, this Port would be HTTPS/2.0 Port (secured SSL).	**DataType:**Integer **Range:**0-65535. **Default Value:**443
`global.staticIpAddressEnabled`	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress else random IP will be assigned by the metalLB from its IP Pool.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`global.staticIpAddress`	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress else random IP will be assigned by the metalLB from its IP Pool.	**DataType:**String **Range:**Valid ASCII aserviceAccountNamend may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:**
`global.dbName`	This is a mandatory parameter. It is the name of the database used for M-CNCC Core user should create DB with unique name before deploying M-CNCC Core.	**DataType:**String **Range:**Valid string **Default Value:** • mcncccommonconfig in case of mcncc-core

Table 3-5 (Cont.) Global Parameters

Parameter	Description	Details
`global.httpsEnabled`	This is an optional parameter. To Initialize SSL related infrastructure in init container.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`global.enableIncomingHttp`	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`global.enableIncomingHttps`	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** False
`global.ingressGwCertReloadEnabled`	This is an optional parameter. If enabled, then certificates can be updated during run-time without up/restart of the application.	**DataType:**Boolean **Range:**True or False **Default Value:** False

3.3.2 Core Backend Parameters

This section includes information about the core backend parameters of the CNC Console Core.

Table 3-6 Core Backend Parameters

Attribute Name	Description	Details
`cmservice.envLoggingLevelApp`	This is an optional parameter. It is the level at which user wants to see the logs. Example: WARN	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE **Default Value:** WARN
`cmservice.image.name`	This is a mandatory parameter. Image Name to be used for "cncc-cmservice" microservice.	**DataType:**String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** cncc/cncc-cmservice
`cmservice.image.tag`	This is a mandatory parameter. Image Tag to be used for "cncc-cmservice" microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An tag name may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** <Current Version>

Table 3-6 (Cont.) Core Backend Parameters

Attribute Name	Description	Details
`cmservice.image.pullPolicy`	This is a mandatory parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:** It can take a value from the following: IfNotPresent, Always, Never IfNotPresent is the default pullPolicy **Default Value:** IfNotPresent
`cmservice.persistence.dbName`	This is an optional parameter. It is the name of the database used for cncc-core. User should create DB with the same name as provided here before deploying CNC Console Core. This values gets read from global variable *mySqlDbRef, no changes needed here. Example: cncccommonconfig	**DataType:**String **Range:**Valid String **Default Value:**
`cmservice.persistence.dbHost`	This is an optional parameter. It the hostname for persistence db. This values gets read from global variable *mySqlHostRef, no changes needed here Example: mysql-sds.default.svc.cluster.local	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. **Default Value:**
`cmservice.persistence.dbPort`	This is an optional parameter. It is the db port for cncc-core. This values gets read from global variable *mySqlPortRef, no changes needed here. Example: 3306	**DataType:**Integer **Range:**0-65535 **Default Value:**
`cmservice.persistence.existingSecret`	This is an optional parameter. It specifies an existing secret to be used for mysql username and password. This values gets read from global variable *mySqlSecretNameRef, no changes needed here. Example: cncc-db-secret	**DataType:**String **Range:** Values will be set by global.secretName Default value is cncc-db-secret **Default Value:**
`cmservice.persistence.existingSecretPasswordKey`	This is an optional parameter. It is the key in the existing secret that stores the password. Example: dbPasswordKey	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** dbPasswordKey

Table 3-6 (Cont.) Core Backend Parameters

Attribute Name	Description	Details
`cmservice.persistence.existingSecretUsernameKey`	This is an optional parameter. It is the key in the existing secret that stores the username. Example: `dbUserNameKey`	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters. **Default Value:** dbUserNameKey
`cmservice.resources.limits.cpu`	This is an optional parameter. It limits the number of CPUs to be used by the "cncc-cmservice" microservice. By default, it is set to '2'.	**DataType:**Float **Range:**Valid floating point value between 0 and 1 **Default Value:**
`cmservice.resources.limits.memory`	This is an optional parameter. It limits the memory utilization by the "cncc-cmservice" microservice. By default, it is set to '2'.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi **Default Value:** 2Gi
`cmservice.resources.limits.logStorage`	This is an optional parameter. It limits the logStorage (ephemeral storage) to be used by the helm test pod.	**DataType:**Integer **Range:**Values will be set by global.ephemeralStorage.limits.containerLogStorage **Default Value:** 2Gi
`cmservice.resources.limits.criticalStorage`	This is an optional parameter. It limits the criticalStorage (ephemeral storage) to be used by the helm test pod.	**DataType:**Integer **Range:**Values will be set by global.ephemeralStorage.limits.containerCrititcalStorage **Default Value:** 2Gi
`cmservice.resources.requests.cpu`	This is an optional parameter. It provides a given number of CPUs for the "cncc-cmservice" microservice.	**DataType:**Float **Range:**Valid floating point value between 0 and 1 **Default Value:**1
`cmservice.resources.requests.memory`	This is an optional parameter. It provides a given amount of memory for the "cncc-cmservice" microservice. By default, it is set to '1.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi **Default Value:** 1
`cmservice.resources.requests.logStorage`	This is an optional parameter. The minimum amount of logStorage (ephemeral storage).	**DataType:**Integer **Range:**Values will be set by global.ephemeralStorage.requests.containerLogStorage
`cmservice.resources.requests.criticalStorage`	This is an optional parameter. The minimum amount of criticalStorage (ephemeral storage).	**DataType:**Integer **Range:**Values will be set by global.ephemeralStorage.requests.containerCrititcalStorage

Table 3-6 (Cont.) Core Backend Parameters

Attribute Name	Description	Details
`cmservice.extraContainers`	This is a mandatory parameter. To enable or disable debug tools container.	**DataType:**enum **Range:** DISABLED, ENABLED, USE_GLOBAL_VALUE **Default Value:** USE_GLOBAL_VALUE
`cmservice.deployment.customExtension.labels`	This is an optional parameter. This can be used to add custom label(s) to all kubernetes resources that will be created by cmservice helm chart.	**DataType:**String **Range:**Custom Labels that needs to be added to all the cmservice kubernetes resources.
`cmservice.deployment.customExtension.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all kubernetes resources that will be created by cmservice helm chart.	**DataType:**String **Range:**Custom Annotations that needs to be added to all the cmservice kubernetes resources.
`cmservice.deployment.envSystemName`	This is a mandatory parameter. This is the name of product which appears as brand name and can be used to mention site name as well. Example: envSystemName: CNCC	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**
`cmservice.deployment.envNFVersion`	This is a mandatory parameter. This is the version of product which appears with brand name. Example: envNFVersion: 24.1.1	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** <Current Version>
`cmservice.deployment.cmWindowName`	This is the name of the window that appears on the browser tab. Example: cmWindowName: CNCC	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** CNCC
`cmservice.deployment.nodeSelector.nodeKey`	This is an optional parameter. Node Selector Key. (note this will be looked first and then if not present global node key will be picked).	**DataType:**Boolean **Range:**True or False **Default Value:**False
`cmservice.deployment.nodeSelector.nodeValue`	This is an optional parameter. Node Selector value.(note this will be looked first and then if not present global node key will be picked).	**DataType:**Integer **Range:** **Default Value:** zone.

Table 3-6 (Cont.) Core Backend Parameters

Attribute Name	Description	Details
cmservice.deployment.livenessProbe.initialDelaySeconds	This is an optional parameter. It tells the kubelet that it should wait second before performing the first probe.	**DataType:**Integer **Range:**0-65535. **Default Value:** 60
cmservice.deployment.livenessProbe.periodSeconds	This is an optional parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
cmservice.deployment.livenessProbe.timeoutSeconds	This is an optional parameter. It is the number of seconds after which the probe times out.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 15
cmservice.deployment.livenessProbe.successThreshold	This is an optional parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**Integer **Range:**0-65535. **Default Value:** 1
cmservice.deployment.livenessProbe.failureThreshold	This is an optional parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
cmservice.deployment.readinessProbe.initialDelaySeconds	This is an optional parameter. It tells the kubelet that it should wait second before performing the first probe.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 20
cmservice.deployment.readinessProbe.timeoutSeconds	This is an optional parameter. It is the number of seconds after which the probe times out.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 3
cmservice.deployment.readinessProbe.periodSeconds	This is an optional parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**Integer **Range:**0-65535. **Default Value:** 10
cmservice.deployment.readinessProbe.successThreshold	This is an optional parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**Integer **Range:**0-65535. **Default Value:** 1
cmservice.deployment.readinessProbe.failureThreshold	This is an optional parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 3
cmservice.deployment.startupProbe.initialDelaySeconds	This is an optional parameter. It tells the kubelet that it should wait second before performing the first probe.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 60

Table 3-6 (Cont.) Core Backend Parameters

Attribute Name	Description	Details
`cmservice.deployment.startupProbe.periodSeconds`	This is an optional parameter. It specifies that the kubelet should perform a liveness probe every xx second.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 3
`cmservice.deployment.startupProbe.timeoutSeconds`	This is an optional parameter. It is the number of seconds after which the probe times out.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 15
`cmservice.deployment.startupProbe.successThreshold`	This is an optional parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 1
`cmservice.deployment.startupProbe.failureThreshold`	This is an optional parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**Integer **Range:** 0-65535. **Default Value:** 3
`cmservice.deployment.dependenciesLogging[].name`	This is an optional parameter. Name of the package that for which log level is to be set. Eg: logging.level.org.springframework	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**
`cmservice.deployment.dependenciesLogging[].value`	This is an optional parameter. It is the level at which user wants to see the logs. Example: WARN	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE **Default Value:**
`cmservice.service.customExtension.labels`	This is an optional parameter. This can be used to add custom label(s) to all kubernetes resources that will be created by cmservice helm chart.	**DataType:**String **Range:**Custom Labels that needs to be added to all the cmservice kubernetes resources.
`cmservice.service.customExtension.annotations`	This is an optional parameter. This can be used to add custom annotation(s) to all kubernetes resources that will be created by cmservice helm chart.	**DataType:**String **Range:**Custom Annotations that needs to be added to all the cmservice kubernetes resources.
`cmservice.service.type`	This is an optional parameter. It is used to decide where user wants to expose the service from outside the Kubernetes cluster or not.	**DataType:**String **Range:** **Default Value:** ClusterIP

Table 3-6 (Cont.) Core Backend Parameters

Attribute Name	Description	Details
`cmservice.servicePorts.cmServiceHttp`	This is an optional parameter. It is the port number which makes cmservice visible to other services running within the same kubernetes cluster.	**DataType:**Integer **Range:**0-65535
`cmservice.containerPorts.monitoringHttp`	This is an optional parameter. It is the monitoring container port for cm service.	**DataType:**Integer **Range:**0-65535 **Default Value:**
`cmservice.containerPorts.cmServiceHttp`	This is an optional parameter. It is the container port for cm service.	**DataType:**Integer **Range:**0-65535 **Default Value:**

3.3.3 Ingress Gateway Parameters

This section includes information about the Ingress Gateway parameters of the CNC Console Core.

Table 3-7 Ingress Gateway Parameters

Attribute Name	Description	Details
`ingress-gateway.extraContainers`	This is a mandatory parameter. To enable or disable debug tools container.	**DataType:**enum **Range:**DISABLED, ENABLED, USE_GLOBAL_VALUE **Default Value:** USE_GLOBAL_VALUE
`ingress-gateway.prefix`	This is a mandatory parameter. Metrics Instance Identifier to uniquely identify CNC Console Core metrics.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** /grafana
`ingress-gateway.image.name`	This is a mandatory parameter. It is the image name of the Ingress Gateway as provided by the user.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc/cncc-apigateway
`ingress-gateway.image.tag`	This is a mandatory parameter. Image Tag to be used for Ingress Gateway.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** <Current Version>

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.image.pullPolicy	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent
ingress-gateway.initContainersImage.name	This is a mandatory parameter. Image Name to be used for "cncc-cmservice" microservice	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc/apigw-configurationinit
ingress-gateway.initContainersImage.tag	This is a mandatory parameter. Image Tag to be used for "cncc-cmservice" microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** <Current Version>
ingress-gateway.initContainersImage.pullPolicy	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent
ingress-gateway.service.ssl.tlsVersion	This is an optional parameter. It is the TLS version.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:**TLSv1.2
ingress-gateway.service.ssl.privateKey.k8SecretName	This is an optional parameter. Name of the privatekey secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc-core-ingress-secret
ingress-gateway.service.ssl.privateKey.k8NameSpace	This is an optional parameter. Namespace of privatekey. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.service.ssl.privateKey.rsa.fileName	This is an optional parameter. RSA private key file name. Example: rsa_private_key_pkcs1.pem	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** rsa_private_key_pkcs1.pem
ingress-gateway.service.ssl.privateKey.ecdsa.fileName	This is an optional parameter. ecdsa private key file name. Example: ssl_ecdsa_private_key.pem	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_ecdsa_private_key.pem
ingress-gateway.service.ssl.certificate.k8SecretName	This is an optional parameter. Name of the certificate secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**cncc-core-ingress-secret
ingress-gateway.service.ssl.certificate.k8NameSpace	This is an optional parameter. Namespace of certificate. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
ingress-gateway.service.ssl.certificate.rsa.fileName	This is an optional parameter. RSA certificate file name. Example: ssl_rsa_certificate.crt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_rsa_certificate.crt
ingress-gateway.service.ssl.certificate.ecdsa.fileName	This is an optional parameter. ECDSA certificate file name. Example: ssl_ecdsa_certificate.crt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_ecdsa_certificate.crt
ingress-gateway.service.ssl.caBundle.k8SecretName	This is an optional parameter. Name of the caBundle secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc-core-ingress-secret

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.service.ssl.caBundle.k8NameSpace	This is an optional parameter. Namespace of caBundle. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
ingress-gateway.service.ssl.caBundle.fileName	This is an optional parameter. RSA caBundle file name. Example: caroot.cer	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** caroot.cer
ingress-gateway.service.ssl.keyStorePassword.k8SecretName	This is an optional parameter. Name of the keyStorePassword secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc-core-ingress-secret
ingress-gateway.service.ssl.keyStorePassword.k8NameSpace	This is an optional parameter. Namespace of keyStorePassword. Example: cncc	**DataType:**String **Range:**VValid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
ingress-gateway.service.ssl.keyStorePassword.fileName	This is an optional parameter. File name that has password for keyStore. Example: ssl_keystore.txt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_keystore.txt
ingress-gateway.service.ssl.trustStorePassword.k8SecretName	This is an optional parameter. Name of the trustStorePassword secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc-core-ingress-secret
ingress-gateway.service.ssl.trustStorePassword.k8NameSpace	This is an optional parameter. Namespace of trustStorePassword. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.service.ssl.trustStorePassword.fileName	This is an optional parameter. File name that has password for trustStore. Example: ssl_truststore.txt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_truststore.txt
ingress-gateway.service.ssl.initialAlgorithm	This is an optional parameter. Default values is RSA256.	**DataType:**String **Range:**VValid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** RS256
ingress-gateway.service.customExtension.labels	This is an optional parameter. This can be used to add custom label(s) to Ingress Gateway service.	**DataType:**String **Range:**Custom Labels that needs to be added to ingress gateway specific service. **Default Value:** NA
ingress-gateway.service.customExtension.annotations	This is an optional parameter. This can be used to add custom annotation(s) to Ingress Gateway service.	**DataType:**String **Range:**VCustom Labels that needs to be added to ingress gateway specific service. **Default Value:** NA
ingress-gateway.deployment.customExtension.labels	This is an optional parameter. This can be used to add custom label(s) to Ingress Gateway deployment.	**DataType:**String **Range:**Custom Labels that needs to be added to ingress gateway specific service. **Default Value:** NA
ingress-gateway.deployment.customExtension.annotations	This is an optional parameter. This can be used to add custom annotation(s) to Ingress Gateway deployment.	**DataType:**String **Range:**Custom Annotations that needs to be added to ingress gateway specific deployment. **Default Value:** NA
ingress-gateway.ports.containerPort	This is an optional parameter. It is the http port of the container for the Ingress Gateway.	**DataType:**Integer **Range:**0-65535 **Default Value:** 8081
ingress-gateway.ports.containersslPort	This is an optional parameter. It is the https port of the container for the Ingress Gateway.	**DataType:**Integer **Range:**0-65535 **Default Value:** 8443
ingress-gateway.ports.actuatorPort	This is an optional parameter. It is the actuator port of the container for the Ingress Gateway.	**DataType:**Integer **Range:**0-65535 **Default Value:** 9090
ingress-gateway.log.level.root	This is an optional parameter. It is the level at which user wants to see the logs. Example: WARN	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.log.level.ingress	This is an optional parameter. Log level for ingress logs.	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
ingress-gateway.log.level.cncc.root	This is a mandatory parameter. Log level for CNC Console root logs.	**DataType:**String **Range:** WARN, DEBUG, INFO, TRACE etc. **Default Value:**WARN
ingress-gateway.log.level.cncc.audit	This is a mandatory parameter. Log level for CNC Console audit logs.	**DataType:**String **Range:** WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
ingress-gateway.log.level.cncc.security	This is an optional parameter. Log level for CNC Console security logs.	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
ingress-gateway.readinessProbe.initialDelaySeconds	This is an optional parameter. It tells the kubelet that it should wait second before performing the first probe.	**DataType:**Integer **Range:**0-65535. **Default Value:** 30
ingress-gateway.readinessProbe.timeoutSeconds	This is an optional parameter. It is the number of seconds after which the probe times out.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
ingress-gateway.readinessProbe.periodSeconds	This is an optional parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**Integer **Range:**0-65535. **Default Value:** 10
ingress-gateway.readinessProbe.successThreshold	This is an optional parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**Integer **Range:**0-65535. **Default Value:** 1
ingress-gateway.readinessProbe.failureThreshold	This is an optional parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
ingress-gateway.livenessProbe.initialDelaySeconds	This is an optional parameter. It tells the kubelet that it should wait second before performing the first probe.	**DataType:**Integer **Range:**0-65535. **Default Value:** 30
ingress-gateway.livenessProbe.timeoutSeconds	This is an optional parameter. It is the number of seconds after which the probe times out.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.livenessProbe.periodSeconds	This is an optional parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**Integer **Range:**0-65535. **Default Value:** 15
ingress-gateway.livenessProbe.successThreshold	This is an optional parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**Integer **Range:**0-65535. **Default Value:** 1
ingress-gateway.livenessProbe.failureThreshold	This is an optional parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
ingress-gateway.resources.limits.cpu	This is an optional parameter. It limits the number of CPUs to be used by the microservice.	**DataType:**Float **Range:**Valid floating point value between 0 and 1 **Default Value:**
ingress-gateway.resources.limits.initServiceCpu	This is an optional parameter. Init Container CPU Limit.	**DataType:**String **Default Value:**1
ingress-gateway.resources.limits.commonHooksCpu	This is an optional parameter. common Hooks Cpu limit.	**DataType:**String **Range:** **Default Value:** 1
ingress-gateway.resources.limits.memory	This is an optional parameter. It limits the memory utilization by the microservice.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc. **Default Value:**
ingress-gateway.resources.limits.initServiceMemory	This is an optional parameter. Init Container Memory Limit.	**DataType:**String **Range:** **Default Value:** 1Gi
ingress-gateway.resources.limits.commonHooksMemory	This is an optional parameter. common Hook Container Memory Limit.	**DataType:**String **Default Value:** 1Gi
ingress-gateway.resources.requests.cpu	This is an optional parameter. It provides a given number of CPUs for the microservice.	**DataType:**Float **Range:**Valid floating point value between 0 and 1 **Default Value:**
ingress-gateway.resources.requests.initServiceCpu	This is an optional parameter. Init Container CPU Limit.	**DataType:**String **Range:** **Default Value:**0.5
ingress-gateway.resources.requests.commonHooksCpu	This is an optional parameter. Common Hook Container CPU for requests.	**DataType:**String **Default Value:** 0.5
ingress-gateway.resources.requests.memory	This is an optional parameter. It provides a given amount of memory for the microservice.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc.

