Oracle® Communications Application Orchestrator

User Guide
Release 1.1

August 2016

Notices

Contents

About This Guide

This document and other product-related documents are described in the Related Documentation table.

Related Documentation

Table 1: Oracle Communications Application Orchestrator Library

Document Name	Document Description
Release Notes	Contains feature support information, and known issues pertaining to this release.
Installation Guide	Contains instructions for installing Oracle Communications Application Orchestrator as a standalone application or installing Oracle Communications Application Orchestrator together with Oracle Communications Session Delivery Manager.
Plug-in Guide for Session Delivery Network Elements	Describes how to use Oracle session delivery product plug-ins with Oracle Communications Application Orchestrator.
User Guide	Describes how to centrally manage and automate your virtual and physical network environment of composite network functions (CNFs). The Oracle Communications Application Orchestrator application is implemented by doing the following: • Use the Security Manager to create new users and new user groups, and set group-based authorization. • Configure X.509 certificate authentication. • Add a virtual infrastructure management (VIM) system to manage VNF life-cycles. • Register an Element Manager (EM) with Oracle Communications Application Orchestrator in order to stage a CNF from its CNF descriptor (CNFD). • Manually use the CNF onboarding workflow to choose, stage, and promote a pre-existing CNF plug-in, and configure the CNF to deploy and make this CNF operational. • Automate the manual process of making a CNF operational by using the hierarchical service configuration (HSC) feature. • Monitor Oracle Communications Application Orchestrator real-time KPI thresholds, device status and performance information for CNFs. • Use the Fault Manager to view events, alarms and trap event settings.
REST API Guide	The Oracle Communications Application Orchestrator REST API interface interacts with the Northbound Interface (NBI) to get the available fault alarms.
Security Guide	Provides the following security guidelines and topics: • Guidelines for performing a secure installation of Oracle Communications Application Orchestrator on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines. • An overview of the Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system.

Document Name	Document Description
	• Security maintenance, which includes a checklist to securely deploy Oracle Communications Application Orchestrator on your network, maintaining security updates, and security considerations for developers.

Revision History

Date	Description
August 2015	• Initial release
April 2016	• The *Customize the Display* and *Application Orchestrator Standard Scaling Policy* sections were added to the *Overview* chapter. • The *Application Orchestrator Parts* section was updated with new HSC-related terms in the *Overview* chapter. • New steps were added to the *Implementing Application Orchestrator on Your Network* section in the *Application Orchestrator Implementation* chapter for the EM Registry and HSC features. • The *Configure External User Authentication* section was improved and the *Configure an Active Directory Domain Controller* section in the *Security Manager* chapter was updated to remove Kerberos authentication protocol choice 2 (Kerberos realm field). The Kerberos protocol can authenticate a user by specifying an existing krb5.conf file only. • Updated the *Configure a RADIUS Server* section in the *Security Manager* chapter to add information about adding an external group name to a local group. • The *Add and Map a Local User Group to an External Domain User Group* section was added to the Security Manager chapter. • The *Apply User Group Privileges for Applications* section in the *Security Manager* chapter was updated to add new HSC configuration folder privileges for a user group. • The *Add Data Center to Oracle OpenStack VIM* and *Add Data Center to VMware vCloud Director VIM* sections in the *Configure a VIM for Application Orchestrator* chapter were updated with a new **Caution** field that contains important configuration information. • The *Register an Element Manager with Application Orchestrator* chapter was added. • The *Configure the CNF* chapter was renamed to *Operationalize a CNF Manually* and the *Configuring an Element Manager* section was removed from this chapter.

Date	Description
	- The *Build the Hierarchical Service Configuration* chapter was added. - The *Synchronize an External Trap Receiver to Validate the Health of a Device* and *Add the Heartbeat Trap to Monitor Server Availability* sections were added to the Fault Manager chapter. - The *Add the Heartbeat Trap to Monitor Server Availability* section was added to the *Fault Manager* chapter. - The *Guidelines for Provisioning Oracle OpenStack* section in *Appendix A: Guidelines for Provisioning Your VIM* was updated with Oracle OpenStack 2.0 information and a new subsection *OpenStack Configuration Drive Requirements and Guidelines*.
August 2016	- The *Application Orchestrator X.509 Certificate Authentication* chapter name was changed to *Certificate Authentication*. The *Upload a New X.509 Certificate to Application Orchestrator* section in this chapter was changed to *Upload a New Certificate* and the *Delete an Existing Certificate from Application Orchestrator* was changed to *Delete an Existing Certificate*.

1

Overview

Oracle Communications Application Orchestrator provides a core management platform for communications service providers (CSPs). This platform supports a composite network function (CNF) that can be any combination of a virtualized network function (VNF) and physical network function (PNF) that runs as part of a network to provide one or more public, private, or hybrid cloud computing solutions.

When Oracle Communications Application Orchestrator starts a CNF, it constructs the CNF topology and deploys the CNF automatically. The following figure shows a simplified diagram for how Oracle Communications Application Orchestrator fits into the infrastructure of a network management environment.

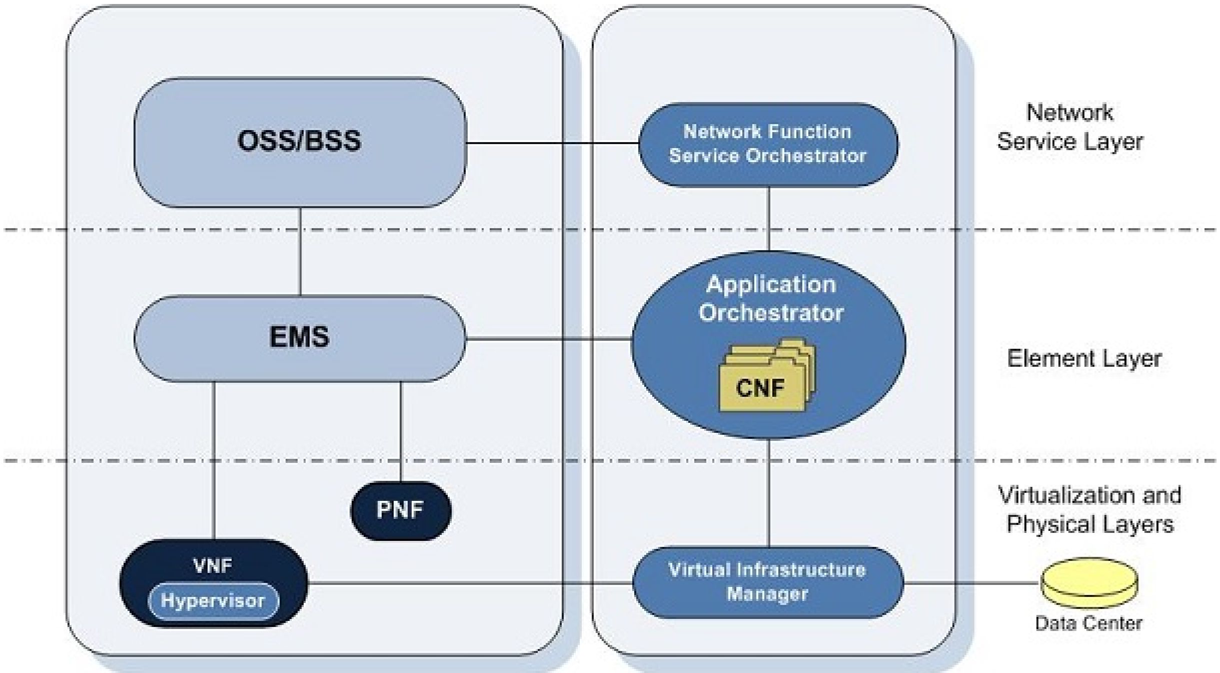

OSS/BSS
Network Function Service Orchestrator
Network Service Layer
EMS
Application Orchestrator
CNF
Element Layer
PNF
Virtualization and Physical Layers
VNF
Hypervisor
Virtual Infrastructure Manager
Data Center

Figure 1: Oracle Communications Application Orchestrator in the network

CSPs use Oracle Communications Application Orchestrator to deploy CNFs on their networks for the following reasons:

- Portability—Pre-existing CNFs can be imported or exported to a virtual network platform.

- Dynamic—Cloud resources can be dynamically and automatically scaled to maintain network capacity requirements. This is accomplished by enabling elasticity mode, which calculates device thresholds on key performance indicator (KPI) metrics.
- Centralized Provisioning—Network functions (NFs) can be provisioned automatically or manually to meet virtual and physical device demands.
- Cost-effective—Supports both virtual and physical network functions through a single CNF. CNFs can be deployed automatically within minutes across a network topology that spans disbursed geographical areas, avoiding the costly manual deployment of Network Functions (NFs).
- Reporting—Performance information can be collected from actively deployed VM instances.

Application Orchestrator Support for Network Functions

Oracle Communications Application Orchestrator supports NFs through work flows that interact and collaborate with virtual infrastructure manager (VIM) systems (for example, Oracle OpenStack or vCloud Director), element managers (for example, Oracle Communications Session Element Manager), and network service orchestrators (NSOs) (for example, Oracle Communications Network Service orchestrator).

Oracle Communications Application Orchestrator supports NFs in the following ways:

- Reinforces the management life cycle of an NF running on VM and physical appliances.
- Supports service agility and dynamic capacity adjustment through elastic, automated control of the network function component (NFc) instances.
- Supports the specified European Telecommunications Standards Institute Management and Orchestration (ETSI MANO) requirement for a VNF manager and extends this model to service all applications that have a virtual or physical presence.
- Provides capacity planners and monitoring capabilities to a self-assess the capacity requirement over the life time of the NF.
- Provides a plug-in platform for all Oracle Communications Global Business (OCGBU) network elements and third-party NE vendors. NE domain knowledge is abstracted for the specific plug-in.
- Supports multiple VIM vendors for managing storage, compute, and network requirements.
- Provides security access to external systems for collaboration through secure HTTP and HTTPS.

About the Application Orchestrator Installation

This section briefly describes the Oracle Communications Application Orchestrator installation scenarios.

When you install the software package that includes Oracle Communications Application Orchestrator, the following setup application appears:

```
Select a product:
[X]  1 - ALL                OCAO+OCSDM   [Default]
[ ]  2 - OCSDM mode         Session Delivery Manager
[ ]  3 - OCAO mode          Application Orchestrator

Please select an option [1]
```

Each installation option that you can select for your system is described below:

- **`ALL`**—Installs both Application Orchestrator (standalone only) and Session Delivery Manager. Oracle Communications Application Orchestrator (standalone only) and *Oracle Communications Session Delivery Manager* (default).

  Note: Oracle Communications Application Orchestrator can only run as a standalone server; clustering is not yet supported.

  Once the installation is complete, the **Application Orchestrator** slider appears with the *Oracle Communications Session Delivery Manager* navigation sliders as shown in the figure below:

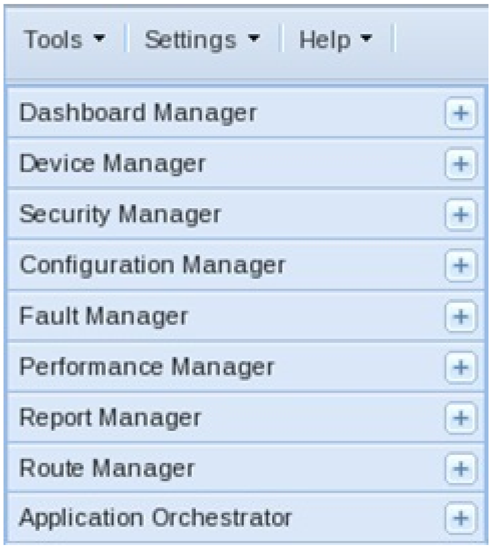


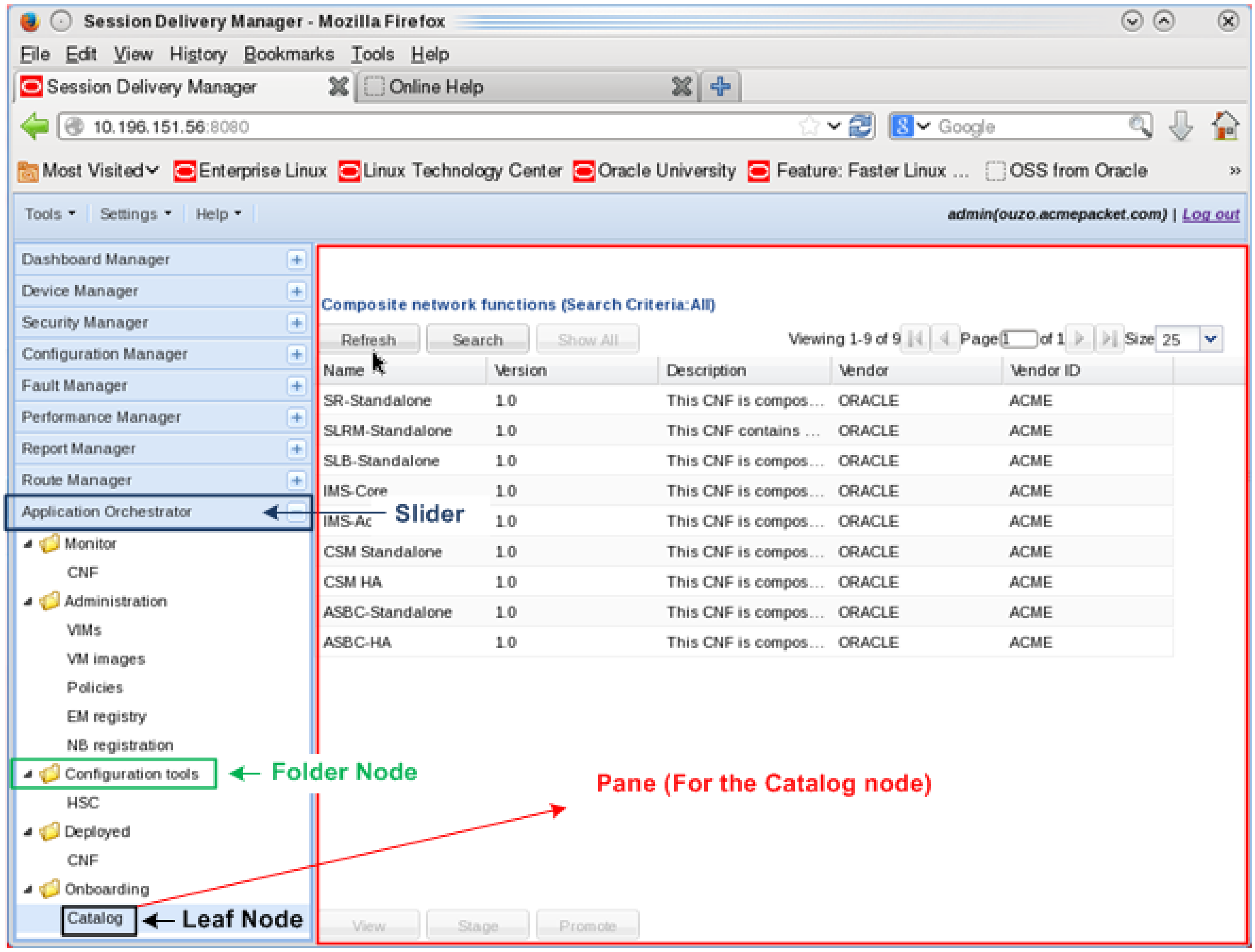
Figure 2: Session Delivery Manager with Application Orchestrator

- `OCSDM mode`—Installs the Oracle Communications Session Delivery Manager (including Oracle Communications Session Element Manager) only.
- `OCAO mode`—Installs Oracle Communications Application Orchestrator only (standalone). In this configuration scenario, the **Security manager**, **Fault manager** and **Application Orchestrator** sliders are provided only. All other sliders are not available.

Note: See the Oracle Communications Application Orchestrator Installation Guide, Release 1.1 for more detailed installation information.

Application Orchestrator Navigation

Once the Oracle Communications Application Orchestrator server starts, you can point your web browser to the server. Once you are logged in, the following page appears in your browser as shown in the following figure. This example shows an implementation scenario in which Oracle Communications Application Orchestrator is installed with *Oracle Communications Session Delivery Manager*.



Composite network functions (Search Criteria:All)

Name	Version	Description	Vendor	Vendor ID
SR-Standalone	1.0	This CNF is compos...	ORACLE	ACME
SLRM-Standalone	1.0	This CNF contains ...	ORACLE	ACME
SLB-Standalone	1.0	This CNF is compos...	ORACLE	ACME
IMS-Core	1.0	This CNF is compos...	ORACLE	ACME
IMS-Ac	1.0	This CNF is compos...	ORACLE	ACME
CSM Standalone	1.0	This CNF is compos...	ORACLE	ACME
CSM HA	1.0	This CNF is compos...	ORACLE	ACME
ASBC-Standalone	1.0	This CNF is compos...	ORACLE	ACME
ASBC-HA	1.0	This CNF is compos...	ORACLE	ACME

Figure 3: Oracle Communications Application Orchestrator Page Attributes

Expand the **Application Orchestrator** slider to display the folder and leaf node(s) described in the following table.

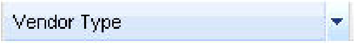
Name	Description
Monitor folder node	Click to expand the folder node and choose from the following leaf nodes to display CNF statistics: • Click **CNF** to view how Composite Network Function (CNF) groups scale either manually or automatically. Oracle Communications Application Orchestrator has a capacity planner that actively reports the capacity state of network function (NF) group(s) within a CNF. The capacity state is reported even if the NF group scales manually. This information helps administrators make resource decisions for these NF groups.
Administration folder node	Click to expand the folder node and choose from the following leaf nodes to configure Oracle Communications Application Orchestrator functional operations:

Name	Description
	• Click the **VIMs** node to add and save all of the access credentials required for the Oracle Communications Application Orchestrator to interact with a virtual infrastructure manager (VIM). • Click the **VM Images** node to manage VM application images used by Oracle Communications Application Orchestrator to initiate a network function (NF) on a VM. • Click the **Policies** node to manage administration policies for Oracle Communications Application Orchestrator.
Deployed folder node	Click to expand the folder node and click the **CNF** leaf node to view pre-deployed, deployed and active CNF table. Detailed views of a CNF can be accessed to modify CNF policies and minor parameters and enter parameters for deploying a CNF. The life cycle of a CNF is managed by the features provided in the deployed CNF node.
Onboarding folder node	Click to expand the folder node and click **Catalog** leaf node to view pre-existing CNFs provided by each registered CNF plug-in. A pre-existing CNF can be staged for sizing and resource usage and deploy the CNF so it is promoted and displayed in the **Deployed CNF** table in the **Deployed** > **CNF** slider and node mentioned above.

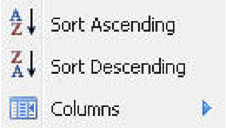
Customize the Display

Depending on the features that you use in the Oracle Communications Application Orchestrator GUI, you can customize the way in which information is displayed by customizing the way table columns are displayed and table entries are ordered. You can also customize the number of records that are displayed per page.

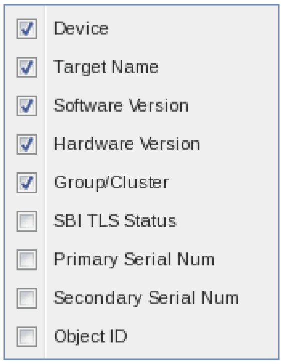
1. Position the cursor over a column heading. An arrow appears on the right hand side of the box. For example:



2. Click the down arrow to display the menu. For example:



3. Select **Sort Ascending** to sort the data in ascending order or **Sort Descending** to sort the data in descending order.
4. Select **Columns** to access a list of column names. For example:

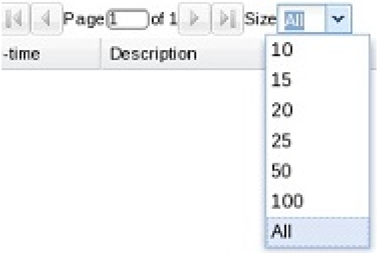


☑ Device
☑ Target Name
☑ Software Version
☑ Hardware Version
☑ Group/Cluster
□ SBI TLS Status
□ Primary Serial Num
□ Secondary Serial Num
□ Object ID

5. Click a marked checkbox to hide that column or click an empty checkbox to display that column. The display view automatically updates.

6. To display a page of records that you want to view, you can use the buttons to move between pages or enter the page number you want.
7. To customize the number of records that are displayed per page, click the **Size** drop-down list.

   Note: If you cannot sort table columns using the **Sort Ascending** or **Descending** column options, select the **All** option from the **Size** drop-down list in order to use these column options. For example, the **All** option appears in the **Size** drop-down list when you load a device in Configuration Manager to display records for the **local-policy** configuration element. If you are having trouble sorting the column order for this configuration element, use the **All** option and try again.



8. Click elsewhere in the display to clear the menus.

Application Orchestrator Parts

Virtual Infrastructure Manager

A virtual infrastructure manager (VIM) is an orchestration engine through which the Oracle Communications Application Orchestrator configures and modifies VM data center instances so that they can be automatically deployed in the virtualization infrastructure. A VIM can be a vendor application such as VMware vCloud Director or Oracle OpenStack that manages the data center.

Data Center

In Oracle Communications Application Orchestrator, a data center is a logical VM instance description of a module that maintains storage, compute, network component functions that is mapped to a VIM.

Composite Network Function

A Composite Network Function (CNF) is a type of network function introduced to extend the infrastructure of a network to support and manage both physical and virtual components together as a single hybrid solution.

A CNF that is composed of all virtual components fits the limited European Telecommunications Standards Institute Management and Orchestration (ETSI MANO) definition of a complex VNF. However, a CNF extends this definition to support physical components. A CNF contains the following parts: NF group, deployment unit (DU), VNF and PNF.

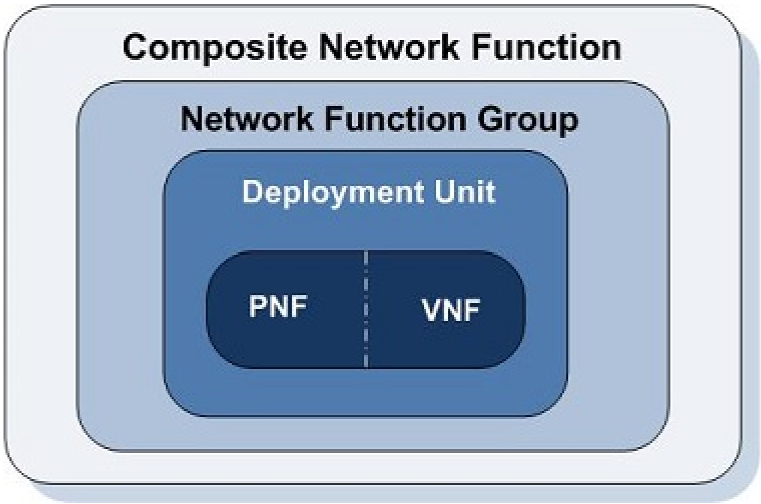


Figure 4: Composite network function and its contents

Network Function Group

The NF Group is the heart of the PNF and VNF scaling and management system of any combination of virtual network functions (VNFs) or physical network functions (PNFs) that comprise a CNF. It provides the monitor, capacity planner, and policies that cater to the specifics of the NF component that it is entrusted to manage. The NF group can only manage one NF component and adopts the sameness policies that provide for maintaining the life-cycle of the component even in a elasticity environment. The NF component can manage NFs that are either deployed on physical appliances or virtual machines (VMs).

The NF group maintains all VM or physical instances which share identical policies, rules, and a common software image. The NF group maintains a one-to-one relationship with its parent CNF, however the CNF maintains a one-to-many relationship with its child NF groups.

NF groups have the following properties:

- Abstracts a VIM— Uses an abstracted container to hide VIM characteristics.
- Network association— Ensures PNFs and VNFs are linked to required networks.
- Data center association—Can span multiple data centers. NF groups that span multiple data centers must have GeoRedundant policies.
- Self-Governing— Maintains a logical group of VM or physical components that subscribe to a set of rules and policies. While a foreign agent can make requests changing these rules, the NF group makes the final decision in a deterministic way. This includes changes to rules, policies, and reconciliation of requests to scale in or out (horizontal scaling). NF groups can scale up and down independent of other NF groups.
- Capacity Monitoring— Provides a method for monitoring based on key performance indicators (KPIs).
- Capacity Planner—Provides the ability to determine the capacity needs of the NF group NF components and also manages the required scaling requirements.
- Bootstrapping— Shares a common set of properties that are fed to the boot loaders of individual VNFs.

Deployment Unit

A DU defines a single unit instance that is dependent on the required topology policies. For example, a DU can be defined for an HA pair consisting of either two VNFs or two PNFs. A DU instance can be either a VDU that manages VM instances, or a PDU that manages physical devices. A DU acts as a sub-component in an NF deployment that can have a one-to-many relationship with a virtual (NFVM) and physical device.

Oracle Communications Application Orchestrator scales in and out NF component instances within the confines of a DU. For example, if a DU is high availability (one VM is in an active state and the other VM is in a standby state) and have geo-redundant topologies (the same active and standby VMs that are on a virtual data center that is not co-located), then the Oracle Communications Application Orchestrator scales out an event to deploy one complete DU that in turn creates and deploys four VMs. The figure below displays an NF group composed of two DUs with an HA topology resilience policy.

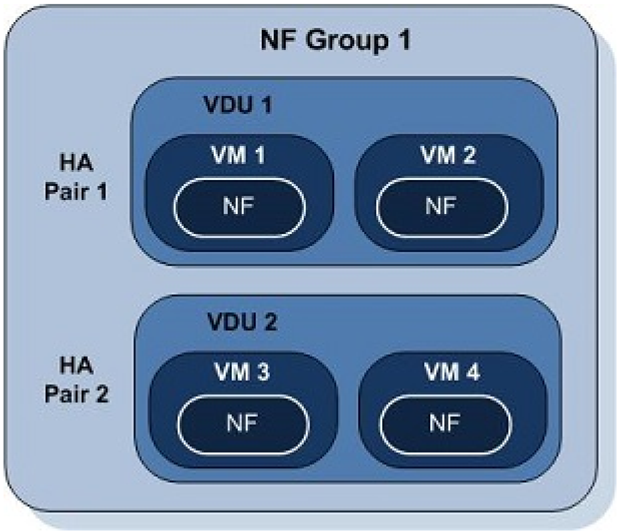


Figure 5: DUs in an HA pair

Virtual Deployment Unit

A VDU manages one or more VM instances.

Physical Deployment Unit

A PDU maintains a one-to-many relationship with physical appliances. For example, a PDU for a high availability pair of appliances consists of two PNFs.

Physical Network Function

A PNF represents the physical appliance. It is a base unit and is indivisible.

Figure 6: PNF Example

Virtual Network Function

The VNF is defined by the European Telecommunications Standards Institute of Management and Orchestration Organization (ESTI-MANO) as being comprised of one virtual network function component (VNFC) instance or multiple VNFC instances. Multiple VNFC instances can each contain multiple VMs. Oracle Communications Application Orchestrator handles either single VNFC instance or multiple VNFC instances as a single, complex VNF, which is managed by the CNF. Oracle Communications Application Orchestrator handles either a single VNFC or multiple VNFCs as a single, seamless VNF.

Virtual Machine

A VM is the software implementation of a machine (for example, a computer) that executes programs like a physical machine. The VM runs on a hypervisor and vSwitch and its operating system is installed and configured by the VIM. An NF application that runs on a single VM instance is described as a network function on a virtual machine (NFVM). An NFVM is considered to be a VNF only if it can be classified as a single VNFC VM instance.

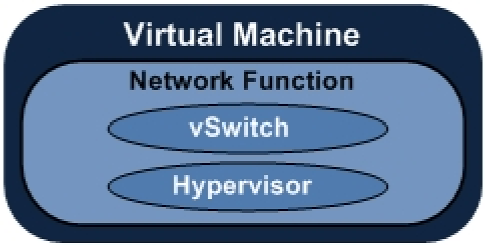


Figure 7: NFVM Running on a VM Example

Network Function

An network function (NF) is a network software application that runs on either VMs or physical devices.

Open Virtualization Appliance or Application

An OVA image package is added (uploaded) to Oracle Communications Application Orchestrator. The VIM can initiate this application on a VM when the application needs to be started.

Composite Network Function plug-in

A CNF plug-in is part of the internal infrastructure of the Oracle Communications Application Orchestrator used so that different technology vendors can onboard their specific CNF. These plug-ins provide additional pre-existing CNFs that are dependent on specified vendor NF requirements. Oracle Communications Application Orchestrator includes default plug-ins for Oracle Session Delivery Products. Additional plug-ins requests can be made to Oracle. See the *Plug-in Guide for Oracle Communications Application Orchestrator Session Delivery Network Elements* for more information.

Element Manager System

The Oracle Communications Application Orchestrator can integrate with element manager systems (EMSs), such as *Oracle Communications Session Delivery Manager Element Manager*, which provides configuration, loading and provisioning capabilities for devices, and performance management for session delivery infrastructure elements. It is the collaboration between the EMS and Oracle Communications Application Orchestrator that provides life cycle support for NF and their configurations. Any Element Manager can be provided by way of a CNF plug-in.

Notification Message

The Oracle Communications Application Orchestrator publishes notification messages (NM) when an event occurs. NM messages are published for scaling events such as scaling out or in of components. Each NM has a unique name that identifies the content of the message to the destination receiver. It is the responsibility of the targeted destination receiver to understand and interpret the contents within the message body. Therefore, the destination receiver can in certain circumstances provide the NM names that it supports. For more information on how this is accomplished, refer to the specific vendor plug-in that supports the NF in which you are interested.

Operations Support Systems and Business Support Systems

Operations support systems (OSS) are devices used by communications service providers (CSPs) to manage their networks in order to support management functions such as network inventory, service provisioning, network configuration and fault management. OSS and business support systems (BSS) are paired together so that they can support various end-to-end telecommunication services. However, these systems have different data and service responsibilities.

Northbound Service Orchestrator

A northbound service orchestrator (NSO), such as the Oracle Communications Network Service Orchestrator, manages complex cross-domain (system, enterprise, firewall) processes. The NSO can connect access Oracle Communications Application Orchestrator through the Oracle Communications Application Orchestrator REST API.

Fault Management

Oracle Communications Application Orchestrator provides a fault management system that provides management and reporting capabilities for events and alarms.

Key Performance Indicator

KPIs are used to monitor the health of the NF. These statistics are also used by capacity planners to determine overall capacity of the NF groups. The KPIs are dependent on the NF component type being monitored. Oracle Communications Application Orchestrator uses this information to determine how an NF group scales vertically or horizontally when maximized.

Capacity Planner

A capacity planner is used to determine overall capacity of the NF groups. A capacity planner is assigned to each NF group to process KPI statistics that determine whether to scale in or scale out DU instances. The capacity planner uses the threshold crossings and the KPI statistics to determine and indicate if scaling process needs to be performed. The algorithms for capacity determination is provided through the vendor plug-in being used.

Composite Network Function Descriptor

The CNF descriptor (CNFD) communicates the deployment, operational behavior and policies that are needed to deploy and manage a single CNF to Oracle Communications Application Orchestrator, and contains information about its PNF and NFVM components.

Monitoring

The Oracle Communications Application Orchestrator assigns a monitor to each NF group that periodically collects KPI statistics for all the deployed VNFs and PNFs. These statistics can provide information for health, performance and capacity.

Connection Point

A layer 2 connection point (CP) provides connectivity for NF group (component) interfaces in a CNF to its appropriate virtual link. The CP can be identified by a virtual port, a virtual network interface card (NIC) address, a physical port, a physical NIC address, or the end point (EP) of an IP VPN that enables network connectivity. All CPs are provided by element manager (EM) configuration templates.

End Point

An end point (EP) is an *Open Systems Interconnection (OSI)* layer 3 or higher logical entity. This EP connectivity supports layer 3 to layer 7 requirements for establishing connectivity. EPs are associated with subnetworks that have a one to many relationship with connection points (CPs).

Subnetwork

A subnetwork or "subnet" is a logical, visible subdivision of an IP network. In Oracle Communications Application Orchestrator, the relationship between a virtual link and subnetwork is one to many.

Virtual Link

A layer 2 virtual link is a logical connection between two or more connection points.

About Application Orchestrator Plug-ins

Oracle Communications Application Orchestrator has pre-existing plug-ins. See the *Plug-in Guide for Oracle Communications Application Orchestrator Session Delivery Network Elements* for more information.