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.resources.requests.initServiceMemory	This is an optional parameter. Init Container Memory for requests.	**DataType:**String **Range:** **Default Value:** 0.5Gi
ingress-gateway.resources.requests.commonHooksMemory	This is an optional parameter. Common Hook Container Memory for requests.	**DataType:**String **Default Value:**0.5Gi
ingress-gateway.resources.target.averageCpuUtil	This is an optional parameter. It gives the average CPU utilization percentage.	**DataType:**String **Range:**A value in between 0-100 **Default Value:**
ingress-gateway.cipherSuites	Allowed CipherSuites for TLS1.2, if ingressgateway.enableIncomingHttps is true.	**DataType:**List[String] **Range:** TLS_ECDHE_ ECDSA_WIT H_AES_256_ GCM_SHA38 4 TLS_ECDHE_ RSA_WITH_ AES_256_GC M_SHA384 TLS_ECDHE_ RSA_WITH_ CHACHA20_ POLY1305_S HA256 TLS_ECDHE_ ECDSA_WIT H_AES_128_ GCM_SHA25 6 TLS_ECDHE_ RSA_WITH_ AES_128_GC M_SHA256 **Default Value:**
ingress-gateway.initssl	This is an optional parameter. To Initialize SSL related infrastructure in init container.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.httpsEnabled
ingress-gateway.enableIncomingHttp	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.enableIncomingHttp q
ingress-gateway.enableIncomingHttps	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.enableIncomingHttps
ingress-gateway.ingressGwCertReloadEnabled	This is a mandatory parameter. If enabled, then certificates can be updated during run-time without up/restart of the application.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.ingressGwCertReloadEnabled

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
`ingress-gateway.nodeSelector.nodeKey`	This is an optional parameter. node selector key specific to chart (Note: This will be looked first and then, if not present global node key will be picked).	**DataType:**String **Range:** **Default Value:**
`ingress-gateway.nodeSelector.nodeValue`	This is an optional parameter. node selector value specific to chart (Note: This will be looked first and then, if not present global node value will be picked).	**DataType:**String **Range:** **Default Value:**
`ingress-gateway.commonCfgClient.enabled`	This is an optional parameter. If set to true Common Config Client would create tables in cncccommonconfig.	**DataType:**Boolean **Range:**True or False **Default Value:**True
`ingress-gateway.commonCfgServer.port`	This is an optional parameter. It specifies the port number which makes cmservice visible to other services running within the same Kubernetes cluster and the also used by common configuration client for db creation.	**DataType:**Integer **Default Value:** Values will be set by global.cmServiceHttpPort
`ingress-gateway.dbConfig.dbHost`	This is an optional parameter. It the hostname for persistence db. Example: mysql.default.svc.cluster.local	**DataType:**String **Range:**Valid String **Default Value:** Values will be set by global.dbHost
`ingress-gateway.dbConfig.dbPort`	This is an optional parameter. It is the db port for CNC Console Core. Example: 3306	**DataType:**Integer **Range:**0-65535. **Default Value:** Values will be set by global.dbPort
`ingress-gateway.dbConfig.secretName`	This is an optional parameter. It specifies an existing secret to be used for mysql username and password. Example: secretName: &mySqlSecretNameRef cncc-db-secret	**DataType:**String **Range:**Valid String **Default Value:** Values will be set by global.secretName

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
`ingress-gateway.dbConfig.dbName`	This is an optional parameter. • It is the name of the database used for M-CNCC Core, user should create DB with unique name before deploying M-CNCC. Example: – DB Name in case M-CNCC Core mcncccommonconfig.	**DataType:**String **Range:**Valid String **Default Value:** Values will be set by mcncc-core.global.dbName in case of mcncc-core
`ingress-gateway.dbConfig.dbUNameLiteral`	This is an optional parameter. It is the key in the existing secret that stores the password Example: `dbPasswordKey`	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** NA
`ingress-gateway.dbConfig.dbPwdLiteral`	This is an optional parameter. It is the key in the existing secret that stores the username Example: `dbUserNameKey`	**DataType:**String **Range:**VValid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** NA
`ingress-gateway.dbHookImage.name`	This is an optional parameter. Image Name to be used for "ingress-gateway db hook" micro service	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters**Default Value:** cncc/apigw-common-config-hook
`ingress-gateway.dbHookImage.tag`	This is an optional parameter. Image Tag to be used for "ingress-gateway db hook"	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** <Current Version>
`ingress-gateway.dbHookImage.pullPolicy`	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always,Never **Default Value:**IfNotPresent

Table 3-7 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
`ingress-gateway.cncc.securitylogEnabled`	This is an optional parameter. This flag is to enable and disable security logs for CNC Console.	**DataType:**Boolean **Range:**True or False **Default Value:**True
`ingress-gateway.cncc.core.sessionTimeout`	This is a mandatory parameter. It takes the timeout value for CNC Console Session in seconds.	**DataType:**Integer **Range:**300-7200 **Default Value:**1800

3.4 A-CNCC Core Configuration Options

This section includes information about the configuration parameters of A-CNCC Core.

> **Note**
>
> The options mentioned in the following tables can be read as *mcncc-core.<field Name>* or *acncc-core.<field Name>*.
>
> Example: The *global.dbName* can be read as *mcncc-core.global.dbName* or *acncc-core.global.dbName*.

3.4.1 Global Parameters

This section includes information about the global parameters of the A-CNC Core:

Table 3-8 Global Parameters

Parameter	Description	Details
`global.publicHttpSignalingPort`	This is an optional parameter. It is the port on which ingress-gateway service is exposed. If httpsEnabled is false, this Port would be HTTP/2.0 Port (unsecured)publicHttpSignalingPort: 80	**DataType:**Integer **Range:**0-65535. **Default Value:**80
`global.publicHttpsSignallingPort`	This is an optional parameter. It is the port on which Ingress Gateway service is exposed. If httpsEnabled is true, this Port would be HTTPS/2.0 Port (secured SSL)	**DataType:**Integer **Range:**0-65535. **Default Value:**443

Table 3-8 (Cont.) Global Parameters

Parameter	Description	Details
global.staticIpAddressEnabled	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress else random IP will be assigned by the metalLB from its IP Pool.	**DataType:**Boolean **Range:**True or False **Default Value:** False
global.staticIpAddress	This is an optional parameter. If Static load balancer IP needs to be set, then set staticIpAddressEnabled flag to true and provide value for staticIpAddress else random IP will be assigned by the metalLB from its IP Pool.	**DataType:**String **Range:**Valid ASCII aserviceAccountNamend may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:**
global.httpsEnabled	This is an optional parameter. To Initialize SSL related infrastructure in init container.	**DataType:**Boolean **Range:**True or False **Default Value:** False
global.enableIncomingHttp	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** False
global.enableIncomingHttps	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** False
global.needClientAuth	This must be true if client certificate identity is required in the header x-custom-ingress-client-identity. Note: This parameter will be set to true only in case of ACNCC-CORE deployment.	**DataType:**Boolean **Range:**True or False **Default Value:** False
global.ingressGwCertReloadEnabled	This is an optional parameter. If enabled, then certificates can be updated during run-time without up/restart of the application.	**DataType:**Boolean **Range:**True or False **Default Value:** False

3.4.2 Ingress Gateway Parameters

This section includes information about the Ingress Gateway parameters of the A- CNC Console Core.

Table 3-9 Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.extraContainers	This is a mandatory parameter. To enable or disable debug tools container.	**DataType:**enum **Range:**DISABLED, ENABLED, USE_GLOBAL_VALUE **Default Value:** USE_GLOBAL_VALUE
ingress-gateway.prefix	This is a mandatory parameter. Metrics Instance Identifier to uniquely identify CNCC Core metrics.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. An image name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** /grafana
ingress-gateway.image.name	This is a mandatory parameter. It is the image name of the Ingress Gateway as provided by the user.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc/cncc-apigateway
ingress-gateway.image.tag	This is a mandatory parameter. Image Tag to be used for Ingress Gateway.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** <Current Version>
ingress-gateway.image.pullPolicy	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent
ingress-gateway.initContainersImage.name	This is a mandatory parameter. Image Name to be used for "cncc-cmservice" microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc/apigw-configurationinit
ingress-gateway.initContainersImage.tag	This is a mandatory parameter. Image Tag to be used for "cncc-cmservice" microservice.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** <Current Version>
ingress-gateway.initContainersImage.pullPolicy	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always, Never **Default Value:** IfNotPresent

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.service.ssl.tlsVersion	This is an optional parameter. It is the TLS version.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:**TLSv1.2
ingress-gateway.service.ssl.privateKey.k8SecretName	This is an optional parameter. Name of the privatekey secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc-core-ingress-secret
ingress-gateway.service.ssl.privateKey.k8NameSpace	This is an optional parameter. Namespace of privatekey. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
ingress-gateway.service.ssl.privateKey.rsa.fileName	This is an optional parameter. RSA private key file name. Example: rsa_private_key_pkcs1.pem	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** rsa_private_key_pkcs1.pem
ingress-gateway.service.ssl.privateKey.ecdsa.fileName	This is an optional parameter. ECDSA private key file name. Example: ssl_ecdsa_private_key.pem	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_ecdsa_private_key.pem
ingress-gateway.service.ssl.certificate.k8SecretName	This is an optional parameter. Name of the certificate secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:**cncc-core-ingress-secret
ingress-gateway.service.ssl.certificate.k8NameSpace	This is an optional parameter. Namespace of certificate. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.service.ssl.certificate.rsa.fileName	This is an optional parameter. RSA certificate file name. Example: ssl_rsa_certificate.crt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_rsa_certificate.crt
ingress-gateway.service.ssl.certificate.ecdsa.fileName	This is an optional parameter. ECDSA certificate file name. Example: ssl_ecdsa_certificate.crt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_ecdsa_certificate.crt
ingress-gateway.service.ssl.caBundle.k8SecretName	This is an optional parameter. Name of the caBundle secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator **Default Value:** cncc-core-ingress-secret
ingress-gateway.service.ssl.caBundle.k8NameSpace	This is an optional parameter. Namespace of caBundle. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
ingress-gateway.service.ssl.caBundle.fileName	This is an optional parameter. RSA caBundle file name. Example: caroot.cer	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** caroot.cer
ingress-gateway.service.ssl.keyStorePassword.k8SecretName	This is an optional parameter. Name of the keyStorePassword secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc-core-ingress-secret
ingress-gateway.service.ssl.keyStorePassword.k8NameSpace	This is an optional parameter. Namespace of keyStorePassword. Example: cncc	**DataType:**String **Range:**VValid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.service.ssl.keyStorePassword.fileName	This is an optional parameter. File name that has password for keyStore. Example: ssl_keystore.txt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_keystore.txt
ingress-gateway.service.ssl.trustStorePassword.k8SecretName	This is an optional parameter. Name of the trustStorePassword secret. Example: cncc-core-ingress-secret	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc-core-ingress-secret
ingress-gateway.service.ssl.trustStorePassword.k8NameSpace	This is an optional parameter. Namespace of trustStorePassword. Example: cncc	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** cncc
ingress-gateway.service.ssl.trustStorePassword.fileName	This is an optional parameter. File name that has password for trustStore. Example: ssl_truststore.txt	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** ssl_truststore.txt
ingress-gateway.service.ssl.initialAlgorithm	This is an optional parameter. Default values is RSA256.	**DataType:**String **Range:**VValid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A name component may not start or end with a separator. **Default Value:** RS256
ingress-gateway.service.customExtension.labels	This is an optional parameter. This can be used to add custom label(s) to Ingress Gateway service.	**DataType:**String **Range:**Custom Labels that need to be added to ingress gateway specific Service. **Default Value:** NA
ingress-gateway.service.customExtension.annotations	This is an optional parameter. This can be used to add custom annotation(s) to Ingress Gateway service.	**DataType:**String **Range:**VCustom Labels that need to be added to ingress gateway specific Service. **Default Value:** NA
ingress-gateway.deployment.customExtension.labels	This is an optional parameter. This can be used to add custom label(s) to Ingress Gateway deployment.	**DataType:**String **Range:**Custom Labels that need to be added to ingress gateway specific Service. **Default Value:** NA

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.deployment.customExtension.annotations	This is an optional parameter. This can be used to add custom annotation(s) to Ingress Gateway deployment.	**DataType:**String **Range:**Custom Annotations that need to be added to ingress gateway specific Deployment. **Default Value:** NA
ingress-gateway.ports.containerPort	This is an optional parameter. It is the http port of the container for the Ingress Gateway.	**DataType:**Integer **Range:**0-65535 **Default Value:** 8081
ingress-gateway.ports.containersslPort	This is an optional parameter. It is the https port of the container for the Ingress Gateway.	**DataType:**Integer **Range:**0-65535 **Default Value:** 8443
ingress-gateway.ports.actuatorPort	This is an optional parameter. It is the actuator port of the container for the Ingress Gateway.	**DataType:**Integer **Range:**0-65535 **Default Value:** 9090
ingress-gateway.log.level.root	This is an optional parameter. It is the level at which user wants to see the logs. Example: WARN	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
ingress-gateway.log.level.ingress	This is an optional parameter. Log level for ingress logs.	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
ingress-gateway.log.level.cncc.root	This is a mandatory parameter. Log level for CNC Console root logs.	**DataType:**String **Range:** WARN, DEBUG, INFO, TRACE etc. **Default Value:**WARN
ingress-gateway.log.level.cncc.audit	This is a mandatory parameter. Log level for CNC Console audit logs.	**DataType:**String **Range:** WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
ingress-gateway.log.level.cncc.security	This is an optional parameter. Log level for CNC Console security logs.	**DataType:**String **Range:**WARN, DEBUG, INFO, TRACE etc. **Default Value:** INFO
ingress-gateway.readinessProbe.initialDelaySeconds	This is an optional parameter. It tells the kubelet that it should wait second before performing the first probe.	**DataType:**Integer **Range:**0-65535. **Default Value:** 30
ingress-gateway.readinessProbe.timeoutSeconds	This is an optional parameter. It is the number of seconds after which the probe times out.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.readinessProbe.periodSeconds	This is an optional parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**Integer **Range:**0-65535. **Default Value:** 10
ingress-gateway.readinessProbe.successThreshold	This is an optional parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**Integer **Range:**0-65535. **Default Value:** 1
ingress-gateway.readinessProbe.failureThreshold	This is an optional parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
ingress-gateway.livenessProbe.initialDelaySeconds	This is an optional parameter. It tells the kubelet that it should wait second before performing the first probe.	**DataType:**Integer **Range:**0-65535. **Default Value:** 30
ingress-gateway.livenessProbe.timeoutSeconds	This is an optional parameter. It is the number of seconds after which the probe times out.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
ingress-gateway.livenessProbe.periodSeconds	This is an optional parameter. It specifies that the kubelet should perform a liveness probe every xx seconds.	**DataType:**Integer **Range:**0-65535. **Default Value:** 15
ingress-gateway.livenessProbe.successThreshold	This is an optional parameter. Minimum consecutive successes for the probe to be considered successful after having failed.	**DataType:**Integer **Range:**0-65535. **Default Value:** 1
ingress-gateway.livenessProbe.failureThreshold	This is an optional parameter. When a Pod starts and the probe fails, Kubernetes will try failureThreshold times before giving up.	**DataType:**Integer **Range:**0-65535. **Default Value:** 3
ingress-gateway.resources.limits.cpu	This is an optional parameter. It limits the number of CPUs to be used by the microservice.	**DataType:**Float **Range:**Valid floating point value between 0 and 1 **Default Value:**
ingress-gateway.resources.limits.initServiceCpu	This is an optional parameter. Init Container CPU Limit.	**DataType:**String **Default Value:**1
ingress-gateway.resources.limits.commonHooksCpu	This is an optional parameter. common Hooks CPU limit.	**DataType:**String **Range:** **Default Value:** 1

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.resources.limits.memory	This is an optional parameter. It limits the memory utilization by the microservice.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc. **Default Value:**
ingress-gateway.resources.limits.initServiceMemory	This is an optional parameter. Init Container Memory Limit.	**DataType:**String **Range:** **Default Value:** 1Gi
ingress-gateway.resources.limits.commonHooksMemory	This is an optional parameter. common Hook Container Memory Limit.	**DataType:**String **Default Value:** 1Gi
ingress-gateway.resources.requests.cpu	This is an optional parameter. It provides a given number of CPUs for the microservice.	**DataType:**Float **Range:**Valid floating point value between 0 and 1 **Default Value:**
ingress-gateway.resources.requests.initServiceCpu	This is an optional parameter. Init Container CPU Limit.	**DataType:**String **Range:** **Default Value:**0.5
ingress-gateway.resources.requests.commonHooksCpu	This is an optional parameter. Common Hook Container CPU for requests.	**DataType:**String **Default Value:** 0.5
ingress-gateway.resources.requests.memory	This is an optional parameter. It provides a given amount of memory for the microservice.	**DataType:**String **Range:**Valid Integer value followed by Mi/Gi etc.
ingress-gateway.resources.requests.initServiceMemory	This is an optional parameter. Init Container Memory for requests.	**DataType:**String **Range:** **Default Value:** 0.5Gi
ingress-gateway.resources.requests.commonHooksMemory	This is an optional parameter. Common Hook Container Memory for requests.	**DataType:**String **Default Value:**0.5Gi
ingress-gateway.resources.target.averageCpuUtil	This is an optional parameter. It gives the average CPU utilization percentage.	**DataType:**String **Range:**A value in between 0-100 **Default Value:**
ingress-gateway.cipherSuites	Allowed CipherSuites for TLS1.2, if ingressgateway.enableIncomingHttps is true.	**DataType:**List[String] **Range:** TLS_ECDHE_ ECDSA_WIT H_AES_256_ GCM_SHA38 4 TLS_ECDHE_ RSA_WITH_ AES_256_GC M_SHA384 TLS_ECDHE_ RSA_WITH_ CHACHA20_ POLY1305_S HA256 TLS_ECDHE_ ECDSA_WIT H_AES_128_ GCM_SHA25 6 TLS_ECDHE_ RSA_WITH_ AES_128_GC M_SHA256 **Default Value:**

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.initssl	This is an optional parameter. To Initialize SSL related infrastructure in init container.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.httpsEnabled acncc-core.global.httpsEnabled
ingress-gateway.enableIncomingHttp	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.enableIncomingHttp acncc-core.global.enableIncomingHttp q
ingress-gateway.enableIncomingHttps	This is an optional parameter. Server Configuration for http and https support.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.enableIncomingHttps acncc-core.global.enableIncomingHttps
ingress-gateway.needClientAuth	This is an optional parameter. This must be true if client certificate identity is required in the header x-custom-ingress-client-identity. **Note**: This parameter will be set to true only in case of ACNCC-Core deployment.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by acncc-core.global.needClientAuth
ingress-gateway.ingressGwCertReloadEnabled	This is a mandatory parameter. If enabled, then certificates can be updated during run-time without up/restart of the application.	**DataType:**Boolean **Range:**True or False **Default Value:** Values will be set by mcncc-core.global.ingressGwCertReloadEnabled acncc-core.global.ingressGwCertReloadEnabled
ingress-gateway.nodeSelector.nodeKey	This is an optional parameter. node selector key specific to chart (Note: This will be looked first and then, if not present global node key will be picked).	**DataType:**String **Range:** **Default Value:**
ingress-gateway.nodeSelector.nodeValue	This is an optional parameter. node selector value specific to chart (Note: This will be looked first and then, if not present global node value will be picked).	**DataType:**String **Range:** **Default Value:**

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
ingress-gateway.commonCfgClient.enabled	This is an optional parameter. If set to true Common Config Client would create tables in cncccommonconfig.	**DataType:**Boolean **Range:**True or False **Default Value:**True
ingress-gateway.commonCfgServer.port	This is an optional parameter. It specifies the port number which makes cmservice visible to other services running within the same Kubernetes cluster and the also used by common config client for db creation.	**DataType:**Integer **Default Value:** Values will be set by global.cmServiceHttpPort
ingress-gateway.dbConfig.dbHost	This is an optional parameter. It the hostname for persistence db. Example: mysql.default.svc.cluster.local	**DataType:**String **Range:**Valid String **Default Value:** Values will be set by global.dbHost
ingress-gateway.dbConfig.dbPort	This is an optional parameter. It is the db port for cncc-core. Example: 3306	**DataType:**Integer **Range:**0-65535. **Default Value:** Values will be set by global.dbPort
ingress-gateway.dbConfig.secretName	This is an optional parameter. It specifies an existing secret to be used for mysql username and password. Example: secretName: &mySqlSecretNameRef cncc-db-secret	**DataType:**String **Range:**Valid String **Default Value:** Values will be set by global.secretName
ingress-gateway.dbConfig.dbName	This is an optional parameter. • It is the name of the database used for M-CNCC OR A-CNCC Core, user should create DB with unique name before deploying M-CNCC OR A-CNCC Core. Example: – DB Name in case M-CNCC Core mcncccommonconfig. – DB Name in case A-CNCC Core acncccommonconfig.	**DataType:**String **Range:**Valid String **Default Value:** Values will be set by mcncc-core.global.dbName in case of mcncc-core acncc-core.global.dbName in case of acncc-core

Table 3-9 (Cont.) Ingress Gateway Parameters

Attribute Name	Description	Details
`ingress-gateway.dbConfig.dbUNameLiteral`	This is an optional parameter. It is the key in the existing secret that stores the password. Example: `dbPasswordKey`	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** NA
`ingress-gateway.dbConfig.dbPwdLiteral`	This is an optional parameter. It is the key in the existing secret that stores the username. Example: `dbUserNameKey`	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. It may not start with a period or a dash and may contain a maximum of 128 characters **Default Value:** NA
`ingress-gateway.dbHookImage.name`	This is an optional parameter. Image Name to be used for "ingress-gateway db hook" micro service.	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period or a dash and may contain a maximum of 128 characters**Default Value:** cncc/apigw-common-config-hook
`ingress-gateway.dbHookImage.tag`	This is an optional parameter. Image Tag to be used for "ingress-gateway db hook".	**DataType:**String **Range:**Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. A tag name may not start with a period, or a dash and may contain a maximum of 128 characters **Default Value:** <Current Version>
`ingress-gateway.dbHookImage.pullPolicy`	This is an optional parameter. Pull Policy decides from where to pull the image.	**DataType:**String **Range:**IfNotPresent, Always,Never **Default Value:**IfNotPresent
`ingress-gateway.cncc.securitylogEnabled`	This is an optional parameter. This flag is to enable and disable security logs for CNC Console.	**DataType:**Boolean **Range:**True or False **Default Value:**True
`ingress-gateway.cncc.core.sessionTimeout`	This is a mandatory parameter. It takes the timeout value for CNC Console session in seconds.	**DataType:**Integer **Range:**300-7200 **Default Value:**1800

3.5 CNC Console Instances Configurations

This section explains about the CNC Console instances configurations.

> **Note**
>
> - Instance id must be globally unique as it will be used for routing, recommendation for *id name <owner>-<instance name>*.
> - Type values are case sensitive, supported type values are POLICY, NRF, SCP, NSSF, SEPP,UDR-PROV, UDR-CONFIG, BSF, CS, DD-UI, DD-API, PROVGW, NWDAF, DBTIER, OCCM.
> - apiPrefix is must for type CS (OCCNE Common Services), DD (DD-UI and DD-API), NWDAF (NWDAF-UI and NWDAF-API). This is not applicable for OCI deployment.
> - Supported common services are grafana, kibana, jaeger, prometheus, alertmanager, promxy, opensearch, and jaeger-es. This is not applicable for OCI deployment.
> - M-CNCC can only communicate to its own M-CNCC IAM on the same cluster.
> - Agent only deployment (A-CNCC) can communicate with multiple M-CNCC IAMs.

CNC Console Supported OCCNE Common Services/NFs with expected apiPrefix format.