Oracle Communications Application Orchestrator accepts vendor-defined CNF and EMS plug-ins. See the vendor-specific plug-in documentation for more information.

Application Orchestrator Standard Scaling Policy

Application Orchestrator has a standard scaling policy for managing CNF resources depending on the dynamic nature of a network.

Capacity States

The Oracle Communications Application Orchestrator standard scaling policy reports the cumulative KPI capacity state for each DU node, DU, and the NFGroup. Capacity planning is only done based on a summary of an NF group's total KPI capacity state.

Capacity states are used by all plugin capacity planners displayed in the **Monitor CNF** groups table (**Application Orchestrator** > **Monitor** > **CNF**) as colored bars, and are rendered individually for each monitored KPI. For example, the capacity state for CPU can be different from the capacity state for memory based on the actual utilization of each metric; so each could have its own capacity state.

Every capacity planner must categorize the current capacity of a KPI with one of the following states in the **Monitor CNF** table:

- Good—The capacity planner determined that the current capacity of the KPI does need additional or fewer resources. A green bar displays.
- Warning—The capacity planner determined that the current capacity of the KPI may require additional resources soon. A yellow bar displays.
- Critical—The capacity planner determined that the current capacity of the KPI requires additional resources immediately. A red bar displays.
- Reducible—The capacity planner determined that the current capacity of the KPI can be satisfied by fewer resources. A gray bar displays.

KPI Thresholds

KPI Thresholds are used by all plug-ins' scaling policies to determine a suitable capacity state for a KPI.

All KPI thresholds have a relative limit field, which is the maximum capacity for the KPI that a single active and healthy device is capable of maintaining. For example, a KPI threshold for 1000 active calls means that a single healthy device is capable of supporting a maximum of 1000 active calls. When determining the cumulative NF group KPI capacity, the relative limit of all active and healthy devices is summarized. For example, if an NF group has two active and healthy devices, each capable of 1000 active calls, the NF group's cumulative relative limit for active calls is 2000 active calls.

Depending on the scaling policy that is used, KPI thresholds can have additional parameters. The standard scaling policy uses the following configurable parameters, in addition to the relative limit:

- Critical %—The percentage of the relative limit at which the KPI capacity should be considered in the critical capacity state.
- Warning %—The percentage of the relative limit at which the KPI capacity should be considered in the warning capacity state.

Note: It is also important to note that this percentage is also used to determine if a KPI capacity should be considered in the reducible capacity state. When the cumulative KPI capacity of the NF group is interpreted, a KPI is considered to be reducible if it is below the Warning % of N-1 DUs. For example, if a single DU were to be removed and the NF group's cumulative KPI capacity still remained below the Warning % threshold, the KPI is considered reducible.

- Growth Duration—The number of minutes that the KPI must remain in the warning capacity state before the capacity planner requests a horizontal scale-out. No scale-out is requested if the KPI drops back to a good or reducible capacity state before the growth duration is exceeded.
- Decline Duration—The number of minutes that the KPI must remain in the reducible capacity state before the capacity planner requests a DU be set offline to start the DU load-shedding process.

Note: DU load shedding is requested only after all KPI thresholds are reducible and any KPI threshold exceeds its decline duration. The capacity planner does not request a scale-in event until the DU completes load shedding.

Scale In and Scale Out Policies

The standard scaling policy requests a DU scale-out process immediately when any cumulative NF group KPI reaches a critical capacity state, and when any cumulative NF group KPI reaches the warning capacity state and remains there longer than the growth duration.

The standard scaling policy only starts the scale-in process when all cumulative NF group KPIs have reached a reducible capacity state, and any cumulative NF group KPI has remained in the reducible capacity state longer than the decline duration. To help an undeployment be graceful, the standard scaling policy uses the load shedding parameters to choose the best DU to scale-in, and requests that it begin load shedding. Once the DU completes load shedding, the standard scaling policy requests that the DU be undeployed.

Load Shedding

The standard scaling policy uses the following parameters for load shedding:

- Load Shedding KPI—Determines when the DU has completed the load shedding operation and is used to select the best DU for scale-in. Specifically, the standard scaling policy selects the DU that has the lowest current capacity for the load shedding KPI as the best DU to scale-in.
- Load Shedding Threshold—A raw value that the DU's KPI capacity must reach before DU load shedding is considered complete. Unlike the Warning% and Critical% KPI threshold parameters, this parameter is not a percentage.
- Load Shedding Timeout—The maximum number of minutes that the standard scaling policy waits for the KPI capacity of the DU to reach the Load Shedding Threshold before considering load shedding complete. A value of zero indicates that there is no timeout, and the load shedding process continues until the DU's KPI capacity has reached the Load Shedding Threshold.

2

Application Orchestrator Implementation

Implementing Application Orchestrator on Your Network

The following workflow outlines how Oracle Communications Application Orchestrator can be implemented on your network. Detailed implementation information is discussed in subsequent sections of this guide or in references made here to other documents.

1. Choose whether to install Oracle Communications Application Orchestrator as a standalone application or install Oracle Communications Application Orchestrator with *Oracle Communications Session Delivery Manager* on your system, which comes with the following applications:

    - *Oracle Communications Session Element Manager*
    - *Oracle Communications Route Manager*
    - *Oracle Communications Report Manager*

    See your user documentation for more details on external dependencies such as a northbound service orchestrator (client application), and if you have a third-party element manager (EM) that can be supported through the Oracle Communications Application Orchestrator REST interface. These dependencies may be required to support a CNF.
2. Start Oracle Communications Application Orchestrator.
3. Configure security parameters for user groups, specific users, views, and operations in Oracle Communications Application Orchestrator. See the *Security Manager* chapter for more information.

    Note: See your EM plug-in documentation before configuring any login or security parameters in Oracle Communications Application Orchestrator.
4. Configure the EM with the parameters needed to properly communicate with Oracle Communications Application Orchestrator. See your EM documentation for more detailed information on EM configurations.

    Note: If you are using *Oracle Communications Session Element Manager* see the *Oracle Communications Session Element Manager User Guide* for more information.
5. Upload trusted certificates to the Oracle Communications Application Orchestrator trust store to authenticate Transport Layer Security (TLS) connections to a virtual infrastructure manager (VIM), a third-party element manager system (EMS), or to devices managed through a plug-in. See the *Certificate Authentication* chapter for more information.
6. Provision your Oracle OpenStack Virtualization Infrastructure Manager (VIM) or VMware vCloud Director VIM with the proper data center, storage profile, and Virtual Machine (VM) parameters. See the *Guidelines for Provisioning Your VIM Appendix* for more information.

7. Add either a VMware vCloud Director or OpenStack Virtualization Infrastructure Manager (VIM) to Oracle Communications Application Orchestrator. See the *Configure a VIM for Application Orchestrator* chapter for more information.
8. Add the data center name that is associated with the VIM(s) that you added. See the *Configure a Virtual Infrastructure Manager for Application Orchestrator* chapter for more information.

   Note: Later in this process, each NF group is associated with a data center.

9. Upload and manage VM applications (OVA image packages) to Oracle Communications Application Orchestrator that are used to initiate a network function (NF) on a VM. See the *Configure a Virtual Infrastructure Manager for Application Orchestrator* chapter for more information.
10. Register your EM with Oracle Communications Application Orchestrator to stage a CNF from its CNF descriptor (CNFD). An EM supports a targeted CNF to determine resource usage requirements for the CNF and its collaboration with Oracle Communications Application Orchestrator. See the *Register an Element Manager with Application Orchestrator* chapter for more information.
11. If you decide to use the hierarchical service configuration (HSC) feature to automate the deployment, scaling and resizing of a CNF, see the *Build the Hierarchical Service Configuration* chapter in this guide for more information about the GUI configuration. The HSC must be configured before you can configure the REST API for the northbound client (such as a northbound service orchestrator (NSO)). See the *NF Operations* chapter in the *Oracle Communications Application Orchestrator REST API Guide* for information about configuring the external northbound service orchestrator with the REST API calls necessary for communicating with Oracle Communications Application Orchestrator.
12. If you decide to make a CNF operational manually, select a pre-existing CNF, stage and promote the CNF, configure the CNF, and deploy and make the CNF operational on your network.

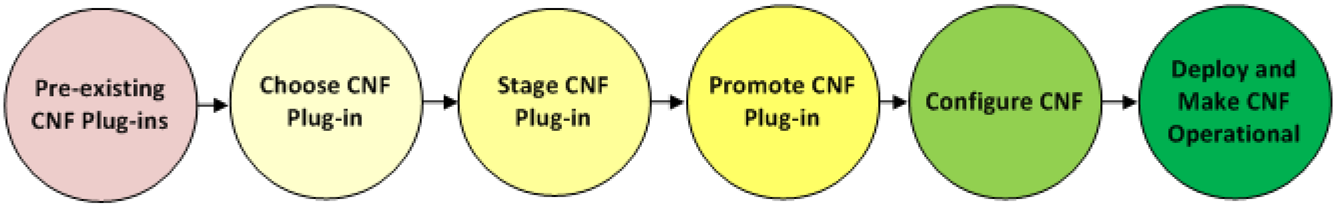


Figure 8: CNF Onboarding Workflow Process

a) Configure the resource criteria for a targeted pre-existing CNF to start the staging and promotion process. See the *Staging and Promoting a CNF* chapter for more information.
The pre-existing CNF is defined by its associated CNF descriptor called a CNFD that defines the resource criteria, NF group, DU topologies of the CNF. The pre-existing CNF needs to be staged and promoted in order to become a configurable CNF. The configurable CNF has some pre-configured parameters, but needs further configuration before it is in a deployable state.

b) Configure the various CNF NF group, DU, and VM parameters. See the *Configure the CNF* chapter for more information.

c) Once the CNF is configured correctly, the CNF can be deployed and made operational. See the *Deploy and Make the CNF Operational* chapter for more information.

   Note: Once a CNF is activated and running after its deployment, you can optionally undeploy or deploy DUs on an individual basis for administrative reasons before a CNF is deployed and made operational again. See the *Manage DU Deployments* section for more information.

13. Use the Oracle Communications Application Orchestrator **Monitor** folder node to check all the major components managed for CNFs. See the *Monitor Application Orchestrator System Information* chapter for more information.
14. Define fault parameters for Oracle Communications Application Orchestrator. See the *Fault Manager* chapter for more information.

3

Security Manager

The Security Manager product allows a user with administrator privileges to do the following:

- Create and manage users.
- Create and manage groups.
- Configure security authorization levels, policies and privileges for user groups.
- Provide specific access controls for individual user groups, views, and operations.
- Limit access to specific features and functionality for specific users.
- Configure audit log parameters.

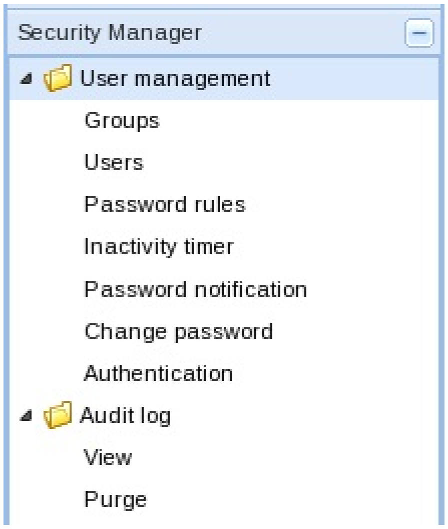


Figure 9: Security Manager Slider Parameters

Configure External User Authentication

Users belonging to the external domain user group are authenticated outside of Oracle Communications Application Orchestrator by an external domain server. You can select either a RADIUS domain server or Active Directory (AD) domain controller:

- A RADIUS server provides centralized Authentication, Authorization, and Auditing/Accounting (AAA) security protocol management for users who connect and use a network service.

- An AD domain controller provides a directory service in a Windows domain type network using Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

An external domain user group must be mapped to an internal (local) user group in Oracle Communications Application Orchestrator so that this external domain user group and its users inherit the authorization privileges that are specific to the local user group. See the *Add and Map a Local User Group to an External Domain User Group* section of this chapter for more information.

Note: Internal and external users are both supported simultaneously. However, external users do not have corresponding stored user records or username and password information.

Configure a RADIUS Server

This task is used to configure a RADIUS server domain for external user authentication.

- The RADIUS server must be configured to use the same shared secret string for all cluster nodes.
- The RADIUS server must be configured to return one or more attribute values in the authentication response message to represent the groups to which a user belongs.

1. Expand the **Security Manager** slider and select **User Management** > **Authentication**.
2. In the **External authentication** pane, select the **RADIUS** radio button and click **Add**.
   The **RADIUS** servers table becomes available for use.
3. In the **Add a radius server** pane, complete the following fields:

Name	Description
Address field	The IP address or DNS name of the RADIUS server.
Port field	This field is pre-populated with the default RADIUS server listening port **1812**. If you are using a different listening port on your RADIUS server, enter a new value.
Shared secret field	Click **Edit** next to the field. In the **Encrypted shared secret** dialog box, enter the following parameters: • **Shared secret**—The string assigned within the RADIUS server configuration to a given RADIUS client. • **Confirmed shared secret**—The same shared secret string again to confirm your input.
Password authentication mechanism drop-down list	**PAP** is chosen by default. The password authentication protocol (PAP) is an authentication protocol that uses a password in a point-to-point (PPP) session to validate users before allowing them to access server resources. Choose from the following options if you want to authenticate the user with another protocol: • **CHAP**—The challenge-handshake authentication protocol (CHAP) authenticates a user or network host to an authentication entity to protect against replay attacks by the peer through the use of an incrementally changing identifier and a variable challenge value. • **MSCHAPV1**—The Microsoft CHAP Version 1 (MS-CHAP v1) version of CHAP is used with RADIUS servers to authenticate wireless networks. In comparison with CHAP, MS-CHAPv1 is enabled by negotiating CHAP Algorithm 0x80 in the link control (authentication) protocol (LCP) option 3. LCP option 3 sends the Configure-Nack LCP packet type when all the LCP options are recognized, but the values of some options are not acceptable. Configure-Nack includes the offending options and their acceptable values). MS-CHAPv1 also provides an authenticator-controlled

Name	Description
	password change and authentication retry mechanisms, and defines failure codes, which are returned in the Failure packet message field. • **MSCHAPV2**—The Microsoft CHAP Version 2 (MS-CHAPv2) uses the same authentication as MS-CHAPv1, except that CHAP Algorithm 0x81 is used instead of the CHAP Algorithm 0x80. • **EAPMD5**—The extensible authentication protocol (EAP-MD5) offers minimal security and is used in wireless networks and point-to-point networks. EAP-MD5 enables a RADIUS server to authenticate a connection request by verifying an MD5 hash of a user password. The server sends the client a random challenge value, and the client proves its identity by hashing the challenge and its password with the MD5 hash. • **EAPMSCHAPV2**—The protected extensible authentication protocol challenge-handshake authentication protocol (EAP-MSCHAPv2) allows authentication to databases that support the MS-CHAPv2 format, including Microsoft NT and Microsoft Active Directory.
Group attribute name field	This field is pre-populated with the attribute **Filter-Id** by default. **Note:** Change the default value if the RADIUS server's group attribute does not match. This attribute (RADIUS attribute 11) is necessary for the device to assign a user to a RADIUS group. This RADIUS attribute connects the user name with the attribute in order to place this user in a RADIUS group. The group attribute name is configured to be included in Access-Accept message that the RADIUS server returns to this device.

4. Click **Apply**.
   External users can now be authenticated by the RADIUS server. See the *Map a Local User Group to an External Domain User Group* section of this chapter for more information.

Configure an Active Directory Domain Controller

This task is used to configure and active directory (AD) domain controller (domain server) for external user authentication.

- The Active Directory must be configured for LDAP over SSL if the Active Directory is enabled in Oracle Communications Application Orchestrator.
- Active Directory must support version 5, if the Kerberos protocol is used.
- Each user object in your Active Directory must store the groups of each member using the *memberOf* attribute.
- Only child groups may be mapped to local groups when group nesting is in use. This limitation is due to the *memberOf* attribute not containing a recursive list of predecessors when nesting.

1. Expand the **Security Manager** slider and select **User Management** > **Authentication**.
2. In the **External authentication** pane, select the **Active directory** radio button and click **Add**.
   The **Active Directory** servers table becomes available for use.
3. In the **Add a Domain Controller** pane, complete the following fields:

Name	Description
Address field	The IP address or DNS name of the domain controller.
Domain field	The domain name for the domain controller.
LDAP Port field	The listening port number of the LDAP service. The default is 389. Use port 636 if using SSL.

Name	Description
Password security drop-down list	Select from the following protocols used to authenticate the user: • **Digest-MD5**—The password cipher based on RFC 2831. • **LDAP over SSL**—The SSL to encrypt all LDAP traffic. • **Kerberos**—The Kerberos protocol to authenticate the user by specifying an existing krb5.conf file containing the information needed by the Kerberos V5 library. This includes information describing the default Kerberos realm, and the location of the Kerberos key distribution centers for known realms.

4. Click **Apply**.
   External users can now be authenticated by the AD domain controller. See the *Map a Local User Group to an External Domain User Group* section of this chapter for more information.

Configure Groups

You can configure a local group to be mapped to an external domain user group so that the external group can inherit the authorization privileges of this local group. You can also add and manage additional local groups other than the default local groups that are provided by Oracle Communications Application Orchestrator.

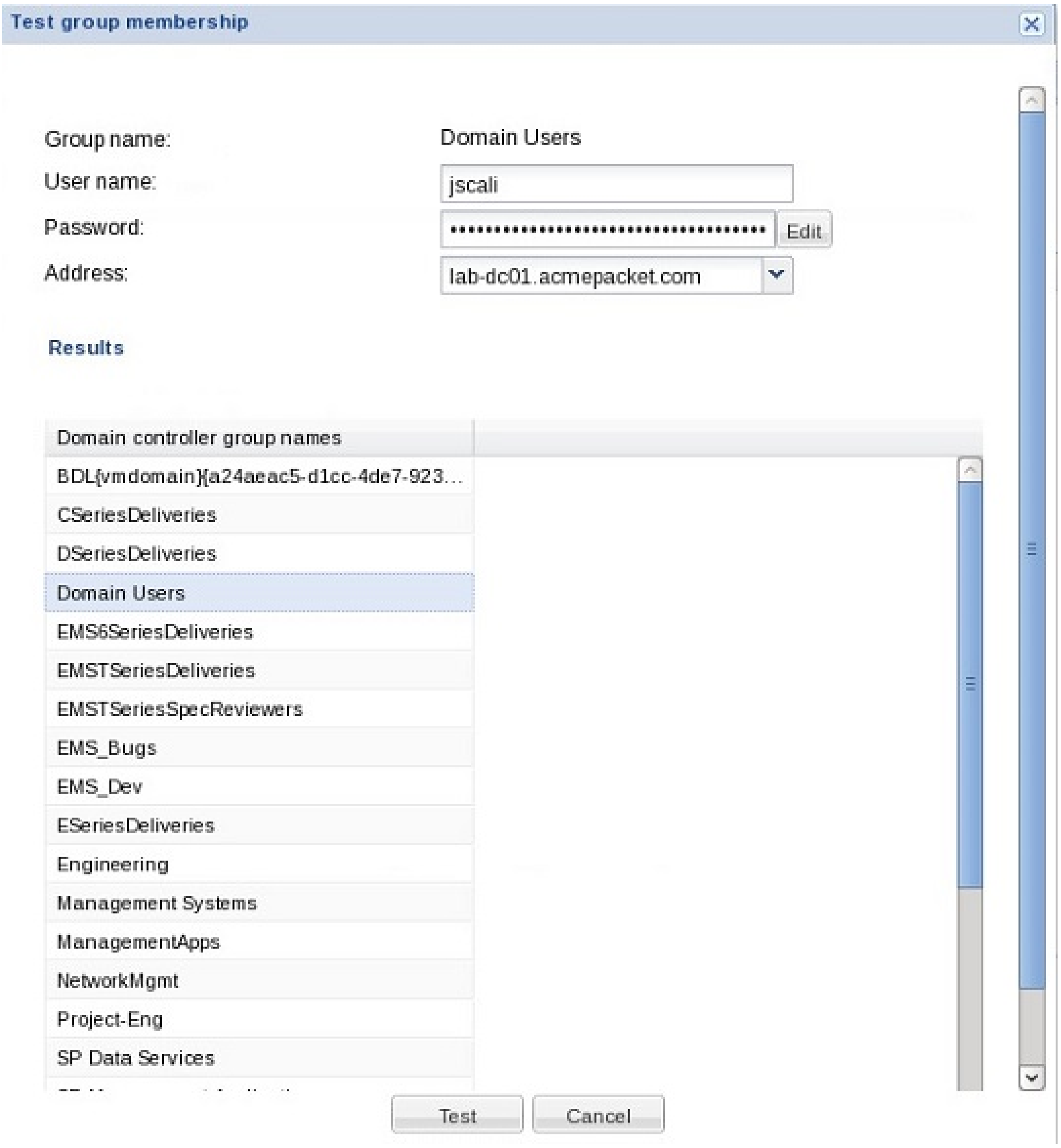
Note: Oracle Communications Application Orchestrator may be required to contact and collaborate with an external Element Management system (EMS). Please refer to the vendor plug-in documentation for additional information about the prerequisites needed for configuring an appropriate user on the EMS before you start configuring group and user privileges in Security Manager. For example, the Oracle Communications Session Element Manager requires the creation of an Oracle Communications Application Orchestrator group with an **AoSystem** user. In this case, see the *Plug-in Guide for Oracle Communications Application Orchestrator Session Delivery Elements* for more information.

Find an External Domain User Group

Use the external membership tool to find the name of an external domain user group so that it can be later mapped to a local (internal) user group.

This tool provides the ability to test external users once an external domain server is configured and returns a list of external domain user groups to which the external domain user was assigned. This makes finding the proper external domain user group names that you need to map to the local user group easier so that the external domain user group can inherit its authorization privileges. Once you find the external domain user group you want, see the *Add and Map a Local User Group to an External Domain User Group* section of this chapter to continue.

1. Expand the **Security Manager** slider and select **User Management** > **Groups**.
2. In the **User Groups** pane, select the local group name that you are using for the external RADIUS user group (for example, MyExternalRADIUSUserGroup) and click **Edit**.
3. In the **Configuration** tab, enter the external group name (for example, Domain Users) and click **Apply and Test**.
   The **Test group membership** dialog box displays with results for the external group.



Test group membership

Group name: Domain Users

User name: jscali

Password: ••••••••••••••••••••••••••••••••••••

Address: lab-dc01.acmepacket.com

Results

Domain controller group names
BDL{vmdomain}{a24aeac5-d1cc-4de7-923...
CSeriesDeliveries
DSeriesDeliveries
Domain Users
EMS6SeriesDeliveries
EMSTSeriesDeliveries
EMSTSeriesSpecReviewers
EMS_Bugs
EMS_Dev
ESeriesDeliveries
Engineering
Management Systems
ManagementApps
NetworkMgmt
Project-Eng
SP Data Services

Figure 10: Example of Test Group membership results for an external group:

Add and Map a Local User Group to an External Domain User Group

Use this task to allow the external domain user belonging to the external domain user group to inherit the group-based authorization privileges of the local user group.

The external domain user is authenticated by a domain server, such as a RADIUS server or Active Directory domain controller. You must map the external domain user group to the local (internal) user group that was created for this purpose.

See the *Use the External Membership Tool to Find External Domain User Groups* section of this chapter for more information about finding the external domain user group name that you need for this task.

1. Under the **User Management** folder, select the **Groups** leaf node.
2. In the **User Groups** pane, click **Add**.
3. In the **Add Group** dialog box, complete the following fields:

Name	Description
Group name field	The local user group name that you want to use for authorization privileges. For example, **LocalUGforDomainUG**. Use the following guidelines for naming this group: • Use a minimum of three characters and maximum of 50. • The name must start with an alphabetical character. • You are allowed to use alphanumeric characters, hyphens, and underscores. • The user group name is case insensitive. • The user group must be unique.
External group name field	For Active Directory (LDAP), the external domain user group name. For example, **Domain UG**. For RADIUS, the external group name should map to attribute 11 (Filter-ID), which is in the RADIUS reply. **Note:** You must have at least one external domain user group entry configured on the domain server in order for this field to be displayed in the dialog box.
Group permissions copy from drop-down list	Choose from the following default user groups to copy their privileges: • **None**—Manually configure privileges for this user group. • **administrators**—This super user group is privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure Oracle Communications Application Orchestrator and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Application Orchestrator, and has the fewest privileges.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. Log out and log back into the system with the external RADIUS user to test your external connection to Oracle Communications Application Orchestrator.

Add a Local User Group

A local (internal) user group is a logical collection of users grouped together to access common information or perform similar tasks in Oracle Communications Application Orchestrator. You assign specific authorization privileges to a group and then assign users to it. Those users in turn, inherit the group-based privileges. See the *Add and Map a Local User Group to an External Domain User Group* section of this chapter if you need to add local group that needs to be mapped to an external domain user group.

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.
2. In the **User Groups** pane, click **Add** to add a new user group.
3. In the **Add Group** dialog box, complete the following fields:

Name	Description
Group name field	The user group name. Use the following guidelines for naming this group: • Use a minimum of three characters and maximum of 50. • The name must start with an alphabetical character. • You are allowed to use alphanumeric characters, hyphens, and underscores. • The user group name is case insensitive. • The user group must be unique.
Group permissions copy from drop-down list	Choose from the following default user groups to copy their privileges: • **None**—Manually configure privileges for this user group. • **administrators**—This super user group is privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure Oracle Communications Application Orchestrator and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Application Orchestrator, and has the fewest privileges.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. Click **Back** to return to the **User Groups** table.

Delete a User Group

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.
2. In the **Groups** pane, choose the (non-default) user group that you want to delete from the **User Groups** table and click **Delete**.
3. In the **Delete** confirmation dialog box, click **Yes** to delete this user group.
   The user group is removed from the **User Groups** table.
4. In the success dialog box, click **OK**.

Change Privileges for User Groups

By default, privileges are assigned to each category of a user group that allow or deny all users within this user group the ability to perform certain operations. You have the option to change the default privilege type for items in each category item of a pre-existing user group or a user group that you create allow or deny all users within this group the ability to perform certain operations. This includes items intended for use with separate application products that you are licensed to use.

Operations Tree Structure

The operations tree structure contains all the security configuration and administrative tasks you can perform in Oracle Communications Application Orchestrator. It is logically arranged with parent and child operations that can be accessed once user group and user accounts are created. Individual access to a specific operation within the tree structure can be provided or denied by assigning a privilege to it. Although Oracle Communications Application Orchestrator displays all the operations it supports, some apply only to users who are licensed for a specific application operation.

The top of the operations tree is the root. There can be one or more operation categories below the root that serve as parents for individual operations (children). The child privilege type of higher-level (or parent) operation is equal or less than the privilege type of its parent. When you change the privilege type of a parent, the child privilege type can change based on this rule. However, if the parent privilege type is returned to its previous privilege type, the child remains at the privilege type to which it was bumped and needs to be promoted manually.

Apply User Group Privileges for the Administrative Operations

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. In the expanded group pane, click the **Administrative operations** tab and click the folder and subfolder sliders to expand the item operations list.
4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following user group privilege options for folders or items in the **Administrative operations** tab table described below:

- **Full**—(Default) Allowed to perform administrative operations.
- **None**—Not allowed to perform administrative operations.
- **View**—Allowed to monitor only.

Name	Description
Administrative operations folder	Set privilege levels for all of the following administrative operations.
Security administration folder	Set privilege levels for all of the following user management operations accessible on the **Security Manager** slider.
Group operations folder	Set privilege levels for all group item operations.
Add group item	Add a new group.
Update group item	Modify groups.
Delete group item	Delete existing groups.
User operations folder	Set privilege levels for all the following user operations accessible on the **Security Manager** slider.
Add users item	Create new users.
Update users item	Modify user information.
Delete users folder	Delete existing users.
Change inactivity timer item	Change the inactivity timer, which logs off the user if the client is no longer being used.
Change Password Rule item	Configure the password rules used when creating a new user.
Password notification	Change the notification interval.
KPI Operation item	Set privilege levels to get device KPIs, register KPIs, deregister KPIs, or update registered KPIs.
Edit login banner item	Allow users of a group to change the informational banner seen when a user logs into Oracle Communications Application Orchestrator.

Name	Description
Change password message interval item	Send alert that prompts user to change their password a certain number of days before their password expires.
View all audit logs item	View all audit logs.
View own audit log item	View only personal audit log.
Change audit log auto purge interval item	Configure the number of days of audit logs to keep.
Export audit logs item	Export all or part of an audit log to a file.
Manual audit log purge item	Manually purge audit logs.
View health monitor console item	Access health monitor console to detect issues.
Update OS/System account password item	Update the operating system and the system account password.
Authentication item	Update authentication parameters.
Server Diagnostics item	Access to server diagnostics.

6. Click **Apply**.

Apply User Group Privileges for Fault Management Operations

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. Click the **Fault management** tab and click the folder and subfolder sliders to expand the item operations list.
4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following user group privilege options for folders or items in the **Fault management** tab table described below:
   - **Full**—(Default) Allowed to perform event or alarm operations.
   - **None**—Not allowed to perform event or alarm operations.

Name	Description
Fault management folder	If the **None** privilege is chosen, the **Fault Manager** slider does not appear in the Oracle Communications Application Orchestrator GUI.
Events and Alarms folder	Assign the privileges for all of the following event and alarm operations accessible on the **Fault Manager** slider.
Alarms folder	Assign the privileges for all of the following alarm operations accessible on the **Fault Manager** slider.
Set email notification item	Create an email list for alarms.
Delete alarm item	Delete alarms.
Remap severities item	Edit the alarm severity levels.
Events folder	Assign the privileges for all of the following event operations accessible on the **Fault Manager** slider.
Delete events item	Delete events.

Name	Description
Configure trap receiver item	Assign privileges to configure a trap receiver.

6. Click **Apply**.

Apply User Group Privileges for Applications

1. Expand the **Security Manager** slider and choose **User Management** > **Groups**.
2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.
3. Select the **Applications** tab and click to expand the **Applications** folder.
4. Select any folder or folder item row that are described in the table below that you want to modify and click the **Privileges** column to activate the drop-down list.

   Select the following privilege from the **Privileges** drop-down list:

   - **Full**—Enable GUI elements (such as tabs) to perform configuration operations.
   - **View**—View information only.
   - **None**—Disable configuration operations and make them disappear from the GUI.

Name	Description
Application folder	Set privilege levels for all of the following applications operations.
Application Orchestrator folder	Set privilege levels for all Oracle Communications Application Orchestrator operations on the **Application Orchestrator** slider.
AO Administration folder	Set administrative privilege levels for configuring NF group parameters on the **Application Orchestrator** slider.
CNF configuration folder	Set administrative privilege levels for configuring CNF parameters on the **Application Orchestrator** slider.
HSC configuration folder	Set administrative privilege levels for configuring Hierarchical Service Configuration (HSC) parameters on the **Application Orchestrator** slider. See the *Build the Hierarchical Service Configuration* chapter for more information about this feature.

5. Click **Apply**.

Configure Users

A user is a person who logs into the system to perform application-related operations. Before this user can access any operations, they must be added to a user group. Each user group has a defined set of privileges. The operations that a user can do depends on the privileges of the user group to which the user belongs.

The following users are created by default when Oracle Communications Application Orchestrator is installed:

- **admin**—Inherits the privileges from the **administrators** group.
- **LIadmin**—Inherits the privileges from the **LIadmin** group.

Users (other than the default users) are created, added, and given the privileges of the user groups to which they are assigned so that they can access Oracle Communications Application Orchestrator.

Add a User

Note: If you are using Oracle Communications Session Element Manager with Oracle Communications Application Orchestrator, see the *Oracle Communications Application Orchestrator Plug-in Guide for Session Delivery Network Elements, Release 1.1* for more information about configuring the **AoSystem** user, which is required for this implementation scenario.