Table 3-10 CNC Console Supported OCCNE Common Services/NFs with expected apiPrefix format

Common Service	apiPrefix format	Example
Grafana	/$OCCNE_CLUSTER/grafana	/mycne-cluster/grafana
Kibana	/$OCCNE_CLUSTER/kibana	/mycne-cluster/kibana
Jaeger	/$OCCNE_CLUSTER/jaeger	/mycne-cluster/jaeger
Prometheus	/$OCCNE_CLUSTER/prometheus	/mycne-cluster/prometheus
Alertmanager	/$OCCNE_CLUSTER/ alertmanager	/mycne-cluster/alertmanager
Promxy	/$OCCNE_CLUSTER/promxy	/mycne-cluster/promxy
OpenSearch	/$OCCNE_CLUSTER/dashboard	/mycne-cluster/dashboard
Jaeger-ES	/$OCCNE_CLUSTER/esjaeger	/mycne-cluster/esjaeger
Data Director (DD-UI)	/$OCCNE_CLUSTER/ocnadd	/mycne-cluster/ocnadd
Data Director (DD-API)	/$OCCNE_CLUSTER/ocnaddapi	/mycne-cluster/ocnaddapi
Network Data Analytics Function (NWDAF-UI)	/$OCCNE_CLUSTER/ocnwdaf	/mycne-cluster/ocnwdaf
Network Data Analytics Function (NWDAF-API)	/$OCCNE_CLUSTER/ocnwdafapi	/mycne-cluster/ocnwdafapi

CNC Console supports common services, Data Director, and Network Data Analytics Function NF only if its api prefix is globally unique like defined in above table.

For the CNCC Core Instances Configuration examples of all supported NFs, see CNC Console Instances Configuration ExamplesCNC Console Instances Configuration Examples in appendix.

3.5.1 CNC Console Instances Configuration Options

This section describes the parameters that are configured in the CNC Console Instances configuration section in custom values.yaml file.

Attribute Name	SubType	Description	Details
global.self.cnccId	NA	This is a mandatory parameter. ID to uniquely identify the deployment. Its also called as owner or site name. Ex: cnccId: Cluster1	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. Id may not start with a period or a dash and may contain a maximum of 40 characters
global.mCnccIams.[]	id	This is a mandatory parameter. ID to uniquely identify the M-CNCC IAM or OCI IAM.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. Id may not start with a period or a dash and may contain a maximum of 40 characters

	fqdn	This is a mandatory parameter (if ip is not provided).
		M-CNCC IAM URI FQDN
		Note: To retrieve the OCI IAM Domain URL, see Accessing OCI IAM. For example:
		
		`self:`
		`  cnccId: Cluster1`
		`mCnccIams:`
		`  - id: Cluster1`
		`  fqdn: idcs-2e0d8xxxxdd43.identity.oraclecloud.com`
		`  scheme: https`
		`mCnccCores:`
		`  ...`
		`  ...`
			DataType: String

Attribute Name	SubType	Description	Details

	ip	This is a mandatory parameter (if ip is not provided).
		M-CNCC IAM URI IP.
		Note:CNC Console supports configuration through IPv4 and IPv6 family IPs.
		IPv6 Sample configuration:
		`mCnccIams:`
		`- id: Cluster1`
		`ip: "[1000:xxxx:xxxx:xxx::yy]"`
		IPv4 Sample Configuration:
		`mCnccIams:`
		`- id: Cluster1`
		`ip: 10.xx.xx.xx`
			DataType: String

	port	This is an optional parameter. M-CNCC IAM or OCI IAM URI port. **Note:** The mCnccIams.port configuration must be added only if port is other than default ones **80** or **443**.	**DataType:** String **Range:** It can take value in the range: 0-65535 Default value is 80
	scheme	This is an optional parameter. M-CNCC IAM or ICI IAM URI scheme.	**DataType:** String **Range:** It can take either http or https value. By default, it is http.
global.mCnccCores.[]	id	This is a mandatory parameter (for M-CNCC Deployment). ID to uniquely identify the M-CNCC Core. Usually its value will be same as global.mCnccIams.id value.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. Id may not start with a period or a dash and may contain a maximum of 40 characters
	fqdn	This is a mandatory parameter (if ip is not provided). M-CNCC Core URI FQDN.	**DataType:** String
	ip	This is a mandatory parameter (if fqdn is not provided). M-CNCC Core URI IP.	**DataType:** String

Attribute Name	SubType	Description	Details
	port	This is an optional parameter. M-CNCC Core URI Port.	**DataType:** String **Range:** It can take value in the range: 0-65535 Default value is 80
	scheme	This is an optional parameter. M-CNCC Core URI scheme.	**DataType:** String **Range:** It can take either http or https value. By default, it is http.
	role	This is an optional parameter. It is an option to override M-CNCC site role. By default role value will be set as id value.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. Id may not start with a period or a dash and may contain a maximum of 40 characters
global.aCnccs.[]	id	This is a mandatory parameter. ID to uniquely identify the A-CNCC.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. Id may not start with a period or a dash and may contain a maximum of 40 characters
	fqdn	This is a mandatory parameter (if ip is not provided). A-CNCC URI FQDN.	**DataType:** String
	ip	This is a mandatory parameter (if fqdn is not provided). A-CNCC URI IP.	**DataType:** String
	port	This is an optional parameter. A-CNCC URI Port.	**DataType:** String **Range:** It can take value in the range: 0-65535 Default value is 80
	scheme	This is an optional parameter. A-CNCC URI scheme.	**DataType:** String **Range:** It can take either http or https value. By default, it is http.

Attribute Name	SubType	Description	Details
	role	This is an optional parameter. It is an option to override A-CNCC site role. By default role value will be set as id value.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. Id may not start with a period or a dash and may contain a maximum of 40 characters
global.instances.[]	id	This is a mandatory parameter. ID to uniquely identify the NF Instance or OCCNE Common Service Instance.	**DataType:** String **Range:** Valid ASCII and may contain lowercase and uppercase letters, digits, underscores, periods, and dashes. Id may not start with a period or a dash and may contain a maximum of 80 characters
	type	This is a mandatory parameter. Type values are case sensitive, supported type values are BSF, NEF, NRF, NSSF, POLICY, SCP, SEPP, UDR-CONFIG, UDR-PROV, CS, DD-UI, DD-API, PROVGW, NWDAF-UI, NWDAF-API, DBTIER, OCCM.	**DataType:** String **Range:**It can take one of these values: BSF, NEF, NRF, NSSF, POLICY, SCP, SEPP, UDR-CONFIG, UDR-PROV, CS, DD-UI, DD-API, PROVGW, NWDAF-UI, NWDAF-API, DBTIER, OCCM.
	fqdn	This is a mandatory parameter (if ip is not provided). FQDN of NF Instance or OC-CNE Common Service Instance.	**DataType:** String
	ip	This is a mandatory parameter (if fqdn is not provided). IP of NF Instance or OCCNE Common Service Instance.	**DataType:** String
	port	This is an optional parameter. Port of NF Instance or OCCNE Common Service Instance.	**DataType:** String **Range:** It can take value in the range: 0-65535 Default value is 80
	scheme	This is an optional parameter. Scheme of NF Instance or OC-CNE Common Service Instance.	**DataType:** String **Range:** It can take either http or https value. By default, it is http.
	owner	This is a mandatory parameter. Owner of NF Instance or OC-CNE Common Service Instance.	**DataType:** String **Range:** It takes the name of deployment that owns the Instance

Attribute Name	SubType	Description	Details
	apiPrefix	This is an optional parameter. ApiPrefix used for routing OCCNE Common Services, Data Data Director, and NWDAF and used for routing OCCNE Common Services, Data Director, and NWDAF instances. Note: ApiPrefix is not required in case of NF instances (except DD and NWDAF) Example : /<Cluster Prefix>/grafana	**DataType:** String

4
Accessing CNC Console

This section explains about the different ways to access CNC Console.

4.1 Accessing M-CNCC IAM

> **Note**
>
> Not applicable for OCI deployment.

This section explains about the different ways to access M-CNC Console IAM. The user can select any of the following methods:

Format:

```
<scheme>://<cncc-iam-ingress IP/FQDN>:<cncc-iam-ingress Port>
```

1. Node-IP and NodePort
   Example:

   ```
   http://10.75.xx.xx:30085/
   ```

2. DNS Resolvable FQDN and NodePort
   Example:

   ```
   http://cncc-iam-ingress-gateway.cncc.svc.cluster.local:30085/
   ```

3. External LB-IP and ServicePort
   Example:

   ```
   http://10.xx.xx.xx:8080/
   ```

4. DNS Resolvable FQDN and ServicePort
   Example:

   ```
   http://cncc-iam-ingress-gateway.cncc.svc.cluster.local:8080/
   ```

4.2 Accessing M-CNCC Core

This section explains about the different ways to access M-CNCC Core. The user can select any of the following methods:

Format:

```
<scheme>://<cncc-mcore-ingress IP/FQDN>:<cncc-mcore-ingress Port>
```

1. Node-IP and NodePort

   Example:

   ```
   http://10.75.xx.xx:30075/
   ```

2. DNS Resolvable FQDN and NodePort

   Example:

   ```
   http://cncc-mcore-ingress-gateway.cncc.svc.cluster.local:30075/
   ```

3. External LB-IP and ServicePort

   Example:

   ```
   http://10.75.xx.xx:8080/
   ```

4. DNS Resolvable FQDN and ServicePort
5. Example:

   ```
   http://cncc-mcore-ingress-gateway.cncc.svc.cluster.local:8080/
   ```

> **Note**
>
> Login to CNC IAM and add redirect url pointing to M-CNCC Core. CNCC cannot be accessed before CNCC IAM is configured to redirect. For more information, see CNC Console IAM Postinstallation Steps section.

> **Note**
>
> NFs or Common Services(CS) deployed with A-CNCC Core should be accessed through M-CNCC Core, direct access is restricted.

4.3 Accessing OCI IAM

4.3.1 OCI IAM with Identity Domain

For information on OCI IAM with Identity Domain, see the IAM with Identity Domains section in Oracle Cloud Infrastructure Documentation.

4.3.2 Access OCI IAM

Access OCI IAM

To access OCI IAM:

1. Sign in to the Oracle Cloud Console.
2. In the navigation menu, click **Identity & Security**. Under **Identity**, check for **Domains**. If you see **Domains**, Select the identity domain that you want to work in.

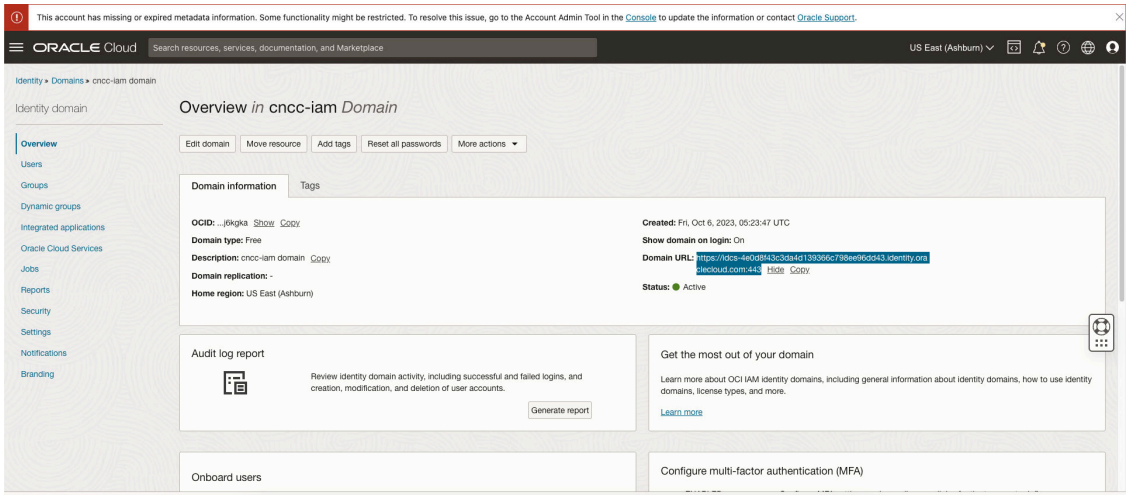
4.3.3 OCI IAM Domain URL

OCI IAM Domain URL

To access OCI IAM domain URL:

1. Sign in to the Oracle Cloud Console.
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**. Select the identity domain that you want to work in.
3. On the **Domain information** tab, one ca view or copy the **Domain URL**.

Figure 4-1 OCI IAM Domain URL



4.3.4 OCI IAM ClientId and ClientSecret

OCI IAMClientId and ClientSecret

To access OCI IAM ClientId and ClientSecret:

1. Log in to OCI Console.
2. Open the navigation menu and click **Identity & Security**. Under **Identity**, click **Domains**.
3. Click the name of the identity domain that you want to work in. You might need to change the compartment to find the domain that you want. Then, click **Integrated applications**.

4. Click the Confidential Application that you created in Create a Confidential Application Under OCI IAM.
5. In the **General information** section, you'll observe the display of the **Client ID** and **Client Secret** details. Record the **Client ID** and **Client secret**. To integrate CNC Console with this confidential application, use this ID and secret as part of the connection settings. The **Client ID** and **Client secret** are equivalent to a credential (for example, an ID and password) that CNC Console application uses to communicate with OCI IAM.

> **Note**
>
> This is required to create secrets as part of Configuring OCI IAM Secret while installing CNC Console.

5
Upgrading CNC Console

This section provides details of CNC Console upgrade procedure to upgrade the following CNC Console components:

- M-CNCC IAM
- M-CNCC Core
- A-CNCC Core

> **Note**
>
> **For OCI**
> The CNC Console IAM DB Backup is not applicable.
>
> The M-CNCC IAM component is not applicable in OCI deployment.

> **Note**
>
> Before proceeding with CNC Console helm upgrade to latest, CNC Console database backup must be taken and stored in a location which can be easily restored. For more information, see CNC Console IAM DB Backup .

The following steps must be followed while performing the upgrade:

1. CNCC IAM DB Backup
2. CNCC Upgrade

This section explains about the CNC Console upgrade procedures for single cluster and multicluster deployments. M-CNCC IAM, M-CNCC Core, and A-CNCC Core can be upgraded from current version to the latest version using helm upgrade feature.

User can upgrade and rollback CNC Console from a source release to a target release using CDCS or CLI procedures as outlined in the following table:

		Non OCI Environment		OCI Environment
Upgrade	**References**	**Applicable for CDCS**	**Applicable for CLI**	**Applicable for CNC Console deployment using OCI**
M- CNCC IAM DB Backup	CNCC IAM DB Backup	Yes	Yes	No
CNC Console Upgrade	CNCC Upgrade	See Oracle Communications CD Control Server Installation and Upgrade Guide	Yes	Yes

> **⚠ Caution**
>
> It is recommended to verify the copy pasted content especially when the hyphens or any special characters are part of copied content.

5.1 Supported Upgrade Paths

This section describes the supported upgrade paths for CNC Console

For more information about supported upgrade paths, see CNC Console Deployment Modes section.

The following table lists the supported upgrade paths for Console:

Table 5-1 CNC Console Upgrade Sequence

Deployment Mode	Source Version	Target Version	Upgrade Sequence
Single Cluster	23.3.x or 23.4.x	24.1.x	**Console Upgrade** Upgrade CNC Console **NF Upgrade** Upgrade Instances (NF or CNE/OSO Common Services) **cnDbtier Upgrade**
Multi Cluster	23.3.x or 23.4.x	24.1.x	**Console Manager Upgrade** Upgrade CNC Console **Console Agent Upgrade** Upgrade A-CNCC Core **NF Upgrade** Upgrade Instances (NF or CNE/OSO Common Services) **cnDbtier Upgrade**

> **ⓘ Note**
>
> **For OCI**
>
> - Starting from version 24.1.0, CNC Console now supports deployment on OCI.
> - CNC Console multicluser feature is not supported.

> **ⓘ Note**
>
> - Console should be upgraded first followed by NF for all the supported NFs.
> - cnDBTier only supports APIs from 23.3.x onwards. Users with a combination of cnDBTier 23.3.x or older, and NF version 23.4.x or newer won't have access to the data in cnDBTier configuration items.

> **Note**
>
> CNC Console supports N-2 NF versions during upgrade window. For example, CNC Console 24.1.x supports SCP 24.1.x, 23.4.x, and 23.3.x. Any newly added features in Console which have NF dependency in latest release may not be available in previous release.

5.2 Preupgrade Tasks

While upgrading an existing CNC Console deployment, the running set of containers and pods are replaced with the new set of containers and pods. However, if there is no change in the pod configuration, the running set of containers and pods are not replaced.

> **Caution**
>
> - No configuration should be performed during upgrade.
> - Do not exit from helm upgrade command manually. After running the helm upgrade command, it takes some time (depending upon number of Pods to upgrade) to upgrade all the services. In the meantime, you must not press "ctrl+c" to come out from helm upgrade command. It may lead to anomalous behavior.

Preupgrade Steps

1. Keep current *occncc_custom_values_<version>.yaml* file as backup, that is

   ```
   occncc_custom_values_<version to be upgraded>.yaml
   ```

2. Update the new custom_values.yaml defined for target CNC Console release. See CNC Console IAM Configuration Parameters section and CNC Console Core Configuration Parameters section for more details about helm configurable parameters.
3. Install or upgrade the network policies, if applicable. For more information, see Configuring Network Policies.

5.3 CNC Console IAM DB Backup

This section describes the procedure to do the DB backup of CNC Console IAM.

> **Note**
>
> Not applicable for OCI deployment.

Prerequisites

The prerequisites for the backup process are:

- MySQL NDB cluster should be in a healthy state.
- Every database node of the MySQL NDB cluster should be in running state.

- In case of cnDBTier to verify the prerequisites, check mysql pod is up and running.
- In case of VM based DB Tier to verify the prerequisites, log in to MCM client on one of the SQL node of the cluster. Run the following command to check the node status:

  ```
  mcm> show status -r occnendbclustera;
  ```

- Log in to the SQL node and run the following command to take the dump (backup) of the database. The user is required to enter the password.

  ```
  kubectl exec -i -n <namespace> <sql-node> -- mysqldump --single-
  transaction --no-tablespaces --no-create-info -h 127.0.0.1 -u <username> -
  p <database-name> | gzip > <backup_filename>.sql.gz
  ```

  For example:

  ```
  kubectl exec -i -n occne-ndb ndbappmysqld-0 -- mysqldump --single-
  transaction --no-tablespaces --no-create-info
        -h 127.0.0.1 -u cnccusr -p cnccdb | gzip > cnccdbBackup.sql.gz
  ```

> **Note**
>
> The operator must ensure there is enough space on the current directory in order to save the backup file.

5.4 CNC Console Upgrade

This section describes the procedure to upgrade CNC Console.

> **Note**
>
> - Existing release name must be used for upgrade.
> - mCncclams port is assumed as 80. The mCncclams port configuration must be added only if port is other than 80.

1. Prepare *occncc_custom_values_<version>.yaml* file for upgrade.
2. Upgrade CNC Console using existing release release name (cncc-iam or cncc) by running the following command:

   ```
   $ helm upgrade <cncc_iam_release_name> <helm_chart> -f
   <occncc_custom_values_<version>.yaml> -n <namespace>
   ```

   Foe example:

   ```
   $ helm upgrade cncc ocspf-helm-repo/cncc -f
   occncc_custom_values_<version>.yaml -n cncc
   ```

3. Check the status of upgrade by running the following command:

   ```
   $ helm status <cncc_iam_release_name> -n <namespace>
   ```

   For example:

   ```
   $ helm status cncc -n cncc
   ```

5.5 Post Upgrade Tasks

This section describes the tasks to be performed after an upgrade.

5.6 Parameters and Definitions During CNC Console Upgrade

Parameters and Definitions during CNC Console Upgrade

Table 5-2 Parameters and Definitions during CNC Console Upgrade

Parameters	Definitions
<release_name>	CNC Console Helm release deployed. It could be found in the output of 'helm list' command
<namespacename>	CNC Console namespace in which release deployed
<helm_chart>	CNC Console helm chart
<chart_version>	CNC Console helm chart version in case helm charts are referred from helm repo
<helm_repo>	CNC Console helm repo
<occncc_custom_values_<version>.yaml>	CNC Console customized values.yaml for target release.
<occncc_rollback_iam_schema_<version>.sql>	CNC Console DB schema file used for rollback

6
Rolling Back CNC Console

This section provides information about rolling back Cloud Native Configuration Console deployment to the previous release.

- M-CNCC IAM
- M-CNCC Core
- A-CNCC Core

The following steps must be followed while performing the rollback:

1. CNCC IAM DB Rollback/Restore
2. CNCC Rollback

> **⚠ Caution**
>
> It is recommended to verify the copy pasted content especially when the hyphens or any special characters are part of copied content.

User can rollback CNC Console from a source release to a target release using CDCS or CLI procedures as outlined in the following table:

Rollback Task	References	Non OCI Environment		OCI Environment
		Applicable for CDCS	Applicable for CLI	Applicable for CNC Console deployment using OCI
M- CNCC IAM DB Rollback or Restore	CNCC IAM DB Rollback or Restore	Yes	Yes	No
CNC Console Rollback	CNCC Rollback	See Oracle Communications CD Control Server Installation and Upgrade Guide	Yes	Yes

> **ⓘ Note**
>
> **For OCI:**
> The CNCC IAM DB Rollback/Restore is not applicable.

6.1 Supported Rollback Paths

This section describes the supported upgrade paths for CNC Console

Table 6-1 CNC Console Rollback Sequence

Deployment Mode	Source Version	Target Version	Rollback Sequence
Single Cluster	24.1.x	23.3.x or 23.4.x	• **cnDbtier Rollback** • **NF Rollback** Rollback Instances (NF or CNE/OSO Common Services) • **Console Rollback** Rollback CNC Console
Multi Cluster	24.1.x	23.3.x or 23.4.x	• **cnDbtier Rollback** • **NF Rollback** Rollback Instances (NF or CNE/OSO Common Services) • **Console Agent Rollback** Rollback A-CNCC Core • **Console Manager Rollback** Rollback CNC Console

> **Note**
>
> **For OCI:**
>
> - Starting from version 24.1.0, the CNC Console now supports deployment on OCI.
> - CNC Console multicluster feature is not supported.

6.2 Pre-rollback Tasks

This section describes the tasks to be performed before a rollback.

6.2.1 M-CNCC IAM DB Rollback or Restore

This section provides details of CNC Console IAM Rollback. In case of CNC Console IAM Upgrade failure, rollback CNC Console IAM DB to previous version by following the below steps.

> **Note**
>
> Not applicable for OCI deployment.