1. Expand the **Security Manager** slider and choose **User Management** > **Users**.
2. In the **Users** pane, click **Add**.
3. In the **Add User** dialog box, complete the following fields:

Name	Description
Group **Assigned group** drop-down list	Choose from the following default user groups: • **administrators**—This super user group privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure Oracle Communications Application Orchestrator and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Application Orchestrator, and has the fewest privileges.
User information **User name** field	The name of the user using the following guidelines: • Use a minimum of 3 characters and maximum of 50 characters. • The name must start with an alphabetical character. • The use of alphanumeric characters, hyphens, and underscores are allowed. • The name is case insensitive. • The name cannot be the same as an existing group name.
User information **Password** field	The password is entered for this user using the following guidelines: • The password must be at least 8 characters long. • Use at least one numeric character from 0 to 9 in the password. • Use at least one alphabetic character from the English language alphabet in the password. • Special characters include {, |, }, ~, [, \,], ^, _, ‘, :, ;, <, =, >, ?, !, “, #, $, %, &, `, (,), *, +, ,, -, ., and /
User information **Confirm password** field	The same password entered again to confirm it.
User account expiration dates **Account** field	Uncheck the check box to change the user account expiration date. Click the calendar icon to open a calendar to choose the date after which the user account expires. **Note:** If the check box is checked (default) the user account never expires.
Password expiration dates **Password** field	Uncheck the check box to change the password expiration date. Click the calendar icon to open a calendar to choose the date after which the user password expires.

Name	Description
	☞ **Note:** If the check box is checked (default) the password never expires.

4. Click **OK**.
   The following information displays in the **Users** table:

Name	Description
User name column	The user name.
Group column	The user group to which the user belongs.
Status column	The status of the user account is either **enabled** or **disabled**.
Operation status field	The state of the user account and its expiration date: • **active**—The account is valid and the user can log in. Neither the account nor password expiration dates have been exceeded. • **account expired**—The account expiration date has expired. • **password expired**—The password expiration date has expired. • **password deactivated**—The failed login attempts by the user exceeded the allowed number of tries as specified by the value set for password reuse count parameter in password rules. • **locked out**—The user has exceeded the login failures and the account is disabled until the lockout duration has passed.

Edit a User

1. Expand the **Security Manager** slider and choose **User Management** > **Users**.
2. In the **Users** pane, choose a user and click **Edit**.
3. In the **User** tab , change the following fields:

Name	Description
Assigned group drop-down list	Change the assigned user group: • **administrators**—This super user group privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure Oracle Communications Application Orchestrator and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Application Orchestrator, and has the fewest privileges.
User status **Administrative status** drop-down list	Choose if the user status is either **enabled** or **disabled**.
Expiration dates **Account** field	Uncheck the check box to change the user account expiration date.

Name	Description
	Click the calendar icon to open a calendar to choose the date after which the user account expires. **Note:** If the check box is checked (default) the user account never expires.
Expiration dates **Password** field	Uncheck the check box to change the password expiration date. Click the calendar icon to open a calendar to choose the date after which the user password expires. **Note:** If the check box is checked (default) the password never expires.

4. Click **Apply**.

Reactivate a User

A user can be denied access to Oracle Communications Application Orchestrator if the user is disabled, expired, the user password expired, or the user logs in more times (due to failed log in attempts) than is allowed by the Password reuse count value.

You can reactivate a user by editing the user profile to reset the status of the user to enable, then reset the expiration in days for the account and password parameters. You can also delete the expired user and recreate the user.

The following table lists the possible causes for user deactivation and how to reactivate the user.

Cause	Action
User expired	Reset the calendar to a new date.
Password expired	Reset the password calendar to a new date.
Password deactivated	Reactivate the user account by: • Changing the user password if all expiration dates are still valid. • Extending the account expiration date. • Extend the password expiration date.
User disabled	Reset the user to enabled.

Delete a User

1. Expand the **Security Manager** slider and choose **User management** > **Users**.
2. In the **Users** pane, choose a user and click **Delete**.
3. In the **Delete** dialog box, click **Yes**.
4. In the success dialog box, click **OK**.
   The user name is removed from the **Users** table.

Reset a User Password

You must have permission to reset passwords.

1. Expand the **Security Manager** slider and select **User management** > **Users**.
2. In the **Users** pane, click a user from the table and click **Reset Password**.
3. In the **Reset password** dialog box, enter a new password for the user in the field provided.
4. The dialog box indicates if you entered the new password successfully. Click **OK**.

Change a User Password

If you have administrative operations permission, you can change the password of a user.

1. Expand the **Security Manager** slider and select **User Management** > **Users**.
2. In the **Users** pane, click a user from the table and click **Change Password**.
3. In the **Change password** dialog box, complete the following fields:

Name	Description
Enter your password field	Enter the existing password for the user.
Enter new password for user field	The new password for the user.
Confirm new password for user field	The new password is entered again to confirm it.

4. Click **OK**.

Change User Password Rules

Use this task to change the password rules that specify the length of the password, how many times it can be reused, and whether specific characters, such as a numeric value, can be used.

1. Expand the **Security Manager** slider and select **User management** > **Password rules**.
2. In the password rules pane, complete the following fields:

Name	Description
Maximum login fail attempts **For administrator users** and **For non-administrator users** fields	The value that indicates the maximum login attempts allowed before the user is locked out of the system. You can set a different value for both administrator users and non-administrator users. The default value is 5 attempts.
Account lockout duration **For administrator users (minutes)** field	Enter the number of minutes that an administrator user is locked out after the maximum login fail attempts **For administrator users** value has been reached. The default is 15 minutes. **Note:** This parameter applies to Administrator users only. Non-administrator users remain locked out until their login is reset.
Password reuse count **For all users** field	The value that indicates the number of counts to use to prevent the reuse of a password. The reuse count restricts the user from reusing the password entered in the last number of counts. For example, if you enter 2 here the user cannot reuse the same password used on the previous two occasions. You can change the password for this user by using the guidelines below.
Password length for administrator users **Minimum length** and **Maximum length** fields	The values for the minimum (no less than eight characters) and maximum (up to 16 characters) length of a password for a user who has administrator privileges.
Password length for non-administrator users **Minimum length** and **Maximum length** fields	The values for the minimum (no less than eight characters) and maximum (up to 16 characters) length of a password for a user who does not have administrator privileges.
Password contains at least one of the following	Check the checkbox for each of the following rules that you want to enforce: • **Numeric character**—Use at least one numeric character from 0 to 9 in the password.

Name	Description
	• **Alphabetic character**—Use at least one alphabetic character from the English language alphabet in the password. • **Special character**—You can include the following: {, |, }, ~, [, \,], ^, _, ‘, :, ;, <, =, >, ?, !, “, #, $, %, &, `, (,), *, +, ,, -, ., and /

3. Click **Apply**.

Notify When to Change the User Password

You can configure when the user is notified to change their password before it expires.

When the user logs into Oracle Communications Application Orchestrator, the system checks user credentials and the password expiry time for the user. If the password is due to expire, Oracle Communications Application Orchestrator displays a warning and prompts the user to change their password.

1. Expand the **Security Manager** slider and select **User management** > **Password notification**.
2. In the **Password expiration notification** panel, enter a value in the **Days prior to password expiration** field.
3. Click **Apply**.

Set the Inactivity Timer to Prevent Unauthorized System Access

We recommend that you set the inactivity timer to prevent unauthorized access to your system as soon as possible.

The inactivity timer logs off the user from the Oracle Communications Session Delivery Manager session when its value is exceeded. The user must re-enter their password to continue. You can set different values for a user with administrative permissions and users who do not have administrative permissions.

Note: The default inactivity timer value for an administrator is set to zero (never expire). You must choose a different value to terminate a user session after a specified time period.

1. Expand the **Security Manager** slider and select **User Management** > **Inactivity timer**.
2. In the **Session timeout** panel, complete the following fields:

Name	Description
Admin field	(Optional) The number of minutes of inactivity after which the user with administrative permissions is logged off. The range is zero to 65535 minutes. Zero sets the inactivity timer to never expire.
Non-Admin field	The number of minutes of inactivity after which a non-administrative user is logged off. The range is 1 to 65535 minutes. Thirty minutes of user inactivity is the default.

3. Click **Apply**.

Audit Logs

You can use the audit log (containing audit trails) generated by Oracle Communications Application Orchestrator to view performed operations information, which includes the time these operations were performed, whether they were successful, and who performed them when they were logged into the system.

Note: Audit logs contain different information depending on its implementation.

Audit trails include the following information:

- The user who performed the operation.
- What operation was performed by the user.
- When the operation was performed by the user.
- Whether the operation performed by the user was successful or failed.

View and Save an Audit Logs

The following Oracle Communications Application Orchestrator operations are logged:

- User logins and logouts.
- Managed devices are added.
- Device groups are added.
- Oracle Communications Session Delivery products are loaded.
- An element is added, deleted, or modified.
- A device is rebooted.
- An HA device roles are switched.
- Configurations are saved or activated.

1. Expand the **Security Manager** slider and choose **Audit log** > **View**.
2. In the **Audit log** pane, select an entry row in the table and click **Details** or double-click the row.
3. In the **Audit log details** dialog box, the following audit trail entry is described:

Name	Description
Sequence number field	The audit log reference number.
Username field	The name of the user who performed the operation.
Time field	The time stamp for when the operation was performed by the user.
Category field	The category of operation performed by the user. For example, Authentication.
Operation field	The specific operation performed by the user.
Management Server field	The IP address of the management server accessed.
Client IP field	The IP address of the client that was used.
Device field	The IP address of the device that the user performed an operation upon.
Status field	The status of the operation performed by the user, whether it was successful or failed.
Description field	The description of the operation performed.

4. Click **OK**.
5. Click **Save to file** to open the audit log file or save it to a file.

Note: The downloaded CSV file is limited to 250 entries. Only the active page’s entries are saved.

Search the Audit Log

1. Expand the **Security Manager** slider and select **Audit log** > **View**.
2. In the **Audit log** pane, choose an entry row in the table and click **Search**.
3. In the **Audit Log Search** dialog box, complete some or all of the following fields to search the audit log:

Name	Description
Username field	Choose the name of the user who performed the operation.

Name	Description
Category drop-down list	Choose the category of operation performed by the user. For example, Authentication.
Operation box	Chose the specific operation performed by the user.
Management Server	The IP address of the management server accessed.
Client IP	The IP address of the client that was used.
Device	The IP address of the device that the user performed an operation upon.
Status	The status of the operation performed by the user, whether it was successful or failed.
Start Time	Choose a start time from the calendar.
End Time	Choose an end time from the calendar.

4. Click **OK**.

Schedule Audit Log Files to Be Purged Automatically

1. Expand the **Security Manager** slider and select **Audit log** > **Purge**.
2. In the **Purge audit logs** pane, specify the number of days of audit logs that are kept in the **Interval in days** field.
3. Click **Apply**.

Purge Audit Log Files Manually

1. Expand the **Security Manager** slider and select **Audit log** > **Purge**.
2. In the **Manual Audit log purge** dialog box, click the calendar icon next to the **Purge audit log records prior to** field and choose the date from the calendar prior to which you want audit logs purged.
3. Click **OK**.

4

Certificate Authentication

The X.509 cryptographic standard is used for security in a public key infrastructure (PKI) that binds public keys with respective identities by way of a certificate authority (CA). The X.509 standard specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

The Oracle Communications Application Orchestrator server can use trusted certificates (certificates validated by a CA or self-signed certificate) in its trust store to authenticate Transport Layer Security (TLS) connections to a network function (NF) when Transport Layer Security (TLS) communication is required.

Upload a New Certificate

From Oracle Communications Application Orchestrator, you can upload a new X.509 certificate from your system to the Oracle Communications Application Orchestrator trust store.

1. On the main menu, choose **Tools** > **Certificates**.
2. In the **Certificates** dialog box, click **Import**.
3. In the **Upload Certificate** dialog box, complete the following fields:

Name	Description
Name field	The name of the X.509 certificate.
File field	The directory path of the certificate file on your system. Alternately, click **Browse** to navigate to the certificate on your system.

The certificate appears in the **Certificates** dialog box with certificate name, issuer, start date, end date and serial number of the certificate. The changes are propagated to any cluster members.

Delete an Existing Certificate

From Oracle Communications Application Orchestrator, you can delete an existing certificate from the Oracle Communications Application Orchestrator trust store.

1. On the main menu, select **Tools** > **Certificates**.
2. In the **Certificates** dialog box, click **Delete**.
3. In the **Delete** confirmation dialog box, click **Yes**.

5

Configure a VIM for Application Orchestrator

Oracle Communications Application Orchestrator manages the life-cycle of a VNF through the Oracle OpenStack virtual infrastructure manager (VIM) or VMWare vCloud Director VIM. The VIM is an orchestration engine that manages a data center, and is required for deploying a CNF.

Before parameters are configured in Oracle Communications Application Orchestrator for a VIM, the VIM itself needs to be provisioned with the proper parameters. See the Guidelines for Provisioning Your VIM section in Appendix A of the Oracle Communications Application Orchestrator User Guide for more information.

Add an Oracle OpenStack VIM

Ensure that you have uploaded the validated certificate or self-signed certificate needed to authenticate the transport layer security (TLS) connection to the VIM.

1. Expand the **Application Orchestrator** slider and select **Administration** > **VIMs**.
2. In the **Virtualization Infrastructure Manager** pane, the VIM tab displays by default. Click **Add**.
3. In the **Add VIM** pane, complete the following fields in the **Settings** tab.

Name	Description
Name field	The unique name for the VIM instance. For example, OpenStack1.
Type drop-down list	Select the **Oracle OpenStack for Oracle Linux 1.0** or **Oracle OpenStack for Oracle Linux 2.0** VIM plug-in type.

4. Click **Load** next to the **Type** drop-down list, and complete the additional configuration parameters.

Name	Description
Identity URL field	The base URL address to the identity service, which acts as the common authentication system. For example: https://mycloud.com:5000
Username field	The user name used to log into the VIM web application account.
Password field	The password used to log into the VIM web application account.
Domain field	The domain name used for the authentication of users. A domain can represent an individual, company, or operator owned space. If OpenStack multi-domain support is not configured, enter **default** for the value.

Name	Description
Project drop-down list	Select the project that end-users use for authentication. Click **Load** to select the project. **Note:** An error message displays if a validated certificate has not been uploaded to Oracle Communications Application Orchestrator for the connection to the VIM.

5. Click **Test connectivity** to test the connection to the Oracle OpenStack cloud management web application.
6. Click **Apply** to add the VIM to Oracle Communications Application Orchestrator.

Add a VMWare vCloud Director VIM

Ensure that you have uploaded the validated certificate or self-signed certificate needed to authenticate the transport layer security (TLS) connection to the VIM.

1. Expand the **Application Orchestrator** slider and select **Administration** > **VIMs**.
2. In the **Virtualization Infrastructure Manager** pane, the VIM tab displays by default. Click **Add**.
3. In the **Add VIM** pane, complete the following fields in the **Settings** tab.

Name	Description
Name field	The unique name for the VIM instance. For example, vCloud1.
Type drop-down list	Select the VIM plug-in type. For example, **vCloud Director 5.5**_x_.

4. Click **Load** next to the **Type** drop-down list, and complete the additional configuration parameters.

Name	Description
VCloud URL field	The base URL address to the cloud service. For example: https://mycloud.com:443
Username field	The user name used to log into the vCloud web application account.
Password field	The password used to log into the vCloud web application account.
Organization	The vCloud organization to which this user belongs.
Catalog drop-down list	Click **Load** to select the catalogue for vAppTemplate storage. When Oracle Communications Application Orchestrator uploads an OVF to vCloud, it adds the resulting vApp Template to the chosen catalog. This vApp Template is used for customizing virtual machines (VMs) that are passed to the vApp. **Note:** An error message displays if a validated certificate has not been uploaded to Oracle Communications Application Orchestrator for the connection to the VIM.
Catalog Reference ID drop-down list	Click **Load** to auto-populate the URL for the cloud catalog identifier.

5. Click the **Test connectivity** to test the connection to the VMWare vCloud Director cloud management web application.
6. Click **Apply** to add the VIM to Oracle Communications Application Orchestrator.

Add Data Center to Oracle OpenStack VIM

The cloud administrator must provision the data center(s) before starting this task. See the *Guidelines for Provisioning Your VIM* appendix for more information.

Use this task to identify the data center, add and register the data center with Oracle Communications Application Orchestrator, and associate the data center to the Oracle OpenStack VIM.

Note: A CNF deployment can span multiple data centers to satisfy load or fault tolerance requirements.

1. Expand the **Application Orchestrator** slider and select **Administration** > **VIMs**.
2. In the **Virtualization Infrastructure Manager** pane, the VIM tab displays by default. Click **Add**.
3. In the **Add VIM** pane, click the **Association data centers** tab.
4. Click **Add**.
5. In the **Add data centers** dialog box, complete the following fields to identify the data center for the Oracle OpenStack VIM.

Name	Description
Name field	The unique name for the data center. This name must be unique among all data centers and VIMs in Oracle Communications Application Orchestrator and have no spaces.
Reference name field	(Pre-populated) The reference name for the data center that was assigned by the cloud administrator. This name is the logical entity in the cloud that Oracle Communications Application Orchestrator considers to be a datacenter. For example, the OpenStack VIM refers to the name of an Availability Zone. Click **Load** to display the fields and drop-down list described below.
Description field	The description that uniquely identifies this data center.
Caution field	(Read-only) This field cautions that all hosts that belong to this data center must support the *Configuration Drive* feature in OpenStack. The Configuration Drive contains a generic metadata that is needed for the VM to bootstrap itself. Actual metadata required is determined by the plugin, and may provide more configuration information other than IP addressing. For example, Acme device metadata contains IP, basic system configuration settings, and in some cases default account passwords. See the *OpenStack Configuration Drive Guidelines and Requirements* section in Appendix A for more information.
Use KVM hosts check-box	Check the check box to allow VM deployment to kernel-based VM (KVM) based hosts.
Use Oracle VM hosts check-box	Check the check box to allow VM deployment to Oracle VM (OVM) based hosts.
Security groups field	Click **Load** to load security group(s) defined in Oracle OpenStack, which appear below this field with their check box(es).
Security group: checkbox	(Optional) Check the check box to enable the security group that was previously defined in Oracle OpenStack.

6. Click **Apply** to register the data center for the VIM.

Add Data Center to VMware vCloud Director VIM

The cloud administrator must provision the data center(s) and storage profile before starting this task.

Note: Ensure that the 'Fast Provisioning' feature is disabled for the data center if you are using a VMware vCloud Director VIM. This feature needs to be disabled so that Oracle Communications Application Orchestrator can deploy the CNF and be able to dynamically size the CNF.

Use this task to identify the data center, add and register the data center with Oracle Communications Application Orchestrator, and associate the data center to the VMware vCloud Director VIM.

Note: A CNF deployment can span multiple data centers to satisfy load or fault tolerance requirements.

1. Expand the **Application Orchestrator** slider and select **Administration** > **VIMs**.
2. In the **Virtualization Infrastructure Manager** pane, the VIM tab displays by default. Click **Add**.
3. In the **Add VIM** pane, click the **Association data centers** tab.
4. Click **Add**.
5. In the **Add data centers** dialog box, complete the following fields to identify the data center for the VIM.

Name	Description
Name field	The unique name for the data center. This name must be unique among all data centers and VIMs in Oracle Communications Application Orchestrator and have no spaces.
Reference name field	(Pre-populated) The reference name for the data center that was assigned by the cloud administrator. This name is the logical entity in the cloud that Oracle Communications Application Orchestrator considers to be a datacenter. For example, the vCloud cloud manager refers to the name of an OrgVDC. Click **Load** to display the fields and drop-down list described below.
Description field	The description that uniquely identifies this data center.
Caution field	(Read-only) This field cautions that the Fast Provisioning feature in vCloud must be disabled for this data center to prevent VM deployment failures. If the Fast Provisioning feature is not disabled, VMs can fail to deploy because this feature prevents the VMs from adjusting their storage volumes.
Cloud ID field	(Pre-populated) The secure web link for the data center cloud identifier.
Storage Profile drop-down list	(Pre-populated) The storage profile name used by this data center to allocate VM storage.
Storage Profile ID field	Click **Load** to enter the secure (HTTPS) web link for the data center cloud storage identifier. Click **Load** to populate this field with the web address.
Enable Anti-Afinity checkbox	(Optional) Check the checkbox and click **Load** to enable anti-affinity rules for high-availability (HA) paired VMs. An anti-affinity rule for VM pairs specify that individual VMs should not run on the same host. **Note:** If the **Enable Anti-Affinity** checkbox is checked, this storage profile must be backed by shared storage (storage volumes accessible to all hosts in the data center). If the storage provider contains any host local storage (storage not accessible by all hosts in the Datacenter), Anti-Affinity DRS rules may fail resulting in VM deployment failure.
VCenter URL field	The web link for the base URL to the vCenter server instance that backs the chosen Org VDC. Each Org VDC is backed by a Provider vDC, which is backed by an instance of vCenter. This parameter is required if anti-affinity rules are enabled.

Name	Description
VCenter Username field	The vCenter user name. This name does not necessarily need to be an administrator user, but must have access rights to create anti-affinity DRS rules for the VMs created by the vCloud user name.
VCenter Password field	The vCenter user password.

6. Click **OK** to register the data center for the VIM.

Deploy VM Application Images for Network Functions

The **VM Image Archive** pane allows you to manage all VM application images assigned to NF groups by a VIM. In order for a VIM to configure and deploy a VM instance, a VM application image (OVA) file must be uploaded to the archive.

A VM application image package is an .OVA file that contains a VM system configuration, which is the base operating system for VNF instances. NF groups require a specified image in order to deploy CNF instances. The following table describes specific VM information can be learned from the open virtualization format (OVF) XML file contained within the OVA. Oracle Communications Application Orchestrator can parse the valid elements from the XML file directory of an OVF to learn this information.

Note: Only virtual disks in the virtual machine disk (VMDK) format are currently supported for virtual hard disc drives. Only one **VirtualDisk** element is currently supported per OVF and there is no support currently for specifying multiple VMs in a single OVF with the **VirtualSystemCollection** element.

VM Information	Description

Software Version	XML file directory:
	/Envelope/VirtualSystem/ProductSection/FullVersion
	Example of software information parsed from the **FullVersion** element:
	Note: If the FullVersion element does not exist, the user must manually enter the software version in the Oracle Communications Application Orchestrator GUI.
	`<ProductSection ovf:required="false">`
	`<Info>VM ISV branding information</Info>`
	`<Product>NNOSVM</Product>`
	`<Vendor>Oracle</Vendor>`
	`<Version>7.2.9.0.1</Version>`
	`<FullVersion>SCZ7.2.9p1</FullVersion>`
	`<ProductUrl/>`
	`<VendorUrl/>`
	`</ProductSection>`

Number of CPUs	XML file directory: /Envelope/VirtualSystem/VirtualHardwareSection/Item/ResourceType[text() = '3']/../VirtualQuantity/text() Example of CPU information parsed from the **VirtualQuantity** element:

<table>
<tr><th>VM Information</th><th>Description</th></tr>
<tr><td></td><td>

```
<Item>

<rasd:AllocationUnits>hertz * 10^6</
rasd:AllocationUnits>
            <rasd:Description>Number
of virtual CPUs</rasd:Description>
            <rasd:ElementName>4
virtual CPU</rasd:ElementName>
            <rasd:InstanceID>1</
rasd:InstanceID>
            <rasd:Reservation>2000</
rasd:Reservation>
            <rasd:ResourceType>3</
rasd:ResourceType>
            <rasd:VirtualQuantity>4</
rasd:VirtualQuantity>
 </Item>
```

</td></tr>
<tr><td><b>Memory (Bytes)</b></td><td>

XML file directory:

/Envelope/VirtualSystem/VirtualHardwareSection/Item/ResourceType[text() = '4']/../VirtualQuantity/text()

Example of memory information parsed from the **VirtualQuantity** and **AllocationUnits** elements:

Note: The **VirtualQuantity** element is converted into bytes using the specified **AllocationUnits** element. Support for the **AllocationUnits** element is limited in the following ways:

- **byte**—The value of the **VirtualQuantity** element is taken as is.
- **byte * x^y**—The value of the **VirtualQuantity** element is multiplied by x^y.

```
<Item>

<rasd:AllocationUnits>byte * 2^20</
rasd:AllocationUnits>

<rasd:Description>Memory Size</
rasd:Description>

<rasd:ElementName>4096 MB of memory</
rasd:ElementName>
                <rasd:InstanceID>2</
rasd:InstanceID>

<rasd:Reservation>4096</
rasd:Reservation>
                <rasd:ResourceType>4</
rasd:ResourceType>

<rasd:VirtualQuantity>4096</
rasd:VirtualQuantity>
    </Item>
```

</td></tr>
<tr><td><b>Total Disk Capacity (Bytes)</b></td><td>XML file directory:</td></tr>
</table>

VM Information	Description

	/Envelope/DiskSection/Disk
	Example of memory information parsed from the **Disk** element:
	Note: The capacity of each **Disk** element is determined from the **ovf:capacity** and **ovf:capacityAllocationUnits** attributes. The specified **ovf:capacity** attribute is converted into bytes using the **ovf:capacityAllocationUnits** attribute. Support for the **ovf:capacityAllocationUnits** attribute is limited in the following ways:
	• **byte**—The value of the **ovf:capacity** attribute is taken as is.
	• **byte * x^y**—The value of the **ovf:capacity** attribute is multiplied by x^y.
	`<DiskSection>`
	`        <Info>List of the virtual`
	`disks and partitions needed</Info>`
	`        <Disk ovf:capacity="40"`
	`ovf:capacityAllocationUnits="byte *`
	`2^30" ovf:diskId="system"`
	
	`ovf:fileRef="system_disk_id"`
	`              ovf:format="http://`
	`www.vmware.com/interfaces/`
	`specifications/`
	`vmdk.html#streamOptimized"`
	
	`ovf:populatedSize="125829120"/>`
	`    </DiskSection>`

Network Interfaces	XML file directory:
	/Envelope/VirtualSystem/VirtualHardwareSection/Item/ResourceType[text() = '10']/..
	Example of network interface information parsed from the **VirtualHardwareSection Item** elements:
	Note: The name of each interface is parsed from the **rasd:Connection** element if it exists. If it does not exist, then a default of **ethX** is used where X starts at 0 and increases in increments of 1.
	`          <Item>`
	
	`<rasd:AddressOnParent>1</`
	`rasd:AddressOnParent>`
	
	`<rasd:AutomaticAllocation>true</`
	`rasd:AutomaticAllocation>`
	
	`<rasd:Connection>wancom0</`
	`rasd:Connection>`

VM Information	Description

	`<rasd:ElementName>Ethernet adapter on`
	`&quot;wancom0&quot;</rasd:ElementName>`
	`                <rasd:InstanceID>5</`
	`rasd:InstanceID>`
	
	`<rasd:ResourceSubType>E1000</`
	`rasd:ResourceSubType>`
	
	`<rasd:ResourceType>10</`
	`rasd:ResourceType>`
	`       </Item>`

Add a VM Application Image to Application Orchestrator

A VM application (OVA) image must be uploaded to the VM image archive in Oracle Communications Application Orchestrator before the VM application instance can be started by the VIM for a network function (NF).

1. Expand the **Application Orchestrator** slider and select **Administration** > **VM images**.
2. Click **Add**.
3. In the **Upload VM image to archive** dialog box, complete the following fields:

Name	Description
Name field	The unique name that is easily distinguishable within Oracle Communications Application Orchestrator for the VM application image.
Description field	A description of the VM application image.
File field	Click the **Browse** button to navigate to the new VM application image on your PC and select it.
Software version field	The VM application image version number appears automatically once the VM application image is uploaded. **Note:** If the OVA file identifier does not support this feature, the user needs to provide the software version number on which the image is based.
Component types field	Click the ellipsis (**...**). In the **Select supported component types** dialog box, a list of component types is provided that is supported by the plug-ins added to Oracle Communications Application Orchestrator. The appropriate component type needs to be selected for the uploaded image. Refer to the appropriate plug-in user documentation for more information about the component types associated with your CNF .

4. Click **OK**.
5. In the **Select supported hypervisor types** section of the **Upload VM Image to Archive** dialog box, select from the following supported hypervisor types on which the VM application can run by checking its check box:

   - **ESXi**—A VMware ESXi type is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers.
   - **KVM**—A Kernel-based Virtual Machine (KVM) type is a Linux kernel module that allows the system to act as a hypervisor.
   - **OVM_PV**— An Oracle Virtual Machine (OVA) para-virtualization (PV) type.
   - **OVM_HVM**—An Oracle Virtual Machine (OVA) hardware virtualized machine (HVM) type.

   Note: If the VM application image version number and hypervisor(s) on which this image runs cannot be determined, you are prompted to enter the VM application image version number and select and check the checkboxes for the hypervisor types on which the VM application can run.

6. Click **Apply** to upload the VM image.
   The VM image appears in the VM application image archive.

Manage VM Application Images

The VM Image Archive allows you to manage all VM applications (OVA images) that are maintained by Oracle Communications Application Orchestrator.

1. Expand the **Application Orchestrator** slider and select **Administration** > **VM Images**.
2. In the **VM Image Archive** pane, click the **Show All** button. The following columns are described for the VM applications in the archive:

Name	Description
Name field	The name of the VM software.
Image File Name field	The VM application image file name.
Hypervisor version	The hypervisor(s) on which VMs deployed from the VM Image can run. For example, ESXi.
Description field	The VM application image description.
Software field	The VM application OVA image version.
Size (Bytes) field	The VM application image file size.
Date/Time created field	The time stamp for when the VM application image was uploaded to the archive.
CPU	The number of CPUs allocated to a VM deployed from this VM application image.
Memory	The memory capacity in gigabytes allocated to a VM deployed from this VM application image.
Disk	The disk capacity in gigabytes allocated to a VM deployed from this VM application image.
# Network Adapters (NICs)	The number of NICs allocated to a VM deployed from this VM application image.

3. Choose from the following **Image Archive** pane buttons to manage VM applications.

Name	Description
Refresh button	Click to refresh the VM application image archive table.
Add button	Click to add additional VM applications.
Delete button	Click on an existing VM application image to delete this image from the image archive.
Search button	Click to search for a specific VM application image in the VM application image archive.

Purge User Logs

1. Expand the **Application Orchestrator** slider and select **Administration** > **Policies**.
2. In the **Purge Policies** pane, enter the number of days when user logs are purged from Oracle Communications Application Orchestrator in the **Interval in days** field.
3. Click **Apply**.

6

Register an Element Manager with Application Orchestrator

An Element Manager (EM) must be registered with Oracle Communications Application Orchestrator in order to stage a CNF from its CNF descriptor (CNFD). An EM supports a targeted CNF to determine resource usage requirements for the CNF and its collaboration with Oracle Communications Application Orchestrator.

Register Element Manager for CNF Collaboration

1. Expand the **Application Orchestrator** slider and select **Administration** > **EM registry**.
2. In the **EM Resgistry** pane, click **Add**.
3. In the **Add EM registry** pane, complete the following fields:

Name	Description
EM registration name field	The unique identifier of the registered EM. For example, **OCSEM Dallas**.
EM reference drop-down list	Select from the predefined EM list that references EM plug-in names.
User name field	The user name for EM access. For example: **AoSystem**.
Password field	The password necessary for EM access.
EM URL	Click **Add**. In the **Add EM URL** dialog box, add the URL necessary for EM access and click **OK**. 👉 **Note:** If the URL is https (secure HTTP), you must have a certificate uploaded in the Oracle Communications Application Orchestrator trust store. See the *Certificate Authentication* chapter for more information.

4. Click **Apply**.
   The EM is registered and saved.
5. In the success dialog box, click **OK.**
6. Click **Test connectivity** to test the connection between Oracle Communications Application Orchestrator and the EM.

Edit a Registered Element Manager

1. Expand the **Application Orchestrator** slider and select **Administration** > **EM registry**.
2. In the **EM resgistry** pane, click **Edit**.
3. In the **Edit EM registry** pane, complete the following fields:

   Note: If the EM registry is populated with many entries, click **Search**. In the Search EMS dialog box, enter the EM registration name that you want to find and edit, and click **OK**.

Name	Description
EM registration name field	The read-only unique identifier of the registered EM that you are editing.
EM reference drop-down list	The read-only EM name derived from the EM plug-in name you chose.
User name field	The user name for EM access.
Password field	The password necessary for EM access.
EM URL	Click **Add** to change the EM URL. In the **Add EM URL** dialog box, add the URL necessary for EM access and click **OK**.

4. Click **Apply**.
   The changes to the EM are saved.
5. Click **Test connectivity** to test the connection between Oracle Communications Application Orchestrator and the EM.