> **Note**
>
> The latest backup must be used for rollback.

To perform a CNC Console IAM DB rollback or Restore:

1. Log in to the deployment cluster, drop the existing database, and create a new database. Restore the new database with the DB Schema file provided as part of package (*<occncc_rollback_iam_schema_<version>.sql>*):
   Run the following command to drop the Database and create a new database:

   ```
   DROP DATABASE <CNCC Database>
   CREATE DATABASE IF NOT EXISTS <CNCC Database>;
   ```

   For example:

   ```
   To be run in the mysql pod:
   DROP DATABASE cnccdb;
   CREATE DATABASE IF NOT EXISTS cnccdb;
   ```

   > **Note**
   >
   > You must take the `<occncc_rollback_iam_schema_<version>.sql>` file from the CNC Console version to which you are performing the rollback. For example, if you are performing rollback from version n to version n-2, you must use the `<occncc_rollback_iam_schema_<version>.sql>` file given in the CNC Console package of version n-2.

2. Copy the DB Schema file provided as part of package into the MYSQl pod (occncc_rollback_iam_schema_<version>.sql).
   Before copying the file into MYSQL pod replace string "InnoDB" with "ndbcluster" using following command:

   ```
   sed -i 's/InnoDB/ndbcluster/g' occncc_rollback_iam_schema_<version>.sql
   ```

   For example:

   ```
   sed -i 's/InnoDB/ndbcluster/g' occncc_rollback_iam_schema_23.4.0.sql
   ```

   Run the following command to copy the DB Schema file:

   ```
   kubectl cp <occncc_rollback_iam_schema.sql> <namespace>/<pod-
   name>:<directory where you want your file placed>
   ```

   For example:

   ```
   kubectl cp occncc_rollback_iam_schema_<version>.sql cndbtier1/
   ndbappmysqld-0:/home/mysql
   ```

3. Run the following command to connect to the SQL node of the NDB cluster or connect to the cnDbBTier:

   ```
   $ kubectl -n <cndbtier_namespace> exec -it <cndbtier_sql_pod_name> -c
   <cndbtier_sql_container_name> -- bash
   ```

For example:

```
$ kubectl -n cndbtier  exec -it ndbappmysqld-0 -c mysqlndbcluster -- bash
```

4. Restore this new database with the DB Schema file provided as part of package (occncc_rollback_iam_schema_<version>.sql).
   Run the following command to Restore DB Schema:

   ```
   mysql -h 127.0.0.1 -u root -p <DB name> < <DB Schema file name>
   ```

   For example:

   ```
   mysql -h 127.0.0.1 -u root -p cnccdb
   <occncc_rollback_iam_schema_<version>.sql
   ```

5. The DB dump has to be rearranged sequentially not to get any foreign key constraints issue. For that, create the ENV variable,s and run it in a loop.

   a. Run the following command to convert the mysqldump file which was taken as a backup (sql.gz file) to a sql file to rearrange it:
      Unzipping the gz file:

      ```
      gunzip -d <<backup_filename>.sql.gz>
      ```

      For example:

      ```
      gunzip -d cnccdbBackup.sql.gz
      ```

   b. Rearrange the backup sql file in correct order by using following procedure:

      i. Run the following command to rearrange the Table Data :

      ```
      export KC_TABLES="ADMIN_EVENT_ENTITY RESOURCE_SERVER
      RESOURCE_SERVER_POLICY
                ASSOCIATED_POLICY REALM CLIENT AUTHENTICATION_FLOW
      AUTHENTICATION_EXECUTION
                AUTHENTICATOR_CONFIG AUTHENTICATOR_CONFIG_ENTRY
      BROKER_LINK CLIENT_ATTRIBUTES
                CLIENT_AUTH_FLOW_BINDINGS KEYCLOAK_ROLE
      CLIENT_INITIAL_ACCESS CLIENT_NODE_REGISTRATIONS
                CLIENT_SCOPE CLIENT_SCOPE_ATTRIBUTES CLIENT_SCOPE_CLIENT
      CLIENT_SCOPE_ROLE_MAPPING
                USER_SESSION CLIENT_SESSION CLIENT_SESSION_AUTH_STATUS
      CLIENT_SESSION_NOTE
                CLIENT_SESSION_PROT_MAPPER CLIENT_SESSION_ROLE
      CLIENT_USER_SESSION_NOTE COMPONENT
                COMPONENT_CONFIG COMPOSITE_ROLE DATABASECHANGELOG
      USER_ENTITY CREDENTIAL
                DATABASECHANGELOGLOCK DEFAULT_CLIENT_SCOPE EVENT_ENTITY
      FEDERATED_IDENTITY FEDERATED_USER
                FED_USER_ATTRIBUTE FED_USER_CONSENT
      FED_USER_CONSENT_CL_SCOPE FED_USER_CREDENTIAL
                FED_USER_GROUP_MEMBERSHIP FED_USER_REQUIRED_ACTION
      FED_USER_ROLE_MAPPING KEYCLOAK_GROUP
                GROUP_ATTRIBUTE GROUP_ROLE_MAPPING IDENTITY_PROVIDER
      ```

```
IDENTITY_PROVIDER_CONFIG
          IDENTITY_PROVIDER_MAPPER IDP_MAPPER_CONFIG
MIGRATION_MODEL OFFLINE_CLIENT_SESSION
          OFFLINE_USER_SESSION POLICY_CONFIG PROTOCOL_MAPPER
PROTOCOL_MAPPER_CONFIG REALM_ATTRIBUTE
          REALM_DEFAULT_GROUPS REALM_LOCALIZATIONS
REALM_ENABLED_EVENT_TYPES REALM_EVENTS_LISTENERS
          REALM_REQUIRED_CREDENTIAL REALM_SMTP_CONFIG
REALM_SUPPORTED_LOCALES REDIRECT_URIS
          REQUIRED_ACTION_CONFIG REQUIRED_ACTION_PROVIDER
RESOURCE_SERVER_RESOURCE
          RESOURCE_ATTRIBUTE RESOURCE_POLICY RESOURCE_SERVER_SCOPE
RESOURCE_SCOPE
          RESOURCE_SERVER_PERM_TICKET RESOURCE_URIS ROLE_ATTRIBUTE
SCOPE_MAPPING SCOPE_POLICY
          USERNAME_LOGIN_FAILURE USER_ATTRIBUTE USER_CONSENT
USER_CONSENT_CLIENT_SCOPE
          USER_FEDERATION_PROVIDER USER_FEDERATION_CONFIG
USER_FEDERATION_MAPPER
          USER_FEDERATION_MAPPER_CONFIG USER_GROUP_MEMBERSHIP
USER_REQUIRED_ACTION USER_ROLE_MAPPING
          USER_SESSION_NOTE WEB_ORIGINS";
```

ii. Run the following command to create an ENV pointing to the sql file to be filtered:

```
export KC_BACKUP="./<Backup SQL Dump File>";
```

For example:

```
export KC_BACKUP="./cnccdbBackup.sql";
```

iii. Run the following command to rearrange the dump file to make it in sequential insertion order:

```
for i in $KC_TABLES; do grep "INSERT INTO \`$i\`"$KC_BACKUP; done >
<file name>
```

Example:

```
for i in $KC_TABLES; do grep "INSERT INTO \`$i\`"$KC_BACKUP; done
> /tmp/restore.sql
```

6. Run the following command to copy file into the pod:

```
kubectl cp <backup_file name>.sql <namespace>/<pod-name>:<directory where
you want your file placed>
```

For example:

```
kubectl cp restore.sql cndbtier1/ndbappmysqld-0:/home/mysql
```

7. Run the following command to connect to the SQL node of the NDB cluster or connect to the cnDBTier:

   ```
   $ kubectl -n <cndbtier_namespace> exec -it <cndbtier_sql_pod_name> -c
   <cndbtier_sql_container_name>-- bash
   ```

   For example:

   ```
   $ kubectl -n cndbtier  exec -it ndbappmysqld-0 -c mysqlndbcluster -- bash
   ```

8. Populate the Database with data using the file that you have, after filtering the sqldump file.
9. Run the following command to restore Database Data:

   ```
   mysql -h 127.0.0.1 -u root -p <DB name> < <backup_filename>
   ```

   For example:

   ```
   mysql -h 127.0.0.1 -u root -p cnccdb < restore.sql
   ```

10. Log in to the MySQL prompt and confirm that the databases are restored.
11. Run the following command to Delete the sql files copied into the pod after the restore process is complete and successful (by logging into the SQL node):

    ```
    rm -rf <DB Schema file name>
    rm -rf <backup_filename>
    ```

    Example:

    ```
    rm -rf occncc_rollback_iam_schema_<version>.sql
    rm -rf restore.sql
    ```

6.3 CNC Console Rollback

This section describes the procedure to Rollback CNC Console.

> **Note**
>
> Existing release name must be used for rollback.

1. Rollback M-CNCC IAM DB.

   > **Note**
   >
   > Not applicable for OCI deployment.

2. Run the following command to check which revision you need to rollback:

   ```
   $ helm history <release_name> -n <namespace>
   ```

   For example:

   ```
   $ helm history cncc -n cncc
   ```

3. Run the following command to rollback to the required revision:

   ```
   $ helm rollback <release_name> <revision_number> -n <namespace>
   ```

   For example:

   ```
   $ helm rollback cncc 1 -n cncc
   ```

7 Uninstalling CNC Console

This chapter provides information about uninstalling Cloud Native Configuration Console.

> **Note**
>
> kubectl commands might vary based on the platform deployment. Replace kubectl with Kubernetes environment-specific command line tool to configure Kubernetes resources through kube-api server. The instructions provided in this document are as per the Oracle Communications Cloud Native Environment (OCCNE) 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.

7.1 Uninstalling CNC Console Using Helm

To uninstall CNC Console, run the following command:

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

Where,

<release_name> is a name provided by the user to identify the helm deployment.

<namespace_name> is a name provided by the user to identify the namespace of CNC Console deployment.

For example:

```
$ helm uninstall cncc --namespace cncc
```

Helm keeps a record of its releases, so you can still reactivate the release after uninstalling it.

To completely remove a release from the cluster, add the `--purge` parameter to `helm delete` command:

```
helm delete --purge release_name
```

For example:

```
helm delete --purge occncc
```

7.2 Deleting Kubernetes Namespace

Perform the following procedure to clean up the CNC Console deployment.

To delete the Jobs after CNC Console is uninstalled or purged:

1. Run the following command to check whether the jobs are present after uninstalling CNC Console:

   ```
   $ kubectl get jobs -n <namespace_name>
   ```

   Example:

   ```
   $ kubectl get jobs -n cncc
   ```

2. If jobs are present, delete jobs using following command:

   ```
   $ kubectl delete jobs --all -n <namespace_name>
   ```

   Example:

   ```
   $ kubectl delete jobs --all -n cncc
   ```

7.3 Deleting the CNC Console MySQL details

Perform the following procedure to delete the CNC Console MySQL database and MySQL user:

1. Log in to the machine which has permission to access the SQL nodes of NDB cluster.
2. Connect to the SQL node of NDB cluster successively.
3. Log in to the MySQL prompt using root permission or as a user with permission to drop the tables.

   For example:

   ```
   mysql -h 127.0.0.1 -uroot -p
   ```

   > **Note**
   >
   > This command may vary from system to system, path for mysql binary, root user and root password. After running this command, user need to enter the password specific to the user mentioned in the command.

4. Run the following command to remove CNC Console databases:

> **Note**
>
> Not applicable for OCI deployment.

a. Run the following command to remove CNC Console IAM database:

```
$ DROP DATABASE if exists <CNCC IAM Database>;
```

For example:

```
$ DROP DATABASE if exists cnccdb;
```

b. Run the following command to remove CNC Console Core database:

```
$ DROP DATABASE if exists <CNCC Core Common Config Database>;
```

For example:

```
$ DROP DATABASE if exists <CNCC Core Common Config Database>;
$ DROP DATABASE if exists mcncccommonconfig;
```

5. Run the following command to remove the CNC Console MySQL users:

```
$ DROP USER IF EXISTS <CNCC User Name>;
```

For example:

```
$ DROP USER IF EXISTS cnccusr;
```

> **Caution**
>
> Remove MySQL users on all the SQL nodes from all the CNCC clusters.

6. Exit from MySQL prompt and SQL node.

7.4 CNC Console Cleanup During Upgrade Failure

The CNC Console 22.2.x or earlier releases used two helm chart deployment for deploying `cncc-iam` and `cncc-core` components. From CNC Console 22.3.0 onwards, single helm chart is used for deploying all the console components.

This section discuss about the required clean up, if the helm upgrade fails due to miss configuration. You must perform this procedure before running helm upgrade again.

Following resources require cleanup during upgrade failure:

- Roles
- RoleBindings

- ServiceAccounts
- ConfigMaps
- PodDisruptionBudgets
- Services

> **Note**
>
> While upgrading from older CNCC version to CNCC 24.1.1, it is recommended to upgrade using the existing IAM release name ("cncc-iam"). The examples mentioned below are based on this assumption that release name is cncc-iam.
>
> For more details about the upgrade, see CNC Console Upgrade and Rollback Procedure section.

Cleanup Steps:

- **For Roles**

1. Run the following command to check for the roles created:

   ```
   $ kubectl get roles –n <namespace_name>
   ```

   Example:

   ```
   $ kubectl get roles –n cncc
   ```

2. Run the following command to delete the following roles if exists:

   ```
   $ kubectl delete roles -n <namespace_name> <release_name>-acore-
   ingressgateway-role
                                              <release_name>-mcore-
   ingressgateway-role
                                              <release_name>-iam-
   ingressgateway-role
                                              <release_name>-helmtest-role
   ```

   Example:

   ```
   $ kubectl delete roles -n cncc cncc-acore-ingressgateway-role cncc-mcore-
   ingressgateway-role cncc-iam-ingressgateway-role cncc-helmtest-role
   ```

- **RoleBindings**

1. Run the following command to check whether the RoleBindings already exist:

   ```
   $ kubectl get rolebindings –n <namespace_name>
   ```

   Example:

   ```
   $ kubectl get rolebindings –n cncc
   ```

2. Run the following command to delete the following RoleBindings if exists:

```
$ kubectl delete rolebindings -n <namespace_name> <release_name>-acore-
ingressgateway-rolebinding-v1
                                                  <release_name>-mcore-
ingressgateway-rolebinding-v1
                                                  <release_name>-iam-
ingressgateway-rolebinding-v1
                                                  <release_name>-helmtest-
rolebinding
```

Example:

```
$ kubectl delete rolebindings -n cncc cncc-acore-ingressgateway-
rolebinding-v1
      cncc-mcore-ingressgateway-rolebinding-v1 cncc-iam-ingressgateway-
rolebinding-v1
      cncc-helmtest-rolebinding
```

- **ServiceAccounts**

1. Run the following command to check whether the ServiceAccounts already exist:

```
$ kubectl get sa –n <namespace_name>
```

Example:

```
$ kubectl get sa –n cncc
```

2. Run the following command to delete the following ServiceAccounts if exists:

```
$ kubectl delete sa -n cncc <release_name>-acore-ingress-gateway
                            <release_name>-helmtest-serviceaccount
                            <release_name>-mcore-ingress-gateway
```

Example:

```
$ kubectl delete sa -n cncc cncc-acore-ingress-gateway cncc-helmtest-
serviceaccount
      cncc-mcore-ingress-gateway cncc-iam-ingress-gateway
```

- **ConfigMaps**

1. Run the following command to check whether the ConfigMaps already exist:

```
$ kubectl get configmap –n <namespace_name>
```

Example:

```
$ kubectl get configmap –n cncc
```

2. Run the following command to delete the following ConfigMaps if exists:

```
kubectl delete configmap -n <namespace_name  <release_name>-acore-ingress-
gateway
                                                <release_name>-mcore-
cmservice
                                                <release_name>-mcore-
ingress-gateway
                                                <release_name>-iam-ingress-
gateway
```

Example:

```
$ kubectl delete configmap -n cncc cncc-acore-ingress-gateway cncc-mcore-
cmservice
      cncc-mcore-ingress-gateway cncc-iam-ingress-gateway
```

- **PodDisruptionBudgets**

1. Run the following command to check whether the PodDisruptionBudgets already exist:

```
$ kubectl get poddisruptionbudget –n <namespace_name>
```

Example:

```
$ kubectl get poddisruptionbudget –n cncc
```

2. Run the following command to delete the following PodDisruptionBudgets if exists:

```
$ kubectl delete poddisruptionbudget -n <namespace_name> <release_name>-
acore-ingress-gateway-podDisruptionBudget
                                                        <release_name>-
mcore-cmservice-podDisruptionBudget
                                                        <release_name>-
mcore-ingress-gateway-podDisruptionBudget
                                                        <release_name>-
iam-ingress-gateway-podDisruptionBudget
```

Example:

```
$ kubectl delete poddisruptionbudget -n cncc  cncc-acore-ingress-gateway-
podDisruptionBudget
      cncc-mcore-cmservice-podDisruptionBudget cncc-mcore-ingress-gateway-
podDisruptionBudget
      cncc-iam-ingress-gateway-podDisruptionBudget
```

- **Services**

1. Run the following command to check whether the Services already exist:

```
$ kubectl get Services –n <namespace_name>
```

Example:

```
$ kubectl get Services –n cncc
```

2. Run the following command to delete the following Services if exists:

```
$ kubectl delete svc -n <namespace_name> <release_name>-acore-igw-cache
                                         <release_name>-acore-ingress-
gateway
                                         <release_name>-mcore-cmservice
                                         <release_name>-mcore-igw-cache
                                         <release_name>-mcore-ingress-
gateway
                                         <release_name>-iam-igw-cache
                                         <release_name>-iam-ingress-gateway
                                         <release_name>-iam-kc-headless
                                         <release_name>-iam-kc-http
```

Example:

```
$ kubectl delete svc -n cncc cncc-acore-igw-cache cncc-acore-ingress-
gateway
      cncc-mcore-cmservice cncc-mcore-igw-cache cncc-iam-igw-cache cncc-
mcore-ingress-gateway
      cncc-iam-ingress-gateway cncc-iam-kc-headless
```

7.5 CNC Console Helm Test Cleanup

For the information about CNC Console Helm Test Cleanup, see Helm Test Cleanup section.

8
Fault Recovery

This chapter provides information about fault recovery for Cloud Native Configuration Console deployment.

8.1 Overview

You must take database backup and restore it either on the same or a different cluster. It uses the CNCC database to run any command or follow instructions.

> **Note**
>
> This chapter describes fault recovery scenarios of CNC Console and how to recover from those scenarios.

> **Note**
>
> The Fault Recovery procedure exclusively applies to CNC Console and does not encompass any aspects related to OCI Resources.

8.2 Impacted Area

The following table describes scenarios about the impacted areas during CNC Console fault recovery:

Table 8-1 Fault Recovery Scenarios Impact Information

Scenario	Requires Fault Recovery or re-install of CNE?	Requires Fault Recovery or re-install of cnDBTier?	Requires Fault Recovery or re-install of CNC Console?	Comments
Scenario 1: Complete Site Failure	Yes	Yes	Yes	
Scenario 2: cnDBTier Corruption	No	Yes	No	DBTier must be restored from backup. Re-install of CnDBTier can be considered, if restoring from backup is not possible. Use helm upgrade if DB configuration is changed

Table 8-1 (Cont.) Fault Recovery Scenarios Impact Information

Scenario	Requires Fault Recovery or re-install of CNE?	Requires Fault Recovery or re-install of cnDBTier?	Requires Fault Recovery or re-install of CNC Console?	Comments
Scenario 3: Console Configuration Database Corruption	No	No	No	Backup and restore of configuration database is required on the impacted site. This needs periodic backup. (Applicable for M-CNCC IAM). **Note:** Not applicable for OCI deployment
Scenario 4: Deployment Failure	No	No	Yes	CNC Console DB is not restored. Only helm uninstall/install is done. (Applicable for M-CNCC IAM, M-CNCC Core and A-CNCC Core). **Note:**For OCI deployment, only M-CNCC Core and A-CNCC Core are applicable.
Scenario 5: NF Instance Failure	No	No	Yes	The NF endpoints must be updated in the custom values.yaml file and helm upgrade must be performed to incorporate the latest endpoints (Applicable at M-CNCC Core and A-CNCC Core).

8.3 Prerequisites

Before you run any fault recovery procedure, ensure that the following prerequisites are met:

- DBTier should be in healthy state and available on multiple sites along with CNC Console.
- On demand backup should be enabled on DBTier. Scheduled regular backups help to:
  - Restore stable version of the CNC Console configuration database.
  - Minimize significant loss of data due to upgrades or roll back failures.
  - Minimize loss of data due to system failure.
  - Minimize loss of data due to data corruption or deletion due to external input.
  - Migrate Console database information from one site to another.

- Custom values file used at the time of Console deployment is retained. If the `custom_values.yaml` file is not retained, then regenerate it manually. This task increases the overall fault recovery time.
- Docker images used during the last installation or upgrade must be retained in the external data source.
  For the CNC Console database backup and restore prerequisites, see Fault Recovery Procedures - DB Backup and Restore section.

8.4 Fault Recovery Scenarios

This section describes the fault recovery procedures for various scenarios.

8.4.1 Scenario 1: Complete 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:

- Scenario 1A: Single or Multiple Site Failure
- Scenario 1B: All Sites Failure

8.4.1.1 Scenario 1A: Single or Multiple Site Failure

This scenario applies when one or more sites, and not all sites, have failed and there is a requirement to perform fault recovery. It is assumed that the user has DBTier and Oracle Communications CNC Console installed on multiple sites with automatic data replication and backup enabled.

To recover the failed sites:

1. Run the Cloud Native Environment (CNE) installation procedure to install a new cluster. For more information, see *Oracle Communications Cloud Native Environment (OCCNE) Installation Guide.*
2. For CnDBTier fault recovery:
   a. Take on-demand backup from the mate site that has health replication with the failed site or sites.
   b. Use the backup data from the mate site to restore the database.
3. Install CNC Console helm chart. For more information about installing CNC Console, see the Installing CNC Console chapter in the *Oracle Communications Cloud Native Configuration ConsoleInstallation and Upgrade Guide.*

8.4.1.2 Scenario 1B: All Sites Failure

This scenario applies when all sites have failed and there is a requirement to perform fault recovery. It is assumed that the user has DBTier and Oracle Communications CNC Console installed on multiple sites with automatic data replication and backup enabled.