7

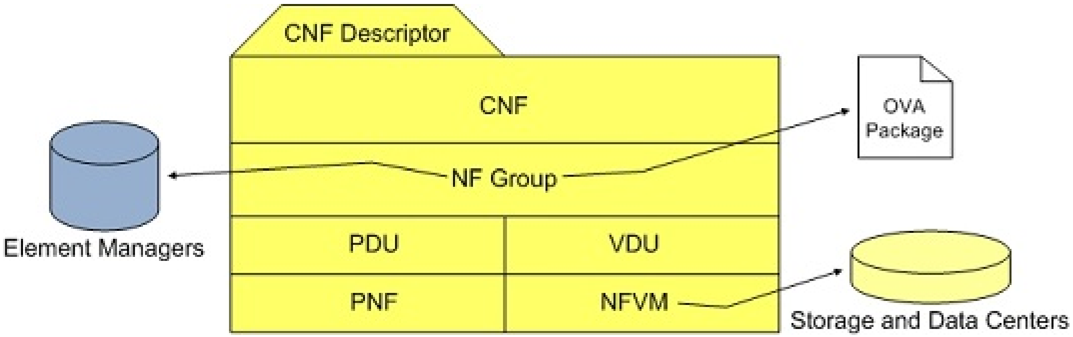
Operationalize a CNF Manually

The manual process of making a CNF operational is accomplished in three major steps: staging any pre-existing CNF from the catalog and promoting it, configuring the CNF NF group and DU parameters, and deploying the CNF and making it operational.

Staging and Promoting a CNF

You can stage any pre-existing CNF that is available in the CNF catalog and promote the CNF that you choose to a configurable CNF.

The CNF catalog is comprised of the list of composite network function descriptors (CNFD) that are provided by each plug-in. The CNFD communicates the deployment, operational behavior and policies that are needed to deploy and manage a single CNF to Oracle Communications Application Orchestrator, and contains information about its PNF and NFVM components.



View CNF Plug-ins

1. Expand the **Application Orchestrator** slider and select **Onboarding** > **Catalog**.
2. In the catalog table, the following columns display information about the pre-existing CNF plug-ins that come with Oracle Communications Application Orchestrator.

Name	Description
Name	The unique name of the CNF plug-in.
Version	The version of the CNF plug-in.
Description	The description of the CNF plug-in application image.

Name	Description
Vendor	The vendor of the CNF plug-in associated with the application image.
Vendor ID	The unique vendor ID of the CNF plug-in.

Stage and Promote a CNF to a Deployable State

Staging is the first phase of the CNF onboarding process. The CNF uses initial parameters (resource criteria) configured in the staging phase to calculate the sizing requirements and resources required for the CNF topology. Once the staging phase is started, the CNF displays the required parameters needed to eventually deploy the CNF. Each CNF plug-in stages the CNF based on its own criteria.

Promotion is the second phase of the CNF staging process. The staged CNF is promoted to a new CNF (with the name that you supply) that requires further configuration before it becomes deployable.

Stage the CNF Plug-in

Oracle Communications Application Orchestrator delegates the calculation of resource requirements to the CNF plug-in, which then returns the modified CNFD for display. For example, if you want to create a CNF that supports 20 million subscribers, the CNF plug-in returns a CNF that identifies all the NF groups, DUs, required IP addresses, and data centers needed to deploy it.

Note: The fields and values described in this task represent one type of CNF plug-in. If you are staging a different type of CNF plug-in, the fields described below and the values for them may not be the same.

1. Expand the **Application Orchestrator** slider and select **Onboarding** > **Catalog**.
2. In the **Composite network functions** pane, select the table row of a pre-existing CNF plug-in and click **Stage**.
3. In the **Stage CNF resources** dialog box, the following fields appear with pre-populated values that are specific to the type of CNF that is used.

   Note: The default resource criteria and parameters can be different for each CNF. Please refer to the appropriate plug-in documentation that supports the targeted CNF for a more detailed description of its resource criteria. This criteria affects the computed minimum or maximum number of DUs that are required.
4. If you decide to keep the default resource criteria or made changes, click **OK**.
   Oracle Communications Application Orchestrator automatically stages the CNF and the staged CNF appears in the **Staged CNFs** table.

Promote the CNF

1. Expand the **Application Orchestrator** slider and select **Onboarding** > **Catalogue**.
2. In the **Staged Composite Network Functions** table, the following column fields display:

Name	Description
Name	The CNF plug-in, NF Group, DU, and VM name in this tree hierarchy.
Resilience	The instantiated NFVMs that are maintained by a preferred or disaster fail-over data center.
Min # of management IP	The number of management IP addresses required for each of the following levels: • NFVM—One or two IP addresses depending on whether there is an HA deployment. • DU—The sum of all IP addresses for NFVM nodes. • NF group—The sum of all IP addresses for DU nodes. • CNF—The total number of IP addresses required to deploy the CNF.

Name	Description
Minimum CPU cores	The minimum number of required central processing unit (CPU) cores for each CNF, NF Group, DU, and NFVM level to deploy the CNF.
Minimum memory(GB)	The minimum memory in gigabytes (GB) required for each CNF, NF Group, DU, and NFVM level to deploy the CNF.
Minimum disk(GB)	The minimum disk space in GB required for each CNF, NF Group, DU, and NFVM level to deploy the CNF.
Minimum DUs	The minimum number of DUs required for this CNF.
Minimum hardware device	The PDU hardware device type.
Platform	The type of platform on which the DU is running.

3. Select the staged CNF row and click **Promote**.
4. In the **CNF staging settings** dialog box, complete the following fields:

Name	Description
CNF Name	The unique name for this deployed CNF. **Note:** The CNF name must be different from the CNF-plug-in name from which it was created.
Description	The description of the CNF, which may include how it is used or deployed.

Oracle Communications Application Orchestrator automatically promotes the staged CNF to the new CNF with the name that you supplied, calculates its required resources and the CNF now appears in the **Composite Network Functions** table showing its status as *Not Configured*.

View the Promoted CNF

A promoted CNF can contain multiple NF groups and each NF group serves as a container for a VDU or PDU that is used to maintain all virtual and physical device instances respectively that share identical policies, rules, and a common software image.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the deployed **Composite Network Functions** table, you can view the following column rows:

Name	Description
Name	The CNF name.
Status	The CNF state.
Deployed DUs	The number of successfully deployed DUs for this CNF.
Failed DUs	The number of DUs that have failed.
Minimum DUs	(Hidden) The minimum number of DUs.
Maximum DUs	(Hidden) The maximum number of DUs.
Description	The CNF description.
CNF plug-in name	(Hidden) The CNF plug-in name.

3. In this table, you can use the following table management actions:

Name	Description
Refresh button	Click to refresh the table contents.

Name	Description
Search button	Click to find a specific deployed CNF. In the **Composite Network Function search** dialog box you can configure the following parameters: • **Name**—The unique name for this deployed CNF. • **Description**—The description of the CNF, which may include how it is used or deployed. • **State**—The state of the CNF.

4. Select the deployed CNF row. You can use the following actions on the CNF you have chosen:

Name	Description
Expand button	Click to go to the **CNF Details** table where you can expand the CNF folder tree hierarchy containing its NF group(s) and DUs.
Edit button	Click to edit the CNF description and specify whether or not the CNF can be enabled to be set operational automatically.
Resize button	Click to adjust sizing parameters for CNF resources.
Auto operational button	Click to allow the CNF to set itself operational automatically after a DU spin-up.
Delete button	Click to delete a CNF that you have chosen.

5. Click **Expand**.
6. In the **CNF details** table, view the following detailed CNF information.

Note: Hidden columns can be made visible by hovering and clicking the down arrow to the right of the column header and choosing **Column** and checking the unchecked (hidden) columns that you want from the pop-up menu.

Name	Description
Name	The CNF, its NF groups, the DUs that belong to each NF group, and the network functions on virtual machines (NFVMs) and physical network functions (PNFs) that belong to each DU.
Resilience	(Hidden) Specifies if the NF group is a standalone or high availability (HA).
State	The state for each CNF, its NF groups, the DUs that belong to each NF group, and the NFVMs and PNFs that belong to each DU. See the following sections for more information about these states.
IP address	Either the NFVM or PNF device management IP address only.
Type	(Hidden) The type of DU that is in the NF group.
Deployed DUs	The number of deployed DUs for a CNF or NF group. For the CNF, this number represents the sum of all DUs belonging to each NF group. For the NF group, this number represents the sum of all DUs for this NF group. This includes DUs that have successfully deployed and DUs that failed to deploy.
Failed DUs	The number of DUs that failed to deploy for a CNF or NF group only. For the CNF, the number of failed DU is the sum of all failed DU for each NF group in this CNF. For NF group, the number of failed DU is the number of deployed DU in this NF group.
Minimum DUs	(Hidden) The minimum number of DUs required for this CNF.

Name	Description
Maximum DUs	(Hidden) The maximum number of DU capacity for a CNF or NF group. For the CNF, this number represents the sum of all DU capacity belonging to each NF group. For the NF group, this number represents the sum of all DU capacity for this NF group.
Virtual	(Hidden) A value of **true** specifies that the NF group contains NFVM and a value of **false** specifies that the NF group contains PNFs.
CPU capacity	The central processing unit (CPU) sum for the DU(s) currently in a running state.
Minimum CPU cores	(Hidden) The minimum number of required CPU cores for each CNF, NF Group, DU, and NFVM level to deploy the CNF.
Maximum CPU cores	(Hidden) The maximum number of required CPU cores for each CNF, NF Group, DU and NFVM level to deploy the CNF.
Memory capacity	The memory allocation sum for the DU(s) currently in a running state.
Minimum memory (GB)	(Hidden) The minimum memory in gigabytes (GB) required for each CNF, NF Group, DU, and NFVM level to deploy the CNF.
Maximum memory (GB)	(Hidden) The total memory resources required for a CNF, NF group, or DUs.
Disk capacity (GB)	The disk usage sum for the DU(s) currently in a running state.
Minimum disk (GB)	(Hidden) The minimum disk space in gigabytes required for each CNF, NF Group, DU, and NFVM level to deploy the CNF.
Maximum disk (GB)	(Hidden) The total disk resources required for a CNF, NF group, or DUs.
Platform	(Hidden) The type of platform on which the DU is running on if it is a PDU.
Parent ID	(Hidden) The number that indicates the hierarchy level of the CNF component.

7. You can use the following tree table action buttons and drop-down list in the expanded CNF view:

Name	Description
Refresh button	Click to refresh either the brief CNF view or expanded CNF tree contents.
Expand All button	Click to expand the tree hierarchy.
Collapse All button	Click to collapse the tree hierarchy.
Logs button	Click the appropriate CNF, NF group, virtual deployment unit (VDU) or physical deployment unit (PDU) to view a log of all the tasks that run on an NF group and its DUs.
Manage drop-down list	The different options for managing a CNF, NF group, a DU and its devices are available depending on what node you select from the tree. See the following **Management Functions for a Promoted CNF** section for more information.
Auto button	Click to enable the NF group capacity planner to automatically start a scaling process when required (NF group node only).
Manual button	Click to manually deploy or undeploy a DU (NF group node only).
Back button	Click to return to the **Deployed CNF** table.

View CNF Deployment States

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.

2. In the deployed **Composite Network Functions** table, select the CNF and click **Expand** to go to the **CNF details** table where you can expand the CNF folder tree hierarchy containing its NF group(s) and DUs.
3. In the **CNF details** table, the following table describes the states that can appear for a CNF.

Name	Description
Not Configured	One or more child NF groups or DUs require user inputs.
Not Deployed	All required user inputs have been specified. The CNF is ready to be deployed.
Deploying	The CNF is in the process of being deployed.
Operational Ready	The CNF has one or more DUs that are ready to be set to an operational state.
Setting Operational	The CNF is in the process of setting its DUs to an operational state.
Set Operational Error	This state indicates that the process of setting the CNF operational failed (a DU failed to be in a set operational state). The user can retry setting the CNF to operational.
Running	The CNF and all of its DUs are in an operational state.
Undeploying	The CNF and its DUs are in the process of undeploying.
Deployment Error	An error was encountered while deploying the CNF and its DUs.
Deleting	The CNF is in the process of being permanently deleted from Oracle Communications Application Orchestrator. The CNF must be in an **Undeployed** state before deletion.
Delete Error	The CNF failed to delete.
Undeployment Error	An error was encountered while undeploying the CNF.
Resizing	The CNF is in the process of resizing. Resizing allows the minimum and maximum number of DUs to change over the lifecycle of the CNF to meet future capacity requirements.
Completing Resize	The CNF is completing the resize process. During this operation, new DUs may be deployed for each NF group to satisfy new minimum DU requirements.
Resize Error	An error was encountered while resizing the CNF.

View NF Group Deployment States

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the deployed **Composite Network Functions** table, select the CNF and click **Expand** to go to the **CNF details** table where you can expand the CNF folder tree hierarchy containing its NF group(s) and DUs.
3. In the **CNF details** table, the following table describes the states that can appear for an NF group.

Name	Description
Not Configured	The NF group requires additional user inputs.
Partially Configured	The NF group received all of the required user inputs, but its DUs still require additional user inputs. Specifically, the NF group remains in the **Partially Configured** state until its minimum number of DUs are fully configured.
Not Deployed	The NF group and its DUs are fully configured and ready for deployment.
Deploying	The NF group, and its minimum number of DUs are being deployed.
Operational Ready	One or more DUs are ready to be set to an operational state.

Name	Description
Setting Operational	The NF group and its DUs are being set to an operational state.
Set Operational Error	An error was encountered when the NF group DUs were set to an operational state.
Running	The NF group and all of its DUs are in an operational state.
Deploying DU	The NF group is scaling out (horizontally) by deploying a DU.
Undeploying DU	The NF group is scaling in (horizontally) by undeploying a DU.
Undeploying	The NF group is in the process of undeploying. All deployed DUs are undeployed during this process.
Deployment Error	The NF group encountered an error while deploying the minimum DUs.
Undeployment Error	The NF group encountered an error while undeploying all DUs.

View DU and DU Node Deployment States

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the deployed **Composite Network Functions** table, select the CNF and click **Expand** to go to the **CNF details** table where you can expand the CNF folder tree hierarchy containing its NF group(s) and DUs.
3. In the **CNF details** table, the following table describes the states that can appear for a DU and its DU nodes.

Name	Description
Not Configured	The DU nodes of a DU require additional configuration inputs from the user.
Not Deployed	The DU and its nodes are fully configured and ready for deployment.
Deploying	The DU and its nodes are in the process of being deployed.
Activation Ready	The DU and its nodes completed the initial deployment phase and are ready to be activated by EMS.
Activating	The DU and its nodes are in the process of being activated.
Activated	The DU and its nodes completed the activation process.
Sending Notifications	The DU and its nodes are sending scale out or *scale in* notifications to registered endpoints to indicate their availability on the network.
Operational Ready	The DU and its nodes are ready to be set to an operational state.
Setting Operational	The DU and its nodes are being set to an operational state.
Set Operational Error	An error was encountered while setting the DU to an operational state.
Running	The DU and its nodes are in an operational state.
Undeploying	The DU and its nodes are in the process of being undeployed.
Undeployment Error	An error was encountered while undeploying the DU and its nodes
Deployment Error	An error was encountered while deploying or activating the DU.

Manage Functions for the Promoted CNF

This task shows how you can manage operations for a promoted CNF, its NF groups, DUs, and DU nodes in the folder tree hierachy.

Note: Manual mode must be enabled in Oracle Communications Application Orchestrator to deploy or undeploy DUs.

Operationalize a CNF Manually

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the deployed **Composite Network Functions** table, select the CNF and click **Expand** to go to the **CNF details** table where you can expand the CNF folder tree hierarchy containing its NF group(s) and DUs.
3. Click the CNF folder and select **Manage** drop-down list to perform the following actions on the CNF:

Name	Description
Set operational	Select to begin the process of setting a CNF and its DUs to an operational state.
Deploy	Select to begin the process of deploying a CNF.
Redeploy	Select after a CNF deployment fails to try a subsequent attempt to deploy this CNF. This attempt to regain a successful status starts from the point at which the previous deployment failed.
Undeploy	Select to begin the CNF undeployment process.
Complete resizing	Select after the resizing process is initiated (a new sizing criteria is entered and promoted). This operation completes the resizing process. New DUs are deployed to satisfy the new minimum DU requirements for each NF group.