To recover all the failed sites:

1. Run the Cloud Native Environment (CNE) installation procedure to install a new cluster. For more information, see *Oracle Communications Cloud Native Environment (OCCNE) Installation Guide.*
2. Use an on-demand backup file to restore the database from previous data backup.

> **Note**
>
> - The auto-data backup file is one that is built from scheduled automatic backup.
> - The Restore Georeplication Failure chapter contains a procedure for two sites where one of the clusters has a fatal error. You can perform the same procedure for all the sites in a multiple site setup.

3. Install CNC Console helm chart. For more information about installing CNC Console, see the Installing CNC Console chapter in the *Oracle Communications Cloud Native Configuration Console Installation and Upgrade Guide.*

8.4.2 Scenario 2: cnDBTier Corruption

This section describes how to recover a database when the data replication has failed due to database corruption and cnDBTier has failed in single, multiple sites, or all sites.

When the database gets corrupted, the database on all the other sites can also get corrupted due to data replication. It depends on the replication status after the corruption has occurred. If the data replication fails due to database corruption, then DBTier fails in either single or multiple sites (not all sites). If the data replication is successful, then database corruption replicates to all the cnDBTier sites and cnDBTier fails in all sites.

The following are cnDBTier failure scenarios:

If corrupted database is replicated to mated sites, follow:

- Scenario 2A: When DBTier fails in Single or Multiple (but not all) Sites

If corrupted database causes replication failure and hence local to a site, follow:

- Scenario 2B: When CnDBTier failed in all Sites

> **Note**
>
> This impacts all the NFs using the corrupted cnDBTier. All the NFs sharing cnDBTier needs to do a fault recovery as cnDBTier is corrupted.

8.4.2.1 Scenario 2A: When DBTier fails in Single or Multiple (but not all) Sites

This section describes how to recover database when the data replication has failed due to database corruption and DBTier has failed in either single or multiple sites (not all sites).

To recover database:

1. Uninstall CNC Console helm chart. For information about uninstalling CNC Console, see the Uninstalling CNC Console chapter in the *Oracle Communications Cloud Native Configuration ConsoleInstallation and Upgrade Guide.*

2. For DBTier fault recovery:
   a. Create on-demand backup from mated site that has health replication with failed site.
   b. Use the backup data from mate site for restoration.
3. Install CNC Console helm chart. For more information about installing CNC Console, see the Installing CNC Console chapter in the Oracle Communication Cloud Native Configuration ConsoleInstallation and Upgrade Guide.

8.4.2.2 Scenario 2B: When CnDBTier failed in all Sites

This section describes how to recover database when successful data replication corrupts all the DBTier sites.

To recover database:

1. Uninstall CNC Console helm charts. For more information about uninstalling CNC Console, see the Uninstalling CNC Console chapter in the *Oracle Communications Cloud Native Configuration ConsoleInstallation and Upgrade Guide.*
2. For CnDBTier fault recovery:
   a. Use an on-demand backup file to restore the database from the previous data backup.

> **Note**
>
> The Restore Georeplication Failure chapter has a procedure for two sites where one of the cluster has fatal error. You can perform that procedure for all the sites in a multiple site setup.

3. Install CNC Console helm charts. For more information about installing CNC Console, see the Installing CNC Console chapter in the *Oracle Communication Cloud Native Configuration Console Installation and Upgrade Guide.*

8.4.3 Scenario 3: Console Configuration Database Corruption

> **Note**
>
> Not applicable for OCI deployment

This section describes how to recover when the CNC Console configuration database is corrupted.

For recovery and restore procedure, see the Fault Recovery Procedures - DB Backup and Restore section.

8.4.4 Scenario 4: Deployment Failure

> **Note**
>
> For OCI deployment, only M-CNCC Core and A-CNCC Core are applicable.

This section describes how to recover CNC Console when its deployment fails.

For recovery and restore procedure, see Restoring CNC Console .

8.4.5 Scenario 5: NF Instance Failure

Perform this procedure to recover from NF instance failure.

1. Refer to the procedures in the specific NF Disaster Recovery Guide to find the necessary action required to be taken.
2. Check whether the NF endpoints are the same.
   a. If the NF endpoints are the same, no change is required in CNC Console side.
   b. If the NF endpoints are different, update the NF IP and Port in the *occncc_custom_values_<version>.yaml* file and perform a helm upgrade operation to incorporate the new NF URL.

A.1 CNC Console Microservices

This section provides the details of CNC Console microservices.

A.1.1 M-CNCC IAM Microservices

> **Note**
>
> Not applicable for OCI deployment.

M-CNCC IAM has the microservices which are responsible for Identity Access Management:

The following is an example of services CNC Console IAM offers:

Table 2 CNC Console IAM Microservices

NAME	TYPE	PORT(S)
cncc-iam-kc-headless	ClusterIP	8285/TCP
cncc-iam-kc-http	ClusterIP	8285/TCP
cncc-iam-ingress-gateway	LoadBalancer	8080:30346/TCP
cncc-iam-cncc-iam-igw-cache	ClusterIP	8000/TCP

> **Note**
>
> `cncc-iam-cncc-iam-igw-cache` is an Ingress Gateway cache service which is enabled by default by Ingress Gateway chart. CNC Console IAM does not use this feature.

A.1.2 M-CNCC Core Microservices

M-CNCC Core has two microservices:

1. **cncc-mcore-ingress-gateway**: cncc-mcore-ingress-gateway is responsible to forward the request either to the Agent CNCC or to CNC Console GUI.
2. **cncc-mcore_cmservice**: cncc-mcore_cmservice is responsible for displaying CNC Console GUI.

Following is an example of services M-CNCC Core offers:

Non OCI

```
NAME                        TYPE          CLUSTER-IP       EXTERNAL-IP
PORT(S)                   AGE
cncc-mcore-cmservice        ClusterIP     10.108.119.182   <none>
8442/TCP                  24h
cncc-mcore-igw-cache        ClusterIP     None             <none>
8000/TCP                  24h
```

```
cncc-mcore-ingress-gateway   LoadBalancer   10.103.6.17      <pending>
8080:30075/TCP             24h
```

OCI

```
NAME                          TYPE           CLUSTER-IP      EXTERNAL-
IP                    PORT(S)         AGE
cncc-mcore-cmservice          ClusterIP      10.96.100.237
<none>                         8442/TCP        44m
cncc-mcore-igw-cache          ClusterIP      None
<none>                         8000/TCP        44m
cncc-mcore-ingress-gateway    LoadBalancer   10.96.64.105
10.0.20.117,129.213.159.165    443:31114/TCP   44m
```

Table 3 M-CNCC Core Microservices

NAME	TYPE	PORT(S)
cncc-mcore-cmservice	ClusterIP	8442/TCP
cncc-mcore-igw-cache	ClusterIP	8000/TCP
cncc-mcore-ingress-gateway	LoadBalancer	8080:31417/TCP

> **Note**
>
> `cncc-iam-cncc-iam-igw-cache` is an Ingress Gateway cache service which is enabled by default by Ingress Gateway chart. CNC Console core does not use this feature.

A.1.3 A-CNCC Core Microservices

A-CNCC Core has the "cncc-acore-ingress-gateway" microservice . It is cncc-acore-ingress-gateway is responsible for forwarding the request to the NF.

Following is an example of services A-CNCC Core offers:

Non OCI

```
NAME                          TYPE           CLUSTER-IP       EXTERNAL-IP
PORT(S)       AGE
cncc-acore-igw-cache          ClusterIP      None             <none>
8000/TCP      24h
cncc-acore-ingress-gateway    ClusterIP      10.105.11.175    <none>
8080/TCP      24h
```

OCI

```
NAME                          TYPE           CLUSTER-IP      EXTERNAL-IP
PORT(S)         AGE
cncc-acore-igw-cache          ClusterIP      None            <none>
8000/TCP        44m
cncc-acore-ingress-gateway    ClusterIP      10.96.171.188   <none>
443/TCP         44m
```

Table 4 A-CNCC Core Microservices

NAME	TYPE	PORT(S)
cncc-acore-cncc-core-igw-cache	ClusterIP	8000/TCP
cncc-acore-ingress-gateway	ClusterIP	8080/TCP

> **Note**
>
> `cncc-acore-igw-cache` is an Ingress Gateway cache service which is enabled by default by Ingress Gateway helm chart. CNC Console Core does not use this feature.

B.1 CNC Console Microservices to Port Mapping

This section contains CNC Console microservices to port mapping details.

Table 5 Microservices to Port Mapping

Flow Description	Source Node	Type	Destination Node	Nature of Port	Nature of IP	Network Type	Service Port	Protocol	Notes
cncc-mcore-ingress-gateway	User interface / LoadBalancer VM	service	cncc-mcore-ingress-gateway	External	LoadBalancer	RAN / F5	8080:30075	http	
cncc-iam-ingress-gateway	User interface / LoadBalancer VM	service	cncc-iam-ingress-gateway	External	LoadBalancer	RAN / F5	8080:30085	http	
DNS query	cncc-iam-ingress-gateway		DNS server	External			53	dns	
DNS query	cncc-mcore-ingress-gateway		DNS server	External			53	dns	
Pod-Service cmservice flow	cncc-mcore-cmservice	service	cncc-mcore-cmservice	Internal	ClusterIP	Internal / K8s	8442	http	
cncc-iam-http	cncc-iam-ingress-gateway	service	cncc-iam-kc-http	Internal	ClusterIP	Internal / K8s	8285	http	
cncc-iam-http	cncc-iam-ingress-gateway	pod	cncc-iam-kc-0	Internal	ClusterIP	Internal / K8s	8080	http	
cncc-iam-http	cncc-iam-kc-0	service	cnDBTier service	Internal	ClusterIP	Internal / K8s	3306	http	
cncc-iam-http	cncc-iam-kc-0	service	Thirdparty LDAP service	External				ldap	Depends on Customer LDAP
cncc-iam-http	cncc-iam-kc-0	service	Thirdparty SAML service	External				saml	Depends on Customer SAML Provider

Table 5 (Cont.) Microservices to Port Mapping

Flow Description	Source Node	Type	Destination Node	Nature of Port	Nature of IP	Network Type	Service Port	Protocol	Notes
cncc-mcore-cmservice	cncc-mcore-ingress-gateway	pod	cncc-mcore-cmservice	Internal	ClusterIP	Internal / K8s	8442	http	
cncc-mcore-cmservice	cncc-mcore-ingress-gateway	service	cncc-mcore-cmservice	Internal	ClusterIP	Internal / K8s	8442	http	
nf configuration	cncc-mcore-ingress-gateway	service	nf config service	Internal	ClusterIP	Internal / K8s	8000	http	Communication between NF and CNCC, there can be more than one NF supported in CNCC.
metrics	worker node	pod	cncc-iam-ingress-gateway	Internal	Internal	Internal / K8s	9090	http	GET /actuator/health
cncc-iam-ingress-gateway	worker node	pod	cncc-iam-ingress-gateway	Internal	Internal	Internal / K8s	8081	http	
Readiness	worker node	pod	cncc-mcore-cmservice	Internal	Internal	Internal / K8s	9000	http	liveness
cncc-iam-http	worker node	pod	cncc-iam-kc-0	Internal	Internal	Internal / K8s	8080	http	User Creation, configuration
cncc-mcore-ingress-gateway	worker node	pod	cncc-mcore-ingress-gateway	Internal	Internal	Internal / K8s	8081	http	
metrics	worker node	pod	cncc-mcore-ingress-gateway	Internal	Internal	Internal / K8s	9090	http	GET /actuator/health

C.1 CNC Console Validation-hook Error Codes

A preinstall hook named Validation-hook is introduced for validating M-CNCC Core and A-CNCC Core helm configurations.

Validation hook pod is auto deleted if validation succeeds. In case of failure, pod status is displayed as" *Error*.

In case of Validation-hook errors, refer to the following error codes:

Table 6 Validation-hook Error Codes

Error Code	Error Message Format	Error Scenarios	Sample Error Messages
1001	Invalid value. Resource: <Configuration Name>, ID: <ID>, Attribute: <Attribute>. <More Info>	• Port should be Numeric • Scheme should be either HTTP/HTTPS • IDs should follow the alphanumeric pattern • Max Limit should be satisfied for M-CNCC IAM, A-CNCC and Instance • Max Length for Instance Id • Max Length for Self Cncc Id • CS instance must have one of these CS subtypes <grafana, kibana, jaeger, prometheus, alertmanager> • DD instances must have one of these subtypes <ocnadd, ocnaddapi> • NWDAF instances must have one of these subtypes <ocnwdaf, ocnwdafapi> • Both ip and fqdn cannot be provided. • InvalidConfig • Only one of the flags among oci-iam, cncc-iam should be enabled at a time • multicluster flag should be false in case of single-cluster deployment – cncc-iam, mcncc-core, acncc-core flags should be set to true • multicluster flag should be true in case of multi-cluster deployment – Multi Cluster(manager only) - cncc-iam, mcncc-cncc should be set to true and acncc-core should be set to false – Multi Cluster(managing local NF's) - cncc-iam, mcncc-cncc and acncc-core should be set to true. – Multi cluster(agent only) - cncc-iam, mcncc-cncc should be set to false and acncc-core should be set to true • multicluster flag should be false in case of single-cluster deployment	Invalid value. Resource: mCncclam, ID: Cluster1, Attribute: Port. It should be numeric value. Invalid value. Resource: instance, ID: Cluster3-instance1, Attribute: Scheme. Allowed values are: [http, https]. Invalid value. Resource: instance, ID: Cluster1-grafana##$$%, Attribute: id. Ids should be alphanumeric with hyphen allowed as special character. The count of mCncclam exceeded max limit. Allowed Value:x. Actual Value: y Max limit exceeded. Allowed Value:x. Actual Value: y Invalid value. Resource: aCncc, ID: Cluster3, Attribute: N/A. Both ip and fqdn cannot be provided. Invalid value. Resource: isMultiClusterEnabled, ID:,Attribute: False. isMultiClusterEnabled is set as false, only single cluster configuration is allowed. Verify oci-iam, cncc-iam, mcncc-core, acncc-core configuration values Invalid value. Resource: isMultiClusterEnabled, ID:,Attribute: True. isMultiClusterEnabled is set as true, only multi cluster configuration is allowed. Verify oci-iam, cncc-iam, mcncc-core, acncc-core configuration values Invalid value. Resource: isMultiClusterEnabled, ID:,Attribute: False. isMultiClusterEnabled is set as false, only single cluster configuration is allowed. Invalid value. Resource: isMultiClusterEnabled, ID:,Attribute: True. isMultiClusterEnabled is set as true, only multi cluster configuration is allowed. Invalid value. Resource: DD, ID: Cluster1-dd-instance1, Attribute: N/A. More than one DD instance

Table 6 (Cont.) Validation-hook Error Codes

Error Code	Error Message Format	Error Scenarios	Sample Error Messages
		• multicluster flag should be true in case of multi-cluster deployment • there must be 2 DD instances with same instance id (one with type DD-UI and the other with DD-API) • there must be 2 NWDAF instances with same instance id (one with type NWDAF-UI and the other with NWDAF-API) • NF type should be present along with cnDBTier instance • Each NF can have a maximum of 2 instances with same instance ID, one of which must have type cnDBTier	with same id and type is not allowed Invalid value. Resource: instance, ID: Cluster1-dd-instance1, Attribute: apiPrefix. For type DD valid Api Prefixes: [/ocnadd, /ocnaddapi] Invalid value. Resource: NF, ID: Cluster1-instance1, Attribute: N/A. NF type should be present along with cnDBTier instance
1002	Duplicate value. Resource: <Configuration Name>, ID: <ID>, Attribute: <Attribute>. <More Info>	• All A-CNCC IDs must be unique • API prefix must be unique for all instances • Owner(Cluster) must have unique CS/DD/NWDAF subtype	• Duplicate value(s). Resource: aCncc, ID: [Cluster3], Attribute: id. • Duplicate value(s). Resource: instance, ID: N/A, Attribute: apiPrefix. Duplicate Attribute values: [/occne12-ip-cluster/ocnadd] for owner: Kolkata
1003	Invalid Reference. Resource: <Configuration Name>, ID: <ID>, Attribute: <Attribute>. <More Info>	• All the Instance owners must be referenced in M-CNCC IAM IDs or A-CNCC IDs • M-CNCC IAM IDs or OCI IAM IDs and M-CNCC Core IDs must be same	• Invalid Reference. Resource: instance, ID: Cluster5, Attribute: Owner. Not present in mCncc ids or aCncc ids. • Invalid Reference. Resource: instance, ID: N/A, Attribute: N/A. M-Cncc Iam ids and M-Cncc Core ids do not match.
1004	Missing value. Resource: <Configuration Name>, ID: <ID>, Attribute: <Attribute>. <More Info>	• Missing apiPrefix parameter for type CS, DD-UI, DD-API, NWDAF-UI, or NWDAF-API • Either of IP/FQDN should be present(Manager) • SelfCnccId should be present	• Missing value. Resource: instance, ID: Cluster4-grafana, Attribute: apiPrefix. • Missing value. Resource: instance, ID: Cluster3-PolicyInstance, Attribute: N/A. Either ip or fqdn is required.

C.1.1 Validation-hook Microservices and Logs

This section explains about Validation-hook Microservice for M-CNCC Core and A-CNCC Core.

Validation-hook Microservice for M-CNCC Core

```
NAME                                          READY   STATUS  RESTARTS   AGE
cncc-mcore-ingress-gateway-pre-install-rfpjq   0/1 Completed   0        40s
cncc-mcore-validation-hook-zt78c               0/1 Completed   0        24s
```

Validation-hook Logs

In case of validation-hook error, check logs for the error details.

```
NAME                                          READY   STATUS  RESTARTS   AGE
cncc-mcore-validation-hook-zt78c               0/1     Error      0   24s
```

Example:

```
kubectl logs -f cncc-mcore-validation-hook-zt78c -n cncc
```

Sample Validation-hook Logs

```
{
   "instant":{
      "epochSecond":1628155229,
      "nanoOfSecond":4094479
   },
   "thread":"main",
   "level":"ERROR",
   "loggerName":"com.oracle.cgbu.cne.cncc.core.Multi-ClusterConfigValidation",
   "message":"{\"type\":null,\"title\":\"Bad
Request\",\"status\":400,\"detail\":\"[{\\\"type\\\":null,\\\"title\\\":\\
\"Validation Error\\\",\\\"status\\\":1001,\\\"detail\\\":\\\"Invalid value.
Resource: instance, ID: Cluster1-grafana, Attribute: N/A. Both ip and fqdn
cannot be provided.\\\",\\\"instance\\\":null,\\\"cause\\\":null},{\\\"type\\
\":null,\\\"title\\\":\\\"Validation Error\\\",\\\"status\\\":1001,\\\"detail\
\\":\\\"Invalid value. Resource: instance, ID: Cluster3-policy-instance,
Attribute: Port. It should be numeric value.\\\",\\\"instance\\\":null,\\
\"cause\\\":null},{\\\"type\\\":null,\\\"title\\\":\\\"Validation Error\\\",\\
\"status\\\":1004,\\\"detail\\\":\\\"Missing value. Resource: Instance, ID:
Cluster3-grafana, Attribute: apiPrefix. \\\",\\\"instance\\\":null,\\\"cause\\
\":null}]\",\"instance\":null,\"cause\":null}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.log4j.spi.AbstractLogger",
   "contextMap":{

   },
   "threadId":1,
   "threadPriority":5,
   "messageTimestamp":"2021-08-05T09:20:29.004+0000",
   "application":"cncc",
   "engineering_version":"1.8.0",
   "marketing_version":"1.0.0",
```

```
   "microservice":"cncc-mcore-validation-hook",
   "cluster":"cncc-mcore",
   "namespace":"cncc",
   "node":"master",
   "pod":"cncc-mcore-validation-hook-zt78c"
}
```

Validation-hook Microservice for A-CNCC Core

```
NAME                                          READY   STATUS  RESTARTS   AGE
cncc-acore-ingress-gateway-pre-install-rfpjq   0/1 Completed   0        40s
cncc-acore-validation-hook-zt78c               0/1 Completed   0        24s
```

Validation-hook Logs

In case of validation-hook error, check logs for the error details.

```
NAME                                          READY   STATUS  RESTARTS   AGE
cncc-acore-validation-hook-zt78c               0/1     Error      0   24s
```

Example:

```
kubectl logs -f cncc-acore-validation-hook-zt78c -n cncc
```

Sample Validation-hook Logs

```
{
   "instant":{
      "epochSecond":1628155569,
      "nanoOfSecond":4076479
   },
   "thread":"main",
   "level":"ERROR",
   "loggerName":"com.oracle.cgbu.cne.cncc.core.Multi-ClusterConfigValidation",
   "message":"{\"type\":null,\"title\":\"Bad
Request\",\"status\":400,\"detail\":\"[{\\\"type\\\":null,\\\"title\\\":\\
\"Validation Error\\\",\\\"status\\\":1001,\\\"detail\\\":\\\"Invalid value.
Resource: instance, ID: Cluster1-grafana, Attribute: N/A. Both ip and fqdn
cannot be provided.\\\",\\\"instance\\\":null,\\\"cause\\\":null},{\\\"type\\
\":null,\\\"title\\\":\\\"Validation Error\\\",\\\"status\\\":1001,\\\"detail\
\\":\\\"Invalid value. Resource: instance, ID: Cluster3-policy-instance,
Attribute: Port. It should be numeric value.\\\",\\\"instance\\\":null,\\
\"cause\\\":null},{\\\"type\\\":null,\\\"title\\\":\\\"Validation Error\\\",\\
\"status\\\":1004,\\\"detail\\\":\\\"Missing value. Resource: Instance, ID:
Cluster3-grafana, Attribute: apiPrefix. \\\",\\\"instance\\\":null,\\\"cause\\
\":null}]\",\"instance\":null,\"cause\":null}",
   "endOfBatch":false,
   "loggerFqcn":"org.apache.logging.log4j.spi.AbstractLogger",
   "contextMap":{
```

```
    },
    "threadId":1,
    "threadPriority":5,
    "messageTimestamp":"2021-08-05T09:20:29.004+0000",
    "application":"cncc",
    "engineering_version":"1.8.0",
    "marketing_version":"1.0.0",
    "microservice":"cncc-acore-validation-hook",
    "cluster":"cncc-acore",
    "namespace":"cncc",
    "node":"master",
    "pod":"cncc-acore-validation-hook-zt78c"
}
```

D.1 cnDBTier Profile

This section includes information about cnDBTier profiles.

cnDBTier Profile

Table 7 cnDBTier Profile

Service/Component	Per Pod						Side Cars:db-backup-exec-service (DB Tier Sidecar)Service Mesh Sidecar (ASM, Istio/ Envoy)				Number of Pods (Replica)	Total					
	CPU		Memory		Storage		CPU		Memory			CPU		Memory		Storage	
	Min	Max	Min	Max	PVC	Count	Min	Max	Min	Max		Min	Max	Min	Max	PVC	Count
Management (MGMT STS) • k8 Resource Type: StatefulSet • Sidecar name: NA • svc: ndbmgmdsvc	2	2	1	1.25	2	1	0.2	0.2	0.256	0.256	**2**(mgmReplicaCount)	4.4	4.4	2.512	3.012	4	2
NDB Data Store (NDB STS) • k8 Resource Type: StatefulSet • Sidecar name: db-executor-svc • svc : ndbmtdsvc	2	2	4	4	64	11	1.2	1.2	2.256	2.256	**2** (ndbReplicaCount)	6.4	6.4	12.512	12.512	128	22
Replication (SQL STS - mysqld) • k8 Resource Type: StatefulSet • Sidecar name: init-sidecar • svc : ndbmysqldsvc	2	2	1	1	4	1	0.3	0.3	0.512	0.512	**2** 2/4/6 (Depending on GR setup of 2/3/4 site) (apiReplicaCount)	4.6	4.6	3.024	3.024	8	2
App Access (SQL STS - appmysqld) • k8 Resource Type StatefulSet • Sidecar name: init-sidecar • svc : ndbappmysqldsvc	2	2	1	1	4	1	0.1	0.1	0.256	0.256	**2** (ndbappReplicaCount)	4.2	4.2	2.512	2.512	8	2

Table 7 (Cont.) cnDBTier Profile

Monitor Service • Sidecar name: NA • k8 Resource Type: Deployment • svc: db-monitor-service	1	1	0.5	0.5	0	0	NA	NA	NA	NA	**1**	1	1	0.5	0.5	0	0
Replication Service • Sidecar name: init-discover-sql-ips • k8 Resource Type: Deployment • svc: db-replication-service	0.6	1	1	2	2	1	0.2	0.2	0.5	0.5	**1**	0.8	1.2	1.5	2.5	2	1
GR Recovery Resources • Used for performing Disaster Recovery	2	2	4	4	0	0	0.2	0.2	0.5	0.5		2.2	2.2	4.5	4.5	0	0
Backup Manager Service • Sidecar name: NA • k8 Resource Type: Deployment • svc: db-backup-manager-svc	0.1	0.1	0.128	0.128	0	0	NA	NA	NA	NA	**1**	0.1	0.1	0.128	0.128	0	0
postUpgradeJob	0.1	0.1	0.256	0.256	0	0						0.1	0.1	0.256	0.256	0	0
preUpgradeJob	0.1	0.1	0.256	0.256	0	0						0.1	0.1	0.256	0.256	0	0
helm test • Sidecar name: NA • k8 Resource Type: Job *Note: This will be created only when "helm test" is performed*	0.1	0.1	0.256	0.256	0	0						0.1	0.1	0.256	0.256	0	0
											11	24	24.4	27.9655	29.4556	42	11

Table 8 cnDBTier Profile Ephemeral Storage

Service / Component	Per Pod		Side Cars:db-backup-exec-service (DB Tier Sidecar)Service Mesh Sidecar (ASM, Istio/Envoy)		Number of Pods (Replica)	Total	
	Ephemeral Storage		Ephemeral Storage			Ephemeral Storage	
	Min	Max	Min	Max		Min	Max
Management (MGMT STS) • k8 Resource Type: StatefulSet • Sidecar name: NA • svc: ndbmgmdsvc	90Mi	100Mi	90Mi	100Mi	**2**(mgmReplicaCount)	360Mi	400Mi
NDB Data Store (NDB STS) • k8 Resource Type: StatefulSet • Sidecar name: db-executor-svc • svc : ndbmtdsvc	90Mi	100Mi	180Mi	1Gi	**2** (ndbReplicaCount)	540Mi	2200Mi
Replication (SQL STS - mysqld) • k8 Resource Type: StatefulSet • Sidecar name: init-sidecar • svc : ndbmysqldsvc	90Mi	100Mi	180Mi	200Mi	**2** 2/4/6 (Depending on GR setup of 2/3/4 site) (apiReplicaCount)	540Mi	600Mi
App Access (SQL STS - appmysqld) • k8 Resource Type StatefulSet • Sidecar name: init-sidecar • svc : ndbappmysqldsvc	90Mi	100Mi	90Mi	100Mi	**2** (ndbappReplicaCount)	360Mi	400Mi
Monitor Service • Sidecar name: NA • k8 Resource Type: Deployment • svc: db-monitor-service	90Mi	100Mi	NA	NA	**1**	90Mi	100Mi
Replication Service • Sidecar name: init-discover-sql-ips • k8 Resource Type: Deployment • svc: db-replication-service	90Mi	1000Mi	90Mi	100Mi	**1**	180Mi	1100Mi
GR Recovery Resources • Used for performing Disaster Recovery	90Mi	1000Mi	90Mi	100Mi		180Mi	1100Mi
Backup Manager Service • Sidecar name: NA • k8 Resource Type: Deployment • svc: db-backup-manager-svc	90Mi	100Mi	NA	NA	**1**	90Mi	100Mi
postUpgradeJob						90Mi	100Mi
preUpgradeJob							

Table 8 (Cont.) cnDBTier Profile Ephemeral Storage

helm test • Sidecar name: NA • k8 Resource Type: Job **Note:** This will be created only when "helm test" is performed							
Totals					11	2430Mi	6100Mi

> **Note**
>
> - In case of shared cnDBTier between Console and NF, Console DB Profile sizing needs to be included in NF DB Profile sizing.
> - cnDBTier custom values.yaml file has been included along with Console package from 23.3.0 release. The yaml file reflects the above cnDBTier profile and is packaged along with the Console custom values.yaml file used for installation. For installing the DBTier, Please refer to the *Oracle Communications Cloud Native Core, cnDBTier Installation, Upgrade, and Fault Recovery Guide.*

E.1 Support for IPv4 or IPV6 Configuration for CNC Console

CNC Console supports following deployment modes:

1. Single Stack with IPv4 only
2. Single Stack with IPv6 only
3. DualStack with IPv4 Preferred
4. DualStack with IPv6 Preferred

Procedure

To deploy the CNC Console in any of these supported modes:

1. Before CNC Console deployment, update *occncc_custom_values<version>.yaml* file and set the **cncc-iam.kc.preferIpv6Stack.enabled** flag to desired value as mentioned in the below table.
2. After CNC Console is deployed, the following CNC Console services must be backed up, deleted and reapplied with preferred IP_Family configuration as mentioned in the following table:

> **Note**
>
> Below services have 'cncc' as the release name cncc-acore-ingress-gateway cncc-iam-ingress-gateway cncc-iam-kc-http cncc-mcore-cmservice cncc-mcore-ingress-gateway
> These services do not have any clusterIP assigned, and hence can be ignored. cncc-acore-igw-cache cncc-mcore-igw-cache cncc-iam-igw-cache cncc-iam-kc-headless.

The following table outlines the changes to be made before and after deploying the CNC Console for each deployment mode:

Table 9 Single or Dual Stack IP Configuration

Cluster Deployment Mode	CNC Console Deployment Mode	CNC Console custom values.yaml (PreInstallation Step)	Service configuration with preferred IP Family (PostInstallation Step)

Single Stack with IPv4 only	NA	`cncc-iam:`
		`  kc:`
		
		`preferIpv6Stack:`
		`  enabled:`
		`false`
			This will lead to no changes in the service file. Depending on the cluster, IPs will be assigned.

Table 9 (Cont.) Single or Dual Stack IP Configuration

Cluster Deployment Mode	CNC Console Deployment Mode	CNC Console custom values.yaml (PreInstallation Step)	Service configuration with preferred IP Family (PostInstallation Step)

Single Stack with IPv6 only	NA	`cncc-iam:`
		`  kc:`
		
		`preferIpv6Stack:`
		`  enabled:`
		`true`
			This will lead to no changes in the service file. Depending on the cluster, IPs will be assigned.

DualStack with IPv4 Preferred	IPv4 Preferred	`cncc-iam:`
		`  kc:`
		
		`preferIpv6Stack:`
		`  enabled:`
		`false`
			This will lead to no changes in the service file. Depending on the cluster, IPs will be assigned.

	IPv6 Preferred	`cncc-iam:`
		`  kc:`
		
		`preferIpv6Stack:`
		`  enabled:`
		`true`
			`spec:`
			
			`ipFamilyPolicy:`
			`RequireDualStack`
			`  ipFamilies:`
			`  - IPv6`
			`  - IPv4`

DualStack with IPv6 Preferred	IPv4 Preferred	`cncc-iam:`
		`  kc:`
		
		`preferIpv6Stack:`
		`  enabled:`
		`false`
			`spec:`
			
			`ipFamilyPolicy:`
			`RequireDualStack`
			`  ipFamilies:`
			`  - IPv4`
			`  - IPv6`

	IPv6 Preferred	`cncc-iam:`
		`  kc:`
		
		`preferIpv6Stack:`
		`  enabled:`
		`true`
			This will lead to no changes in the service file. Depending on the cluster, IPs will be assigned.

> **Note**
>
> Run the following commands to edit the service:
>
> ```
> kubectl edit svc -n <cncc_namespace> <cncc_service>
> ```
>
> For example:
>
> ```
> kubectl edit svc -n cncc -n cncc-iam-ingress-gateway
> ```

Sample CNC Deployment with IPv6 on DualStack with IPv4 Preferred Setup

Consider an example where you want to deploy CNC Console preferred with IPv6 on DualStack with IPv4 Preferred setup. This example describes the configuration changes required for single service of CNC Console after the deployment. You must follow a similar procedure for rest of the CNC Console services. Here:

- CNC Console deployment namespace: **cncc**
- CNC Console release name: **cncc**
- CNC Console service to be edited: **cncc-iam-ingress-gateway**
- Infrastructure Deployment Mode: **DualStack with IPv4 Preferred**
- CNC Console Deployment Mode: **IPv6 Preferred**

Procedure:

1. Run the following command to verify that cncc-iam-ingress-gateway service is set to IPv4 address:

   ```
   kubectl get svc cncc-iam-ingress-gateway -n cncc
   ```

   Output:

   ```
   NAME                                 TYPE           CLUSTER-IP
   EXTERNAL-IP     PORT(S)             AGE
   cncc-iam-ingress-gateway             LoadBalancer   1x.xxx.xx.xx
   1x.xxx.xx.xx    30085:32556/TCP     5h8m
   ```

2. Run the following command to take a backup of cncc-iam-ingress-gateway service and duplicate it for recovery purpose:

   ```
   kubectl get svc cncc-iam-ingress-gateway -n cncc -o yaml > cncc-iam-
   ingress-gateway.yaml;

   cp cncc-iam-ingress-gateway.yaml cncc-iam-ingress-gateway_orig.yaml;
   ```

3. Run the following command to delete the original cncc-iam-ingress-gateway service:

   ```
   kubectl delete svc cncc-iam-ingress-gateway -n cncc
   ```

4. Run the following command to edit the cncc-iam-ingress-gateway.yaml file generated as part of step 2:

   ```
   vim cncc-iam-ingress-gateway.yaml
   ```

5. Update following in the cncc-iam-ingress-gateway.yaml:

   a. Delete **clusterIPs** and **clusterIP** fields completely.

   ```
   # Remove the clusterIP and clusterIPs field
   ...
   spec:
     ...
     clusterIP: 1x.xxx.xx.xx
     clusterIPs:
     - 1x.xxx.xx.xx
   ...
   ```

   b. Under **spec.ipFamilyPolicy** set **RequiredDualStack** and under **spec.ipFamilies** set **[- IPv6, - IPv4]** as follows:

   ```
   apiVersion: v1
   kind: Service
   metadata:
     ...
     name: cncc-iam-ingress-gateway
     namespace: cncc
   spec:
     allocateLoadBalancerNodePorts: true
     ...
     ...
     ipFamilies:
     - IPv6
     - IPv4
     ipFamilyPolicy: RequireDualStack
     ...
     ...
     sessionAffinity: None
     type: LoadBalancer
   status:
     loadBalancer: {}
   ```

6. Run the following command to apply the cncc-iam-ingress-gateway.yaml file:

   ```
   kubectl apply -f cncc-iam-ingress-gateway.yaml -n cncc
   ```

7. Run the following command to check the service output. You should find the service with updated the IPv6 address:

   ```
   kubectl get svc cncc-iam-ingress-gateway -n cncc
   ```

   Output:

   ```
   NAME                                TYPE           CLUSTER-IP
   EXTERNAL-IP             PORT(S)             AGE
   ```

```
cncc-iam-ingress-gateway             LoadBalancer   xxxx:0:0:2::xxxx
xxxx:b400:605:xxx::3     30085:32556/TCP     5h8m
```

F.1 CNC Console Instances Configuration Examples

The following section lists the CNC Console instances configuration examples for single cluster and multi-cluster deployment of supported NFs.

> **Note**
>
> - In the following examples, mCnccIams port is assumed as "80". The mCnccIams port configuration must be added only if port is other than "80".
> - To enable cnDBTier menu for NFs, see the NF Instance Configuration With cnDBTier Menu Enabled section.

> **Note**
>
> **For OCI:**
>
> - To deploy CNC Console on OCI, in all the below mentioned sample configurations for various deployments, ensure setting the **cncc-iam.enabled** flag to *false* and **oci-iam.enabled** flag to *true.*.
>
> ```
> global:
>
>   oci-iam:
>     enabled: true
>   cncc-iam:
>     enabled: false
>   mcncc-core:
>     enabled: true
>   acncc-core:
>     enabled: true
> ```
>
> - the following multicluster configuration is not applicable as Multi-Cluster is not supported on OCI.

Support for Instance Configuration over IPV6 Family IPs

- CNC Console supports configuration of NF and Common Service Instances over IPv6 Family IPs as well. For configuring an IPv6 IP in the Instances:
  - IP must be enclosed in square brackets "[]" as per IPv6 standards
  - The complete IP String must be enclosed in double quotes (""). For example, "[2606:b400:605:b82e::]"

Sample Configuration Using IPV6

```
global:

  oci-iam:
```

```
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
   # Automatic route generation for CNCC Manager & Agent Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: "[2606:b400:605:b82e::]"
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.con6.svc.trypticon.lab.us.oracle.com
      port: 80
  instances:
    - id : Cluster1-bsf-instance1
      type: BSF
      owner: Cluster1
      ip: "[2606:b400:605:b82e::1]"
      port: 80
    - id: Cluster1-kibana
      type: CS
      owner: Cluster1
      ip: "[2606:b400:605:b82e::3]"
      apiPrefix: /jazz/kibana
```

F.1.1 BSF Instances Configuration Examples

F.1.1.1 BSF Single Cluster Deployment Instance Configuration Examples

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
```

```
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-bsf-instance1
      type: BSF
      owner: Cluster1
      fqdn: bsf-ocbsf-config-mgmt.bsf.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-bsf-instance1
      type: BSF
      owner: Cluster1
```

```
    fqdn: bsf-ocbsf-config-mgmt.bsf.svc.cluster.local
    port: 80
```

F.1.1.2 BSF Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-bsf-instance1
      type: BSF
      owner: Cluster1
      fqdn: bsf-ocbsf-config-mgmt.bsf.svc.cluster.local
      port: 80
    - id : Cluster2-bsf-instance1
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf1.svc.cluster.local
      port: 80
    - id : Cluster2-bsf-instance2
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-bsf-instance1
      type: BSF
      owner: Cluster1
      fqdn: bsf-ocbsf-config-mgmt.bsf.svc.cluster.local
      port: 80
    - id : Cluster2-bsf-instance1
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf1.svc.cluster.local
      port: 80
    - id : Cluster2-bsf-instance2
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf2.svc.cluster.local
      port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core is considered to be deployed in Manager Cluster, its an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

 oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-bsf-instance1
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf1.svc.cluster.local
      port: 80
    - id : Cluster2-bsf-instance2
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
```

```
    enabled: false
  cncc-iam:
   enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-bsf-instance1
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf1.svc.cluster.local
      port: 80
    - id : Cluster2-bsf-instance2
      type: BSF
      owner: Cluster2
      fqdn: bsf-ocbsf-config-mgmt.bsf2.svc.cluster.local
      port: 80
```

F.1.2 DD Instance Configuration Examples

F.1.2.1 DD Single Cluster Deployment Instance Configuration Examples

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
```

```
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-12ipcluster      port:
80
  instances:
    - id : Cluster1-dd-instance1
      type: DD-UI
      owner: Cluster1
      fqdn: ocnaddgui.ocnadd-deploy.svc
      port: 80
      apiPrefix: /occne-12ipcluster/ocnadd
    - id : Cluster1-dd-instance1
      type: DD-API
      owner: Cluster1
      fqdn: ocnaddbackendrouter.ocnadd-deploy.svc
      port: 80
      apiPrefix: /occne-12ipcluster/ocnaddapi
```

Sample Configuration for HTTPS Enabled Deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
```

```
    role: Cluster1
    scheme: https
    fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-12ipcluster
    port: 443
instances:
  - id : Cluster1-dd-instance1
    type: DD-UI
    owner: Cluster1
    fqdn: ocnaddgui.ocnadd-deploy.svc
    port: 80
    apiPrefix: /occne-12ipcluster/ocnadd
  - id : Cluster1-dd-instance1
    type: DD-API
    owner: Cluster1
    fqdn: ocnaddbackendrouter.ocnadd-deploy.svc
    port: 80
    apiPrefix: /occne-12ipcluster/ocnaddapi
```

F.1.2.2 DD Multicluster Deployment Instances Configuration Examples

M-CNCC Core on Cluster1, A-CNCC Core on Cluster1 and A-CNCC Core on Cluster2

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-12ipcluster
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
```

```
  - id : Cluster1-dd-instance1
    type: DD-UI
    owner: Cluster1
    fqdn: ocnaddgui.ocnadd-deploy.svc
    port: 80
    apiPrefix: /occne-12ipcluster/ocnadd
  - id : Cluster1-dd-instance1
    type: DD-API
    owner: Cluster1
    fqdn: ocnaddbackendrouter.ocnadd-deploy.svc
    port: 80
    apiPrefix: /occne-12ipcluster/ocnaddapi
  - id : Cluster2-dd-instance1
    type: DD-UI
    owner: Cluster2
    fqdn: ocnaddgui.ocnadd-deploy2.svc
    port: 80
    apiPrefix: /occne-13ipcluster/ocnadd
  - id : Cluster2-dd-instance1
    type: DD-API
    owner: Cluster2
    fqdn: ocnaddbackendrouter.ocnadd-deploy2.svc
    port: 80
    apiPrefix: /occne-13ipcluster/ocnaddapi
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCncclams and aCnccs
- Https port should be updated in mCncclams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
```

```
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-12ipcluster
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-dd-instance1
      type: DD-UI
      owner: Cluster1
      fqdn: ocnaddgui.ocnadd-deploy.svc
      port: 80
      apiPrefix: /occne-12ipcluster/ocnadd
    - id : Cluster1-dd-instance1
      type: DD-API
      owner: Cluster1
      fqdn: ocnaddbackendrouter.ocnadd-deploy.svc
      port: 80
      apiPrefix: /occne-12ipcluster/ocnaddapi
    - id : Cluster2-dd-instance1
      type: DD-UI
      owner: Cluster2
      fqdn: ocnaddgui.ocnadd-deploy2.svc
      port: 80
      apiPrefix: /occne-13ipcluster/ocnadd
    - id : Cluster2-dd-instance1
      type: DD-API
      owner: Cluster2
      fqdn: ocnaddbackendrouter.ocnadd-deploy2.svc
      port: 80
      apiPrefix: /occne-13ipcluster/ocnaddapi
```

> **Note**
>
> In this example local NF and A-CNCC Core is considered to be deployed in Manager Cluster, its an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

 oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
```

```
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-dd-instance1
      type: DD-UI
      owner: Cluster2
      fqdn: ocnaddgui.ocnadd-deploy2.svc
      port: 80
      apiPrefix: /occne-13ipcluster/ocnadd
    - id : Cluster2-dd-instance1
      type: DD-API
      owner: Cluster2
      fqdn: ocnaddbackendrouter.ocnadd-deploy2.svc
      port: 80
      apiPrefix: /occne-13ipcluster/ocnaddapi
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

 oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
```

```
  - id : Cluster2-dd-instance1
    type: DD-UI
    owner: Cluster2
    fqdn: ocnaddgui.ocnadd-deploy.svc
    port: 80
    apiPrefix: /occne-13ipcluster/ocnadd
  - id : Cluster2-dd-instance1
    type: DD-API
    owner: Cluster2
    fqdn: ocnaddbackendrouter.ocnadd-deploy2.svc
    port: 80
    apiPrefix: /occne-13ipcluster/ocnaddapi
```

F.1.3 NRF Instances Configuration Examples

F.1.3.1 NRF Single Cluster Deployment Instance Configuration Examples

NRF Single-Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-nrf-instance1
      type: NRF
      owner: Cluster1
      fqdn: ocnrf-nrfconfiguration.nrf.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCncclams and aCnccs
- Https port should be updated in mCncclams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-nrf-instance1
      type: NRF
      owner: Cluster1
      fqdn: ocnrf-nrfconfiguration.nrf.svc.cluster.local
      port: 80
```

F.1.3.2 NRF Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
```

```
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-nrf-instance1
      type: NRF
      owner: Cluster1
      fqdn: nocnrf-nrfconfiguration.nrf.svc.cluster.local
      port: 80
    - id : Cluster2-nrf-instance1
      type: NRF
      owner: Cluster2
      fqdn: ocnrf-nrfconfiguration.nrf1.svc.cluster.local
      port: 80
    - id : Cluster2-nrf-instance2
      type: NRF
      owner: Cluster2
      fqdn: ocnrf-nrfconfiguration.nrf2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true
```

```
isMultiClusterDeployment: true
# Automatic route generation for CNCC Manager Deployment
 self:
   cnccId: Cluster1
 mCnccIams:
   - id: Cluster1
     scheme: https
     ip: 10.xx.xx.xx
 mCnccCores:
   - id: Cluster1
 aCnccs:
   - id: Cluster1
     role: Cluster1
     scheme: https
     fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
     port: 443
   - id: Cluster2
     role: Cluster2
     scheme: https
     ip: 10.xx.xx.xx
     port: 443
 instances:
   - id : Cluster1-nrf-instance1
     type: NRF
     owner: Cluster1
     fqdn: ocnrf-nrfconfiguration.nrf.svc.cluster.local
     port: 80
   - id : Cluster2-nrf-instance1
     type: NRF
     owner: Cluster2
     fqdn: ocnrf-nrfconfiguration.nrf1.svc.cluster.local
     port: 80
   - id : Cluster2-nrf-instance2
     type: NRF
     owner: Cluster2
     fqdn: ocnrf-nrfconfiguration.nrf2.svc.cluster.local
     port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
```

```
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-nrf-instance1
      type: NRF
      owner: Cluster2
      fqdn: ocnrf-nrfconfiguration.nrf1.svc.cluster.local
      port: 80
    - id : Cluster2-nrf-instance2
      type: NRF
      owner: Cluster2
      fqdn: ocnrf-nrfconfiguration.nrf2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
```

```
    role: Cluster2
instances:
  - id : Cluster2-nrf-instance1
    type: NRF
    owner: Cluster2
    fqdn: ocnrf-nrfconfiguration.nrf1.svc.cluster.local
    port: 80
  - id : Cluster2-nrf-instance2
    type: NRF
    owner: Cluster2
    fqdn: ocnrf-nrfconfiguration.nrf2.svc.cluster.local
    port: 80
```

F.1.4 NSSF Instances Configuration Examples

F.1.4.1 NSSF Single Cluster Deployment Instance Configuration Examples

NSSF Single Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-nssf-instance1
      type: NSSF
      owner: Cluster1
      fqdn: ocnssf-nsconfig.ocnssf-nssf.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-nssf-instance1
      type: NSSF
      owner: Cluster1
      fqdn: ocnssf-nsconfig.ocnssf-nssf.svc.cluster.local
      port: 80
```

F.1.4.2 NSSF Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
```

```
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-nssf-instance1
      type: NSSF
      owner: Cluster1
      fqdn: ocnssf-nsconfig.ocnssf-nssf1.svc.cluster.local
      port: 80
    - id : Cluster2-nssf-instance1
      type: NSSF
      owner: Cluster2
      fqdn: ocnssf-nsconfig.ocnssf-nssf2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
```

```
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-nssf-instance1
      type: NSSF
      owner: Cluster1
      fqdn: ocnssf-nsconfig.ocnssf-nssf1.svc.cluster.local
      port: 80
    - id : Cluster2-nssf-instance1
      type: NSSF
      owner: Cluster2
      fqdn: ocnssf-nsconfig.ocnssf-nssf2.svc.cluster.local
      port: 80
```

> **Note**
>
> In this example local NF and A-CNCC Core is considered to be deployed in Manager Cluster, its a optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
```

```
    ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-nssf-instance1
      type: NSSF
      owner: Cluster2
      fqdn: ocnssf-nsconfig.ocnssf-nssf2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-nssf-instance1
      type: NSSF
      owner: Cluster2
      fqdn: ocnssf-nsconfig.ocnssf-nssf2.svc.cluster.local
      port: 80
```

F.1.5 NWDAF Instance Configuration Examples

F.1.5.1 NWDAF Single Cluster Deployment Instance Configuration Examples

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-223cluster
      port: 80
  instances:
    - id : Cluster1-nwdaf-instance1
      type: NWDAF-UI
      owner: Cluster1
      fqdn: nwdafgui.nwdaf-gui.svc
      port: 80
      apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdaf
    - id : Cluster1-nwdaf-instance1
      type: NWDAF-API
      owner: Cluster1
      fqdn: nwdaf-portal-service.nwdaf-gui.svc
      port: 80
      apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdafapi
```

Sample Configuration for HTTPS Enabled Deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-223cluster
      port: 443
  instances:
    - id : Cluster1-nwdaf-instance1
      type: NWDAF-UI
      owner: Cluster1
      fqdn: nwdafgui.nwdaf-gui.svc
      port: 80
      apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdaf
    - id : Cluster1-nwdaf-instance1
      type: NWDAF-API
      owner: Cluster1
      fqdn: nwdaf-portal-service.nwdaf-gui.svc
      port: 80
      apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdafapi
```

F.1.5.2 NWDAF Multicluster Deployment Instances Configuration Examples

M-CNCC Core on Cluster1, A-CNCC Core on Cluster1 and A-CNCC Core on Cluster2

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
```

```
  enabled: true
mcncc-core:
  enabled: true
acncc-core:
  enabled: true

isMultiClusterDeployment: true
# Automatic route generation for CNCC Manager Deployment
self:
  cnccId: Cluster1
mCnccIams:
  - id: Cluster1
    ip: 10.xx.xx.xx
mCnccCores:
  - id: Cluster1
aCnccs:
  - id: Cluster1
    role: Cluster1
    fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-223cluster
    port: 80
  - id: Cluster2
    role: Cluster2
    ip: 10.xx.xx.xx
    port: 80
instances:
  - id : Cluster1-nwdaf-instance1
    type: NWDAF-UI
    owner: Cluster1
    fqdn: nwdafgui.nwdaf-gui.svc
    port: 80
    apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdaf
  - id : Cluster1-nwdaf-instance1
    type: NWDAF-API
    owner: Cluster1
    fqdn: nwdaf-portal-service.nwdaf-gui.svc
    port: 80
    apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdafapi
  - id : Cluster2-nwdaf-instance1
    type: NWDAF-UI
    owner: Cluster2
    ip: 10.xx.xx.xx
    port: 80
    apiPrefix: /occne-224cluster/nwdaf-gui/ocnwdaf
  - id : Cluster2-nwdaf-instance1
    type: NWDAF-API
    owner: Cluster2
    ip: 10.xx.xx.xx
    port: 80
    apiPrefix: /occne-224cluster/nwdaf-gui/ocnwdafapi
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.occne-223cluster
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-nwdaf-instance1
      type: NWDAF-UI
      owner: Cluster1
      fqdn: nwdafgui.nwdaf-gui.svc
      port: 80
      apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdaf
    - id : Cluster1-nwdaf-instance1
      type: NWDAF-API
      owner: Cluster1
      fqdn: nwdaf-portal-service.nwdaf-gui.svc
      port: 80
      apiPrefix: /occne-223cluster/nwdaf-gui/ocnwdafapi
    - id : Cluster2-nwdaf-instance1
      type: NWDAF-UI
      owner: Cluster2
      ip: 10.xx.xx.xx
      port: 80
      apiPrefix: /occne-224cluster/nwdaf-gui/ocnwdaf
    - id : Cluster2-nwdaf-instance1
      type: NWDAF-API
      owner: Cluster2
```

```
    ip: 10.xx.xx.xx
    port: 80
    apiPrefix:  /occne-224cluster/nwdaf-gui/ocnwdafapi
```

> **Note**
>
> In this example local NF and A-CNCC Core is considered to be deployed in Manager Cluster, its an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-nwdaf-instance1
      type: NWDAF-UI
      owner: Cluster2
      ip: 10.xx.xx.xx
      port: 80
      apiPrefix: /occne-224cluster/nwdaf-gui/ocnwdaf
    - id : Cluster2-nwdaf-instance1
      type: NWDAF-API
      owner: Cluster2
      ip: 10.xx.xx.xx
      port: 80
      apiPrefix: /occne-224cluster/nwdaf-gui/ocnwdafapi
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-nwdaf-instance1
      type: NWDAF-UI
      owner: Cluster2
      ip: 10.xx.xx.xx
      port: 80
      apiPrefix: /occne-224cluster/nwdaf-gui/ocnwdaf
    - id : Cluster2-nwdaf-instance1
      type: NWDAF-API
      owner: Cluster2
      ip: 10.xx.xx.xx
      port: 80
      apiPrefix: /occne-224cluster/nwdaf-gui/ocnwdafapi
```

F.1.6 Policy Instances Configuration Examples

F.1.6.1 Policy Single Cluster Deployment Instance Configuration Examples

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
```

```
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true
  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-policy-instance1
      type: POLICY
      owner: Cluster1
      fqdn: policy-occnp-config-mgmt.policy.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
```

```
    role: Cluster1
    scheme: https
    fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
    port: 443
instances:
  - id : Cluster1-policy-instance1
    type: POLICY
    owner: Cluster1
    fqdn: policy-occnp-config-mgmt.policy.svc.cluster.local
    port: 80
```

F.1.6.2 Policy Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1 and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-policy-instance1
      type: POLICY
      owner: Cluster1
      fqdn: policy-occnp-config-mgmt.policy.svc.cluster.local
      port: 80
    - id : Cluster2-policy-instance1
      type: POLICY
      owner: Cluster2
```

```
      fqdn: policy-occnp-config-mgmt.policy1.svc.cluster.local
      port: 80
    - id : Cluster2-policy-instance2
      type: POLICY
      owner: Cluster2
      fqdn: policy-occnp-config-mgmt.policy2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

 isMultiClusterDeployment: true
 # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-policy-instance1
      type: POLICY
      owner: Cluster1
      fqdn: policy-occnp-config-mgmt.policy.svc.cluster.local
      port: 80
    - id : Cluster2-policy-instance1
      type: POLICY
      owner: Cluster2
```

```
    fqdn: policy-occnp-config-mgmt.policy1.svc.cluster.local
    port: 80
  - id : Cluster2-policy-instance2
    type: POLICY
    owner: Cluster2
    fqdn: policy-occnp-config-mgmt.policy2.svc.cluster.local
    port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-policy-instance1
      type: POLICY
      owner: Cluster2
      fqdn: policy-occnp-config-mgmt.policy1.svc.cluster.local
      port: 80
    - id : Cluster2-policy-instance2
      type: POLICY
      owner: Cluster2
      fqdn: policy-occnp-config-mgmt.policy2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs

- Https port should be updated in mCncclams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-policy-instance1
      type: POLICY
      owner: Cluster2
      fqdn: policy-occnp-config-mgmt.policy1.svc.cluster.local
      port: 80
    - id : Cluster2-policy-instance2
      type: POLICY
      owner: Cluster2
      fqdn: policy-occnp-config-mgmt.policy2.svc.cluster.local
      port: 80
```

F.1.7 PROVGW Instances Configuration Examples

F.1.7.1 PROVGW Single Cluster Deployment Instance Configuration Examples

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
```

```
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-provgw-instance1
      type: PROVGW
      owner: Cluster1
      fqdn: provgw1-provgw-config.provgw.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS Enabled Deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
```

```
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-provgw-instance1
      type: PROVGW
      owner: Cluster1
      fqdn: provgw1-provgw-config.provgw.svc.cluster.local
      port: 80
```

F.1.7.2 PROVGW Multicluster Deployment Instances Configuration Examples

M-CNCC Core on Cluster1, A-CNCC Core on Cluster1 and A-CNCC Core on Cluster2

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-provgw-instance1
      type: PROVGW
      owner: Cluster1
      fqdn: provgw1-provgw-config.provgw.svc.cluster.local
```

```
    port: 80
  - id : Cluster2-provgw-instance1
    type: PROVGW
    owner: Cluster2
    fqdn: provgw1-provgw-config.provgw2.svc.cluster.local
    port: 80
  - id : Cluster2-provgw-instance2
    type: PROVGW
    owner: Cluster2
    fqdn: provgw1-provgw-config2.provgw2.svc.cluster.local
    port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCncclams and aCnccs
- Https port should be updated in mCncclams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-provgw-instance1
      type: PROVGW
      owner: Cluster1
      fqdn: provgw1-provgw-config.provgw.svc.cluster.local
```

```
    port: 80
  - id : Cluster2-provgw-instance1
    type: PROVGW
    owner: Cluster2
    fqdn: provgw1-provgw-config.provgw2.svc.cluster.local
    port: 80
  - id : Cluster2-provgw-instance2
    type: PROVGW
    owner: Cluster2
    fqdn: provgw1-provgw-config2.provgw2.svc.cluster.local
    port: 80
```

> **Note**
>
> In this example local NF and A-CNCC Core is considered to be deployed in Manager Cluster, its a optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-provgw-instance1
      type: PROVGW
      owner: Cluster2
      fqdn: provgw1-provgw-config.provgw2.svc.cluster.local
      port: 80
    - id : Cluster2-provgw-instance2
      type: PROVGW
      owner: Cluster2
      fqdn: provgw1-provgw-config2.provgw2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCncclams and aCnccs
- Https port should be updated in mCncclams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-provgw-instance1
      type: PROVGW
      owner: Cluster2
      fqdn: provgw1-provgw-config.provgw2.svc.cluster.local
      port: 80
    - id : Cluster2-provgw-instance2
      type: PROVGW
      owner: Cluster2
      fqdn: provgw1-provgw-config2.provgw2.svc.cluster.local
      port: 80
```

F.1.8 SCP Instances Configuration Examples

F.1.8.1 SCP Single Cluster Deployment Instance Configuration Examples

SCP Single Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.scp.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
```

```
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.scp.svc.cluster.local
      port: 80
```

F.1.8.2 SCP Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1 and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
```

```
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.scp.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance1
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp1.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance2
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
```

```
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.scp.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance1
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp1.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance2
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp2.svc.cluster.local
      port: 80
```

> **Note**
>
> In this example local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
```

```
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-scp-instance1
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp1.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance2
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-scp-instance1
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.scp1.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance2
      type: SCP
      owner: Cluster2
```

```
    fqdn: ocscp-scpc-configuration.scp2.svc.cluster.local
    port: 80
```

F.1.9 SEPP Instances Configuration Examples

F.1.9.1 SEPP Single Cluster Deployment Instance Configuration Examples

SEPP Single Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-sepp-instance1
      type: SEPP
      owner: Cluster1
      fqdn: ocsepp-config-mgr-svc.sepp.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Core

```
global:

  oci-iam:
    enabled: false
```

```
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-sepp-instance1
      type: SEPP
      owner: Cluster1
      fqdn: ocsepp-config-mgr-svc.sepp.svc.cluster.local
      port: 80
```

F.1.9.2 SEPP Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
```

```
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-sepp-instance1
      type: SEPP
      owner: Cluster1
      fqdn: ocsepp-config-mgr-svc.sepp.svc.cluster.local
      port: 80
    - id : Cluster2-sepp-instance1
      type: SEPP
      owner: Cluster2
      fqdn: ocsepp-config-mgr-svc.sepp1.svc.cluster.local
      port: 80
    - id : Cluster2-sepp-instance2
      type: SEPP
      owner: Cluster2
      fqdn: ocsepp-config-mgr-svc.sepp2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true
 isMultiClusterDeployment: true
 # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
```

```
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-sepp-instance1
      type: SEPP
      owner: Cluster1
      fqdn: ocsepp-config-mgr-svc.sepp.svc.cluster.local
      port: 80
    - id : Cluster2-sepp-instance1
      type: SEPP
      owner: Cluster2
      fqdn: ocsepp-config-mgr-svc.sepp1.svc.cluster.local
      port: 80
    - id : Cluster2-sepp-instance2
      type: SEPP
      owner: Cluster2
      fqdn: ocsepp-config-mgr-svc.sepp2.svc.cluster.local
      port: 80
```

> **Note**
>
> In this example, the local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
```

```
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-sepp-instance1
      type: SEPP
      owner: Cluster2
      fqdn: ocsepp-config-mgr-svc.sepp1.svc.cluster.local
      port: 80
    - id : Cluster2-sepp-instance2
      type: SEPP
      owner: Cluster2
      fqdn: ocsepp-config-mgr-svc.sepp2.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-sepp-instance1
      type: SEPP
      owner: Cluster2
      fqdn: ocsepp-config-mgr-svc.sepp1.svc.cluster.local
      port: 80
    - id : Cluster2-sepp-instance2
      type: SEPP
      owner: Cluster2
```

```
    fqdn: ocsepp-config-mgr-svc.sepp2.svc.cluster.local
    port: 80
```

F.1.10 UDR Instances Configuration Examples

F.1.10.1 UDR Single Cluster Deployment Instance Configuration Examples

UDR Single Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-udr-instance1
      type: UDR-PROV
      owner: Cluster1
      fqdn: udr1-ingressgateway-prov.udr.svc.cluster.local
      port: 80
    - id : Cluster1-udr-instance1
      type: UDR-CONFIG
      owner: Cluster1
      fqdn: udr1-nudr-config.udr.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-udr-instance1
      type: UDR-PROV
      owner: Cluster1
      fqdn: udr1-ingressgateway-prov.udr.svc.cluster.local
      port: 80
    - id : Cluster1-udr-instance1
      type: UDR-CONFIG
      owner: Cluster1
      fqdn: udr1-nudr-config.udr.svc.cluster.local
      port: 80global:

 oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
```

```
 mCnccCores:
   - id: Cluster1
 aCnccs:
   - id: Cluster1
     role: Cluster1
     scheme: https
     fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
     port: 443
 instances:
   - id : Cluster1-udr-instance1
     type: UDR-PROV
     owner: Cluster1
     fqdn: udr1-ingressgateway-prov.udr.svc.cluster.local
     port: 80
   - id : Cluster1-udr-instance1
     type: UDR-CONFIG
     owner: Cluster1
     fqdn: udr1-nudr-config.udr.svc.cluster.local
     port: 80
```

F.1.10.2 UDR Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1 , A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNCC Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

 isMultiClusterDeployment: true
 # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
```

```
instances:
  - id : Cluster1-udr-instance1
    type: UDR-PROV
    owner: Cluster1
    fqdn: udr1-ingressgateway-prov.udr.svc.cluster.local
    port: 80
  - id : Cluster1-udr-instance1
    type: UDR-CONFIG
    owner: Cluster1
    fqdn: udr1-nudr-config.udr1.svc.cluster.local
    port: 80
  - id : Cluster2-udr-instance1
    type: UDR-PROV
    owner: Cluster2
    fqdn: udr1-ingressgateway-prov.udr1.svc.cluster.local
    port: 80
  - id : Cluster2-udr-instance1
    type: UDR-CONFIG
    owner: Cluster2
    fqdn: udr1-nudr-config.udr1.svc.cluster.local
    port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNCC Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
```

```
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-udr-instance1
      type: UDR-PROV
      owner: Cluster1
      fqdn: udr1-ingressgateway-prov.udr.svc.cluster.local
      port: 80
    - id : Cluster1-udr-instance1
      type: UDR-CONFIG
      owner: Cluster1
      fqdn: udr1-nudr-config.udr1.svc.cluster.local
      port: 80
    - id : Cluster2-udr-instance1
      type: UDR-PROV
      owner: Cluster2
      fqdn: udr1-ingressgateway-prov.udr1.svc.cluster.local
      port: 80
    - id : Cluster2-udr-instance1
      type: UDR-CONFIG
      owner: Cluster2
      fqdn: udr1-nudr-config.udr1.svc.cluster.local
      port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNCC Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
```

```
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-udr-instance1
      type: UDR-PROV
      owner: Cluster2
      fqdn: udr1-ingressgateway-prov.udr1.svc.cluster.local
      port: 80
    - id : Cluster2-udr-instance1
      type: UDR-CONFIG
      owner: Cluster2
      fqdn: udr1-nudr-config.udr1.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNCC Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-udr-instance1
      type: UDR-PROV
      owner: Cluster2
      fqdn: udr1-ingressgateway-prov.udr1.svc.cluster.local
      port: 80
    - id : Cluster2-udr-instance1
      type: UDR-CONFIG
      owner: Cluster2
```

```
    fqdn: udr1-nudr-config.udr1.svc.cluster.local
    port: 80
```

F.1.11 Common Service Instances Configuration Examples

F.1.11.1 Common Service Single Cluster Deployment Instance Configuration Examples

Common Service Single Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
      port: 80
  instances:
    - id: Cluster1-grafana
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
      apiPrefix: /jazz/grafana
    - id: Cluster1-kibana
      type: CS
      owner: Cluster1
      fqdn: occne-kibana.occne-infra.svc
      apiPrefix: /jazz/kibana
    - id: Cluster1-jaeger
      type: CS
      owner: Cluster1
      fqdn: occne-tracer-jaeger-query.occne-infra.svc
      apiPrefix: /jazz/jaeger
```

```
    - id: Cluster1-prometheus
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
      apiPrefix: /jazz/prometheus
    - id: Cluster1-alertmanager
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
      apiPrefix: /jazz/alertmanager
    - id: Cluster1-promxy
      type: CS
      owner: Cluster1
      fqdn: occne-promxy-apigw-nginx.occne-infra.svc
      apiPrefix: /jazz/promxy
    - id: Cluster1-opensearch
      type: CS
      owner: Cluster1
      fqdn: occne-opensearch-dashboards.occne-infra.svc
      apiPrefix: /jazz/dashboard
    - id: Cluster1-jaegeres
      type: CS
      owner: Cluster1
      fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
      apiPrefix: /jazz/esjaeger
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

 oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
```

```
    role: Cluster1
    scheme: https
    fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
    port: 443
instances:
  - id: Cluster1-grafana
    type: CS
    owner: Cluster1
    fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
    apiPrefix: /jazz/grafana
  - id: Cluster1-kibana
    type: CS
    owner: Cluster1
    fqdn: occne-kibana.occne-infra.svc
    apiPrefix: /jazz/kibana
  - id: Cluster1-jaeger
    type: CS
    owner: Cluster1
    fqdn: occne-tracer-jaeger-query.occne-infra.svc
    apiPrefix: /jazz/jaeger
  - id: Cluster1-prometheus
    type: CS
    owner: Cluster1
    fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
    apiPrefix: /jazz/prometheus
  - id: Cluster1-alertmanager
    type: CS
    owner: Cluster1
    fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
    apiPrefix: /jazz/alertmanager
  - id: Cluster1-promxy
    type: CS
    owner: Cluster1
    fqdn: occne-promxy-apigw-nginx.occne-infra.svc
    apiPrefix: /jazz/promxy
  - id: Cluster1-opensearch
    type: CS
    owner: Cluster1
    fqdn: occne-opensearch-dashboards.occne-infra.svc
    apiPrefix: /jazz/dashboard
  - id: Cluster1-jaegeres
    type: CS
    owner: Cluster1
    fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
    apiPrefix: /jazz/esjaeger
```

F.1.11.2 Common Service Multicluster Deployment Instance Configuration Examples

(M-CNCC Core on Cluster1 , A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id: Cluster1-grafana
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
      apiPrefix: /jazz/grafana
    - id: Cluster1-kibana
      type: CS
      owner: Cluster1
      fqdn: occne-kibana.occne-infra.svc
      apiPrefix: /jazz/kibana
    - id: Cluster1-jaeger
      type: CS
      owner: Cluster1
      fqdn: occne-tracer-jaeger-query.occne-infra.svc
      apiPrefix: /jazz/jaeger
    - id: Cluster1-prometheus
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
      apiPrefix: /jazz/prometheus
    - id: Cluster1-alertmanager
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
```

```
  apiPrefix: /jazz/alertmanager
- id: Cluster1-promxy
  type: CS
  owner: Cluster1
  fqdn: occne-promxy-apigw-nginx.occne-infra.svc
  apiPrefix: /jazz/promxy
- id: Cluster1-opensearch
  type: CS
  owner: Cluster1
  fqdn: occne-opensearch-dashboards.occne-infra.svc
  apiPrefix: /jazz/dashboard
- id: Cluster1-jaegeres
  type: CS
  owner: Cluster1
  fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
  apiPrefix: /jazz/esjaeger
- id: Cluster2-grafana
  type: CS
  owner: Cluster2
  fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
  apiPrefix: /rivendell-2210/grafana
- id: Cluster2-kibana
  type: CS
  owner: Cluster2
  fqdn: occne-kibana.occne-infra.svc
  apiPrefix: /rivendell-2210/kibana
- id: Cluster2-jaeger
  type: CS
  owner: Cluster2
  fqdn: occne-tracer-jaeger-query.occne-infra.svc
  apiPrefix: /rivendell-2210/jaeger
- id: Cluster2-prometheus
  type: CS
  owner: Cluster2
  fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
  apiPrefix: /rivendell-2210/prometheus
- id: Cluster2-alertmanager
  type: CS
  owner: Cluster2
  fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
  apiPrefix: /rivendell-2210/alertmanager
- id: Cluster2-promxy
  type: CS
  owner: Cluster2
  fqdn: occne-promxy-apigw-nginx.occne-infra.svc
  apiPrefix: /rivendell-2210/promxy
- id: Cluster2-opensearch
  type: CS
  owner: Cluster2
  fqdn: occne-opensearch-dashboards.occne-infra.svc
  apiPrefix: /rivendell-2210/dashboard
- id: Cluster2-jaegeres
  type: CS
  owner: Cluster2
  fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
  apiPrefix: /rivendell-2210/esjaeger
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id: Cluster1-grafana
      type: CS
      owner: Cluster1
      fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
      apiPrefix: /jazz/grafana
    - id: Cluster1-kibana
      type: CS
      owner: Cluster1
      fqdn: occne-kibana.occne-infra.svc
      apiPrefix: /jazz/kibana
    - id: Cluster1-jaeger
      type: CS
      owner: Cluster1
      fqdn: occne-tracer-jaeger-query.occne-infra.svc
      apiPrefix: /jazz/jaeger
```

```
  - id: Cluster1-prometheus
    type: CS
    owner: Cluster1
    fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
    apiPrefix: /jazz/prometheus
  - id: Cluster1-alertmanager
    type: CS
    owner: Cluster1
    fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
    apiPrefix: /jazz/alertmanager
  - id: Cluster1-promxy
    type: CS
    owner: Cluster1
    fqdn: occne-promxy-apigw-nginx.occne-infra.svc
    apiPrefix: /jazz/promxy
  - id: Cluster1-opensearch
    type: CS
    owner: Cluster1
    fqdn: occne-opensearch-dashboards.occne-infra.svc
    apiPrefix: /jazz/dashboard
  - id: Cluster1-jaegeres
    type: CS
    owner: Cluster1
    fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
    apiPrefix: /jazz/esjaeger
  - id: Cluster2-grafana
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
    apiPrefix: /rivendell-2210/grafana
  - id: Cluster2-kibana
    type: CS
    owner: Cluster2
    fqdn: occne-kibana.occne-infra.svc
    apiPrefix: /rivendell-2210/kibana
  - id: Cluster2-jaeger
    type: CS
    owner: Cluster2
    fqdn: occne-tracer-jaeger-query.occne-infra.svc
    apiPrefix: /rivendell-2210/jaeger
  - id: Cluster2-prometheus
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
    apiPrefix: /rivendell-2210/prometheus
  - id: Cluster2-alertmanager
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
    apiPrefix: /rivendell-2210/alertmanager
- id: Cluster2-promxy
  type: CS
  owner: Cluster2
  fqdn: occne-promxy-apigw-nginx.occne-infra.svc
  apiPrefix: /rivendell-2210/promxy
- id: Cluster2-opensearch
```

```
    type: CS
    owner: Cluster2
    fqdn: occne-opensearch-dashboards.occne-infra.svc
    apiPrefix: /rivendell-2210/dashboard
  - id: Cluster2-jaegeres
    type: CS
    owner: Cluster2
    fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
    apiPrefix: /rivendell-2210/esjaeger
```

> **Note**
>
> In this example, local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id: Cluster2-grafana
      type: CS
      owner: Cluster2
      fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
      apiPrefix: /rivendell-2210/grafana
    - id: Cluster2-kibana
      type: CS
      owner: Cluster2
      fqdn: occne-kibana.occne-infra.svc
      apiPrefix: /rivendell-2210/kibana
    - id: Cluster2-jaeger
      type: CS
```

```
    owner: Cluster2
    fqdn: occne-tracer-jaeger-query.occne-infra.svc
    apiPrefix: /rivendell-2210/jaeger
  - id: Cluster2-prometheus
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
    apiPrefix: /rivendell-2210/prometheus
  - id: Cluster2-alertmanager
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
    apiPrefix: /rivendell-2210/alertmanager
  - id: Cluster2-promxy
    type: CS
    owner: Cluster2
    fqdn: occne-promxy-apigw-nginx.occne-infra.svc
    apiPrefix: /rivendell-2210/promxy
  - id: Cluster2-opensearch
    type: CS
    owner: Cluster2
    fqdn: occne-opensearch-dashboards.occne-infra.svc
    apiPrefix: /rivendell-2210/dashboard
  - id: Cluster2-jaegeres
    type: CS
    owner: Cluster2
    fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
    apiPrefix: /rivendell-2210/esjaeger
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
```

```
  - id: Cluster1
aCnccs:
  - id: Cluster2
    role: Cluster2
instances:
  - id: Cluster2-grafana
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-grafana.occne-infra.svc
    apiPrefix: /rivendell-2210/grafana
  - id: Cluster2-kibana
    type: CS
    owner: Cluster2
    fqdn: occne-kibana.occne-infra.svc
    apiPrefix: /rivendell-2210/kibana
  - id: Cluster2-jaeger
    type: CS
    owner: Cluster2
    fqdn: occne-tracer-jaeger-query.occne-infra.svc
    apiPrefix: /rivendell-2210/jaeger
  - id: Cluster2-prometheus
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-kube-prometheus.occne-infra.svc
    apiPrefix: /rivendell-2210/prometheus
  - id: Cluster2-alertmanager
    type: CS
    owner: Cluster2
    fqdn: occne-kube-prom-stack-kube-alertmanager.occne-infra.svc
    apiPrefix: /rivendell-2210/alertmanager
  - id: Cluster2-promxy
    type: CS
    owner: Cluster2
    fqdn: occne-promxy-apigw-nginx.occne-infra.svc
    apiPrefix: /rivendell-2210/promxy
  - id: Cluster2-opensearch
    type: CS
    owner: Cluster2
    fqdn: occne-opensearch-dashboards.occne-infra.svc
    apiPrefix: /rivendell-2210/dashboard
  - id: Cluster2-jaegeres
    type: CS
    owner: Cluster2
    fqdn: occne-tracer-elasticsearch-jaeger-query.occne-infra.svc
    apiPrefix: /rivendell-2210/esjaeger
```

F.1.12 CNC Console Instances Configuration With cnDBTier Menu Enabled

F.1.12.1 CNC Console Single-Cluster Configuration with cnDBTier Menu Enabled

CNC Console Core

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-cncc-instance1
      type: CNCC
      owner: Cluster1
    - id : Cluster1-cncc-instance1
      type: DBTIER
      owner: Cluster1
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-cncc-instance1
      type: CNCC
      owner: Cluster1
    - id : Cluster1-cncc-instance1
      type: DBTIER
      owner: Cluster1
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

F.1.12.2 CNC Console Multicluster Configuration with cnDBTier Menu Enabled

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Core (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
```

```
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-cncc-instance1
      type: CNCC
      owner: Cluster1
    - id : Cluster1-cncc-instance1
      type: DBTIER
      owner: Cluster1
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
    - id : Cluster2-cncc-instance1
      type: CNCC
      owner: Cluster2
    - id : Cluster2-cncc-instance1
      type: DBTIER
      owner: Cluster2
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true
```

```
  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-cncc-instance1
      type: CNCC
      owner: Cluster1
    - id : Cluster1-cncc-instance1
      type: DBTIER
      owner: Cluster1
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
    - id : Cluster2-cncc-instance1
      type: CNCC
      owner: Cluster2
    - id : Cluster2-cncc-instance1
      type: DBTIER
      owner: Cluster2
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core is considered to be deployed in Manager Cluster, its an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
```

```
mcncc-core:
  enabled: false
acncc-core:
  enabled: true

isMultiClusterDeployment: true
# Automatic route generation for CNCC Agent Deployment
self:
  cnccId: Cluster2
mCnccIams:
  - id: Cluster1
    ip: 10.xx.xx.xx
mCnccCores:
  - id: Cluster1
aCnccs:
  - id: Cluster2
    role: Cluster2
instances:
  - id : Cluster2-cncc-instance1
    type: CNCC
    owner: Cluster2
  - id : Cluster2-cncc-instance1
    type: DBTIER
    owner: Cluster2
    fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
    port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
```

```
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-cncc-instance1
      type: CNCC
      owner: Cluster2
    - id : Cluster2-cncc-instance1
      type: DBTIER
      owner: Cluster2
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

F.1.13 OCCM Instance Configuration Examples

F.1.13.1 OCCM Single Cluster Configuration

OCCM Single Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-occm-instance1
      type: OCCM
      owner: Cluster1
      fqdn: occm.occm.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-occm-instance1
      type: OCCM
      owner: Cluster1
      fqdn: occm.occm.svc.cluster.local
      port: 80
```

F.1.13.2 OCCM Multicluster Configuration

(M-CNCC Core on Cluster1 , A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
```

```
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-occm-instance1
      type: OCCM
      owner: Cluster1
      fqdn: occm.occm.svc.cluster.local
      port: 80
    - id : Cluster2-occm-instance1
      type: OCCM
      owner: Cluster2
      fqdn: occm.occm.svc.cluster.local
      port: 80
    - id : Cluster2-occm-instance2
      type: OCCM
      owner: Cluster2
      fqdn: occm.occm.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNCC Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true
```

```
isMultiClusterDeployment: true
# Automatic route generation for CNCC Manager Deployment
 self:
   cnccId: Cluster1
 mCnccIams:
   - id: Cluster1
     scheme: https
     ip: 10.xx.xx.xx
 mCnccCores:
   - id: Cluster1
 aCnccs:
   - id: Cluster1
     role: Cluster1
     scheme: https
     fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
     port: 443
   - id: Cluster2
     role: Cluster2
     scheme: https
     ip: 10.xx.xx.xx
     port: 443
 instances:
   - id : Cluster1-occm-instance1
     type: OCCM
     owner: Cluster1
     fqdn: occm.occm.svc.cluster.local
     port: 80
   - id : Cluster2-ocm-instance1
     type: OCCM
     owner: Cluster2
     fqdn: occm.occm.svc.cluster.local
     port: 80
   - id : Cluster2-occm-instance2
     type: OCCM
     owner: Cluster2
     fqdn: occm.occm.svc.cluster.local
     port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNCC Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
```

```
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-occm-instance1
      type: OCCM
      owner: Cluster2
      fqdn: occm.occm.svc.cluster.local
      port: 80
    - id : Cluster2-occm-instance2
      type: OCCM
      owner: Cluster2
      fqdn: occm.occm.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNCC Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
```

```
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-occm-instance1
      type: OCCM
      owner: Cluster2
      fqdn: occm.occm.svc.cluster.local
      port: 80
    - id : Cluster2-occm-instance2
      type: OCCM
      owner: Cluster2
      fqdn: occm.occm.svc.cluster.local
      port: 80
```

F.1.14 NEF Instance Configuration Examples

F.1.14.1 NEF Single Cluster Configuration

NEF Single Cluster Configuration

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
  instances:
    - id : Cluster1-nef-instance1
      type: NEF
      owner: Cluster1
```

```
    fqdn: ocnef-consoledataservice.nef.svc.cluster.local
    port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-nef-instance1
      type: NEF
      owner: Cluster1
      fqdn: ocnef-consoledataservice.nef.svc.cluster.local
      port: 80
```

F.1.14.2 NEF Multicluster Configuration

(M-CNCC Core on Cluster1 , A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
```

```
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-nef-instance1
      type: NEF
      owner: Cluster1
      fqdn: ocnef-consoledataservice.nef.svc.cluster.local
      port: 80
    - id : Cluster2-nef-instance1
      type: NEF
      owner: Cluster2
      fqdn: ocnef-consoledataservice.nef.svc.cluster.local
      port: 80
    - id : Cluster2-nef-instance2
      type: NEF
      owner: Cluster2
      fqdn: ocnef-consoledataservice.nef.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNCC Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
```

```
 acncc-core:
   enabled: true

isMultiClusterDeployment: true
# Automatic route generation for CNCC Manager Deployment
 self:
   cnccId: Cluster1
 mCnccIams:
   - id: Cluster1
     scheme: https
     ip: 10.xx.xx.xx
 mCnccCores:
   - id: Cluster1
 aCnccs:
   - id: Cluster1
     role: Cluster1
     scheme: https
     fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
     port: 443
   - id: Cluster2
     role: Cluster2
     scheme: https
     ip: 10.xx.xx.xx
     port: 443
 instances:
   - id : Cluster1-nef-instance1
     type: NEF
     owner: Cluster1
     fqdn: ocnef-consoledataservice.nef.svc.cluster.local
     port: 80
   - id : Cluster2-nef-instance1
     type: NEF
     owner: Cluster2
     fqdn: ocnef-consoledataservice.nef.svc.cluster.local
     port: 80
   - id : Cluster2-nef-instance2
     type: NEF
     owner: Cluster2
     fqdn: ocnef-consoledataservice.nef.svc.cluster.local
     port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core are considered to be deployed in Manager Cluster, it is an optional configuration.

CNCC Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
```

```
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-nef-instance1
      type: NEF
      owner: Cluster2
      fqdn: ocnef-consoledataservice.nef.svc.cluster.local
      port: 80
    - id : Cluster2-nef-instance2
      type: NEF
      owner: Cluster2
      fqdn: ocnef-consoledataservice.nef.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNCC Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
```

```
mCnccCores:
  - id: Cluster1
aCnccs:
  - id: Cluster2
    role: Cluster2
instances:
  - id : Cluster2-nef-instance1
    type: NEF
    owner: Cluster2
    fqdn: ocnef-consoledataservice.nef.svc.cluster.local
    port: 80
  - id : Cluster2-nef-instance2
    type: NEF
    owner: Cluster2
    fqdn: ocnef-consoledataservice.nef.svc.cluster.local
    port: 80
```

F.1.15 NF Instance Configuration With cnDBTier Menu Enabled

F.1.15.1 NF Single Cluster Configuration With cnDBTier Menu Enabled

NF instance configuration should include DBTIER instance configuration to enable DBTIER menu items for NF.

Here is the example for SCP instance configuration. Similar configuration should be performed for other NFs.

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 80
```

```
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
      port: 80
    - id : Cluster1-scp-instance1
      type: DBTIER
      owner: Cluster1
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: false
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.cluster.local
      port: 443
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
      port: 80
    - id : Cluster1-scp-instance1
      type: DBTIER
      owner: Cluster1
```

```
    fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
    port: 80
```

F.1.15.2 NF Multicluster Configuration With cnDBTier Menu Enabled

(M-CNCC Core on Cluster1, A-CNCC Core on Cluster1, and A-CNCC Core on Cluster2)

CNC Console Core (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
      port: 80
    - id: Cluster2
      role: Cluster2
      ip: 10.xx.xx.xx
      port: 80
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
      port: 80
    - id : Cluster1-scp-instance1
      type: DBTIER
      owner: Cluster1
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance1
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance1
```

```
      type: DBTIER
      owner: Cluster2
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Manager Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: true
  mcncc-core:
    enabled: true
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Manager Deployment
  self:
    cnccId: Cluster1
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster1
      role: Cluster1
      scheme: https
      fqdn: cncc-acore-ingress-gateway.cncc.svc.jazz
      port: 443
    - id: Cluster2
      role: Cluster2
      scheme: https
      ip: 10.xx.xx.xx
      port: 443
  instances:
    - id : Cluster1-scp-instance1
      type: SCP
      owner: Cluster1
      fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
      port: 80
    - id : Cluster1-scp-instance1
      type: DBTIER
      owner: Cluster1
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance1
```

```
    type: SCP
    owner: Cluster2
    fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
    port: 80
  - id : Cluster2-scp-instance1
    type: DBTIER
    owner: Cluster2
    fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
    port: 80
```

> **Note**
>
> In this example, local NF and A-CNCC Core is considered to be deployed in Manager Cluster, its an optional configuration.

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-scp-instance1
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance1
      type: DBTIER
      owner: Cluster2
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

Sample Configuration for HTTPS enabled deployment

- Scheme should be updated to "https" in mCnccIams and aCnccs
- Https port should be updated in mCnccIams and aCnccs

CNC Console Configuration (Agent Cluster)

```
global:

  oci-iam:
    enabled: false
  cncc-iam:
    enabled: false
  mcncc-core:
    enabled: false
  acncc-core:
    enabled: true

  isMultiClusterDeployment: true
  # Automatic route generation for CNCC Agent Deployment
  self:
    cnccId: Cluster2
  mCnccIams:
    - id: Cluster1
      scheme: https
      ip: 10.xx.xx.xx
  mCnccCores:
    - id: Cluster1
  aCnccs:
    - id: Cluster2
      role: Cluster2
  instances:
    - id : Cluster2-scp-instance1
      type: SCP
      owner: Cluster2
      fqdn: ocscp-scpc-configuration.ocscp.svc.cluster.local
      port: 80
    - id : Cluster2-scp-instance1
      type: DBTIER
      owner: Cluster2
      fqdn: mysql-cluster-db-monitor-svc.cndbtier.svc.cluster.local
      port: 80
```

G.1 Fault Recovery Procedures - DB Backup and Restore

Introduction

This section describes the backup and restore procedures specific to CNC Console. The instructions are for the operator to take CNC Console database's backup and restore the database on a different cluster. These instructions can be used for Fault Recovery of Console and are part of the Fault Recovery guide.

The commands used for these procedures are given by the MySQL NDB Cluster.

Prerequisite

See the **Preupgrade Tasks** and Pre-rollback Tasks sections before performing backup or restore procedure.

Backup Procedure

CNC Console Database Backup
If the Console database backup is required, do the following:

Periodically keep baking up CNC Console Database using the DB backup procedure and store it. For more information see CNC Console IAM DB Backup .

CNC Console Deployment Backup

- Keep a backup of the *occncc_custom_values_<version>.yaml* file that was used for last installation or upgrade of Console.
- Docker images used during the last installation or upgrade must be retained in the external data source.

Restore Procedure

CNC Console Database Restore

> **Note**
>
> Not applicable for OCI deployment.

Follow restore procedure mentioned in the M-CNCC IAM DB Rollback or Restore section.

CNC Console Deployment Restore

To restore the CNC Console Deployment:

- Run the following command to uninstall the existing CNC Console deployment (if needed)

  ```
  helm uninstall <deployment name> --namespace <deployment namespace>
  ```

  For example:

  ```
  helm uninstall cncc --namespace cncc
  ```

- Use the backed up copy of *occncc_custom_values_<version>.yaml* file, taken as part of CNC Console custom_values.yaml Backup to install the CNC Console.

H.1 Restoring CNC Console

Perform this procedure to restore CNC Console.

Prerequisites:

- Take a backup of the `occncc_custom_values_<version>.yaml` file that was used for installing CNC Console.
- Take a backup of the CNC Console database and restore the database as described in Fault Recovery Procedures - DB Backup and Restore section.

Corruption in CNC Console Deployment

This section describes how to recover the CNC Console when the deployment is corrupted.

Console Deployment Corruption

If Console deployment is corrupted, do the following:

1. Run the following command to uninstall the corrupted CNCC deployment deployment:

   ```
   helm uninstall <deployment name> --namespace <namespace>
   ```

   Where,

   - `<deployment name>` is a name used to track this installation instance.

   Example:

   ```
   helm uninstall cncc --namespace cncc
   ```

2. Install Console using the backed up copy of the `occncc_custom_values_<version>.yaml` file.
   For information about installing CNC Console using Helm, see *Oracle Communication Cloud Native Configuration Console Installation and Upgrade Guide*.