4. Click the NF group folder, select **Manage** drop-down list, and select **Edit**.
   The **Edit NF group** dialog box for the NF group displays its configuration on each tab for you to edit.
5. Click the DU folder and select **Manage** drop-down list to perform the following actions on the DU:

Name	Description
Deploy	Select to begin the process of deploying a DU.
Undeploy	Select to begin the DU undeployment process.
Force undeploy	Select only after the undeployment of a DU has failed. This action is used as a measure of last resort. When you select this action, the undeployment process is tried again, but this time several failures as possible are tolerated. This action allows Oracle Communications Application Orchestrator to continue an undeploy operation even when it has lost connectivity to a third-party VIM or EMS system. This can result in abandoned VMs or other Oracle Communications Application Orchestrator-provided configuration data on the third-party system.

6. Click the DU node, select **Manage** drop-down list, and select **Edit**.
   The **Configuration** dialog box for the DU node displays its configuration on each tab for you to edit.

Configure the CNF

The tasks in this chapter are used to configure scaling, cloud attributes, and networking parameters for an NF group belonging to the promoted CNF so that it can be put into a deployable state.

Note: The parameters and fields described in this chapter for a promoted CNF may be different than the parameters and fields that you see for your CNF depending on the type of CNF that you decided to use.

The tasks in this chapter must be completed to put the CNF into a deployable state.

Enable Auto-scaling for an NF Group

The NF group for a deployed CNF is in manual mode by default (auto-scaling is not enabled). The NF group for a deployed CNF can be enabled to auto-scale DUs based on KPIs, rules, and policies to meet the current capacity requirements of a network.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.

2. In the deployed **Composite Network Functions** table, select the CNF and click **Expand**.
3. In the **Composite Network Function details** detailed view, click the CNF folder to expand it, select an NF group, and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF Group** pane, click the **Settings** tab to view NF group parameters for a CNF:

Name	Description
Name	(Pre-populated) The NF group name.
Description	The NF group description.
CNF plug-in type drop-down list	(Pre-populated) The CNF plug-in type is provided by Oracle Communications Application Orchestrator.
Component type drop-down list	(Pre-populated) The vendor component type.
Virtual/physical radio button	(Pre-populated) Either a virtual deployment unit (VDU) or physical deployment unit (PDU) is selected for the NF group.
Maximum DUs field	(Pre-populated) The maximum number to DUs that can be deployed for this NF group.
Minimum DUs field	(Pre-populated) The minimum number to DUs that can be deployed for this NF group.
Auto-scaling check box	The NF group is in manual mode by default (the auto-scaling checkbox is unchecked). To enable auto-scale mode for the NF group, check the check box.

5. Click **Apply** to set your changes to the description of the NF group.
6. In the success dialog box, click **OK**.

Add a Registered Element Manager to the NF Group

Use this task to configure options required by the element manager so that it can collaborate with Oracle Communications Application Orchestrator to manage the life cycles of each DU in the NF group.

Note: The fields and values described in this task show the parameters common to all configurations that assign an EM to an NF Group. See your specific plug-in user guide for more information about the parameters associated with its EM requirements.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF** to navigate to the **Deployed CNF** table.
2. Select a CNF from the **Deployed CNF** table and click **Expand**.
3. In the CNF detailed view, select an NF group and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF Group** pane, click the **EM** tab and complete the following fields:

Name	Description
VM image drop-down list	In the **Version** content area of the pane, select an existing VM image from the **VM image** drop-down list that is populated with all the VM images which are tagged with the component type of the NF group. Click **Load** to confirm your selection. The plug-in is notified that a VM image was selected, and the plug-in can use this information to re-render the parameters on the page to fit the software version of the selected VM. **Note:** No VM image options are available in the drop-down list if there are no VM images that support the component type of the NF group.
Software version field	The VM image software version.

Name	Description
EM reference field	The type of EM device as it was pre-defined by the CNFD. This field is read-only. For example: **OCSEM** (Oracle Communications Session Element Manager).
EM registration name drop-down list	Select the unique name of the registered EM that you want this NF group to use. For example, **OCSEM Dallas**. Select from the predefined EM list that references EM plug-in names. **Note:** Select **None** if there is no registered EM involved in making the CNF operational.

5. Click **Apply**.

Associate a DU with a Data Center

After VIM(s) are added to Oracle Communications Application Orchestrator, multiple data centers register with the VIM(s). Each DU must be associated with one or more data centers.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select a CNF and click **Expand**.
3. In the CNF detailed view, select an NF group and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF Group** pane, click the **Data centers** tab.
5. Select a DU node (which is populated depending on the resilience policy) from the **Data center association** table and click **Associate Data center**.

   Note: If the resilience policy has geo-redundancy, two DU nodes are displayed (one is preferred and the other is for disaster recovery). This allows each node to be assigned data-centers that are not co-located. An HA pair that is redundant has two DUs. If an NF group resilience policy does not include geo redundancy, only the preferred option is available.
6. In the **Associate data center** dialog box, select one or more data centers to associate with this DU node.
7. Click **Associate**.
   The DU node displays the data centers associated with this DU node in the **Map networks to interfaces** table.
8. Map any of the network interfaces (pre-populated by the VIM) for each VM instance to a virtual cloud network or datacenter network using the drop-down menu for each relevant interface.

   Note: You must associate at least one network interface to a virtual cloud network or datacenter network.
9. If the DU node is an HA pair with Geo-redundancy, repeat the previous steps for either the preferred or disaster recovery DU node.
10. Click **Apply**.

Specify Common Boot Parameters

Common boot parameters for all NFVM instances associated with each DU of the NF group can be configured in the DU tab. These are delivered along with the targeted device specific parameters to the appropriate VIM when a set of NFVMs is to be instantiated. The parameters provided here depend on the requirements of the vendor product. See your specific vendor plug-in documentation for more details.

The table in **Edit NF group** pane displays all the data centers (preferred and disaster recovery) that were associated with the NF group. For each data center, you must configure a set of parameters that are applied to all VNFs deployed to the data center. For example, these parameters can be used to ensure that all VNFs deployed to a single data center share a common network configuration such as the same network mask or default gateway.

Note: Boot parameters are not configured for PDUs because it is a prerequisite that physical devices be bootstrapped and reachable by an EMS.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.

2. In the **Deployed CNF** table, select the CNF and click **Expand**.
3. In the CNF detailed view, select an NF group and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF Group** pane, click the **DU** tab.
5. Select a data center and click **Configure**.
   The **Configure common DU settings** dialog box appears where you can configure attributes that are specific to the NF component of the plug-in that is specific to the CNF being deployed.
6. Click **OK**.
7. In the the **DU** tab, click **Apply**.

Configure Scaling Notification Messages

The Oracle Communications Application Orchestrator publishes notification messages (NM) each time a scaling event occurs. The dependent groups are used to construct a valid NM, which Oracle Communications Application Orchestrator publishes to the rest of its domain. External systems such as an EMS and NSO can register through the REST API interface to receive these notifications.

> **Note:** We recommend that you do not modify CNF NM dependencies and messages and keep with the original intent of the CNF. The ability to configure scaling notification messages is considered to be an advanced feature, therefore changes to NM dependencies and messages should occur only if a copy of the original CNF is used for a network domain solution for which it was not intended. Please consult your Oracle support professional services for proper guidance.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select a CNF and click **Expand**.
3. In the CNF detailed view, select an NF group and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF Group** pane, click the **Notifications** tab.
5. In the **Add Dependent NF Group** dialog box, select a dependent NF group from the **NF Group** drop-down list.
   The NF group appears in the **Dependent NF Groups** table.
6. Click **OK**.
7. Below the **Notification Messages** table, click **Add** to add a dependent NF group that belongs to the same CNF.
8. In the **Add Notification Message** dialog box, complete the following fields:

Name	Description
Target component type drop-down list	Select a pre-populated component type for the notification message sent to the EM.
Condition drop-down list	The scaling condition for which the notification message is sent to the EM. For example, **ScaleUp**.
Name field	Select the scaling notification metadata message name created by the EM and learned by Oracle Communications Application Orchestrator from the RMS NM template configured in the EM. For example, **CSMAdded**.

9. Click **OK**.
   The notification message appears in the **Notification messages** table.
10. Click **Apply**.

Manage NF Groups through KPI Thresholds

The KPI scaling policy for an NF group is pre-defined by the CNF with scale down and load shedding KPI values. The KPI scaling policy is different depending on which CNF is chosen. The CNF determines the capacity scaling process for where the resources are and how the NF group scales vertically (scales up or down) or horizontally (scales in or out) based on its domain knowledge. Vertical scaling consumes or releases resources that are added to a running DU instance such as CPU, Memory, etc., dependent on a scaling up or scaling down event.

In Oracle Communications Application Orchestrator Release 1.1, vertical scaling is restricted to the first instantiation of the NFVM in an NF Group. Dynamic vertical scaling is not supported. Horizontal scaling equally consumes or releases resources to a running DU instance such as CPU, Memory, etc., dependent on a scaling out or scaling in event. Dynamic horizontal scaling to allow for elastically is supported.

The parameters provided in this task are subject to the scaling policy enforced by the targeted CNF. The default scaling policy is the Oracle Communications Application Orchestrator standard scaling policy that is discussed in this section. For other non-default scaling policies, please see the specific vendor plug-in documentation for more details.

Use this task to change parameters for the default KPI scaling policy provided by the CNF plug-in if needed.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select a CNF and click **Expand**.
3. In the CNF detailed view, select an NF group and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF Group** pane, click the **KPIs** tab and complete the following fields:

Name	Description
Load shedding KPI field	This is the KPI metric used for DU load shedding. A default KPI is chosen by the plugin. The chosen KPI is used to determine when the load on a DU has reduced enough so that the DU can be undeployed without major service disruption. The default pre-populated KPI scaling policy name provided by Oracle Communications Application Orchestrator for DU load shedding.
Load shedding threshold field	(Optional) Enter the load-shedding threshold raw value for the chosen load shedding KPI used by the standard Oracle capacity planner for load shedding during a scale-in scenario. Load shedding is the process of reducing traffic from a DU in order to facilitate a graceful shutdown in order to limit service disruption. In this example, the DU would be undeployed when the active calls falls below 50 For example, you can choose the **active calls** for the Oracle **Load shedding KPI** scaling policy and have the **Load shedding threshold** parameter set to **50** percent. In this scenario, the capacity planner determines (based on NF group defined KPI thresholds) that the current KPI capacity of all deployed DUs in the NF group can be maintained by fewer DUs than are currently deployed (scale-in scenario). To limit service disruption, the capacity planner selects the DU which has the lowest number of *active calls*. This DU is then set *offline*, which means that the DU continues to service existing calls, but does not accept new calls. Since the DU is not accepting new calls, the number of *active calls* decreases over time. Only when the number of active calls has fallen below the defined threshold of 50 does the capacity planner begin the DU undeployment process. The DU is not undeployed until its active number of calls reaches 0.
Load shedding timeout field	(Optional) Enter the load shedding timeout in minutes. This is the time Oracle Communications Application Orchestrator waits for load shedding to statically go below the threshold value. After this time, the DU is shutdown and resources are reclaimed (even if the load is reached before the above threshold, the DU is ready to be un-deployed). If you enter **0**, there is no timeout, and load shedding continues until the load shedding threshold is crossed.

5. Click **Apply**.

Add a KPI Threshold Policy

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select a CNF and click **Expand**.
3. In the CNF detailed view, select an NF group and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF group** pane, click the **KPIs** tab.
5. Below the table of KPI thresholds, click **Add**.
6. In the **Add KPI threshold** dialog box, complete the following fields:

   Note: The **Relative limit** applies to all policies (not just the standard scaling policy), **Warning %**, **Critical %**, **Growth Duration** and **Decline Duration** parameters apply to the default scaling policy for Oracle session delivery network element CNF plug-ins and are unique to the component type. The KPI metrics available are unique to each component type, but the fields mentioned in this note apply to all thresholds when using the standard scaling policy. See your plug-in vendor user documentation for different threshold parameters for the targeted CNF.

Name	Description
Name drop-down list	Select from the following pre-populated KPI scaling policy name provided by the CNF: **Note:** This drop-down list contains different KPIs depending on the component type and software version that the NF group is managing. See specific CNF plug-in documentation for additional information. • **Calls Per Second** • **System State** • **Memory Utilization** • **CPU Utilization** • **Active Local Contacts** • **Active Sessions**
KPI name field	The pre-populated KPI name. For example: **apSysGlobalCPS**
Description field	The pre-populated KPI description. For example: **Calls Per Second**
Enable threshold check box	Check the check-box to enable the KPI threshold policy. The fields described below appear.
Relative limit field	The "soft" maximum limit value which provides the basis for calculating a KPI value as a percentage on a per NF device basis. For example, a NF device might be capable of 1000 active calls.
Warning % field	The percentage relative to the specific **Relative Limit** parameter. When this limit is crossed, the capacity planner begins a timer. When the timer exceeds the specified **Growth Duration** parameter, the spin-up of DU resources begins. This field applies to the default Oracle scaling policy.
Critical % field	The percentage at which the immediate spin-up of resources occurs for a DU. This field applies to the Oracle default scaling policy.
Growth Duration field	The minutes to wait after the warning threshold is crossed before a spin-up of resources occurs for a DU. This field applies to the Oracle default scaling policy.
Decline Duration field	The minutes to wait before a spin-down of resources occurs for a DU. This field applies to the Oracle default scaling policy.

7. Click **OK**.
8. Click **Apply**.

Edit an Existing KPI Threshold Policy

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select a CNF and click **Expand**.
3. In the CNF detailed view, select an NF group and click the **Manage** drop-down list and click **Edit**.
4. In the **Edit NF group** pane, click the **KPIs** tab.
5. Select a KPI threshold policy from the table of KPI thresholds and click **Edit**.
6. In the **Edit KPI threshold** dialog box, edit the following fields as needed:

   Note: The **Relative limit**, **warningThreshold**, **criticalThreshold**, **growthDuration** and **declineDuration** parameters apply to the default scaling policy for Oracle session delivery network element CNF plug-ins. See your plug-in vendor user documentation for different threshold parameters.

Name	Description
Name drop-down list	The pre-populated KPI scaling policy name provided by the CNF plug-in.
KPI name field	The pre-populated KPI name.
Description field	The pre-populated KPI description.
Enable threshold check box	Check the check-box to enable or disable the KPI threshold policy.
Relative limit field	The "soft" maximum limit value which provides the basis for calculating a KPI value as a percentage on a per NF device basis. For example, a NF device might be capable of 1000 active calls.
Warning % field	The percentage relative to the specific **Relative Limit** parameter. When this limit is crossed, the capacity planner begins a timer. When the timer exceeds the specified **Growth Duration** parameter, the spin-up of DU resources begins. This field applies to the default Oracle scaling policy.
Critical % field	The percentage at which the immediate spin-up of resources occurs for a DU. This field applies to the Oracle default scaling policy.
Growth Duration field	The minutes to wait after the warning threshold is crossed before a spin-up of resources occurs for a DU. This field applies to the Oracle default scaling policy.
Decline Duration field	The minutes to wait before a spin-down of resources occurs for a DU. This field applies to the Oracle default scaling policy.

7. Click **OK**.
8. Click **Apply**.

Configure VDU Boot Loader Parameters

Each DU node containing a data center VM device must be configured for a CNF. This type of DU node can also be referred to as a virtual DU or VDU. Data center VM devices can either be singular or HA-paired VNF deployments.

Note: A VDU cannot deploy unless device-specific boot parameters are configured.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select a CNF and click **Expand**.
3. In the **CNF details** pane, select a DU node data center VM device (For example, NFVM1), and click the **Manage** drop-down list and click **Configure**.
4. In the configure panel, click the data center VM device in the table, and click **Configure**.
5. In the **NFVM** tab, complete the following fields to configure parameters for the device boot loader program that loads an operating system on data center VM device(s) associated with the VDU node.

Note: The following parameters apply to the Oracle session delivery network element CNF plug-ins. See your vendor plug-in vendor documentation for more information about the targeted CNF in which you are interested.

Name	Description
IP Address field	Enter the IP address of the VM device. For Oracle session delivery network VMs, this is the management IP address that is assigned to the **wancom0** VM interface. The EMS uses this IP address to communicate with the VM. **Note:** If the VDU policy is for HA, there are two IP address fields (one field for each data center VM device).
Targetname field	Enter the name of the VM device associated with this DU node. For example: sbc10. If you are using an Oracle session delivery network VM, the target name is the same thing as a VM host name.

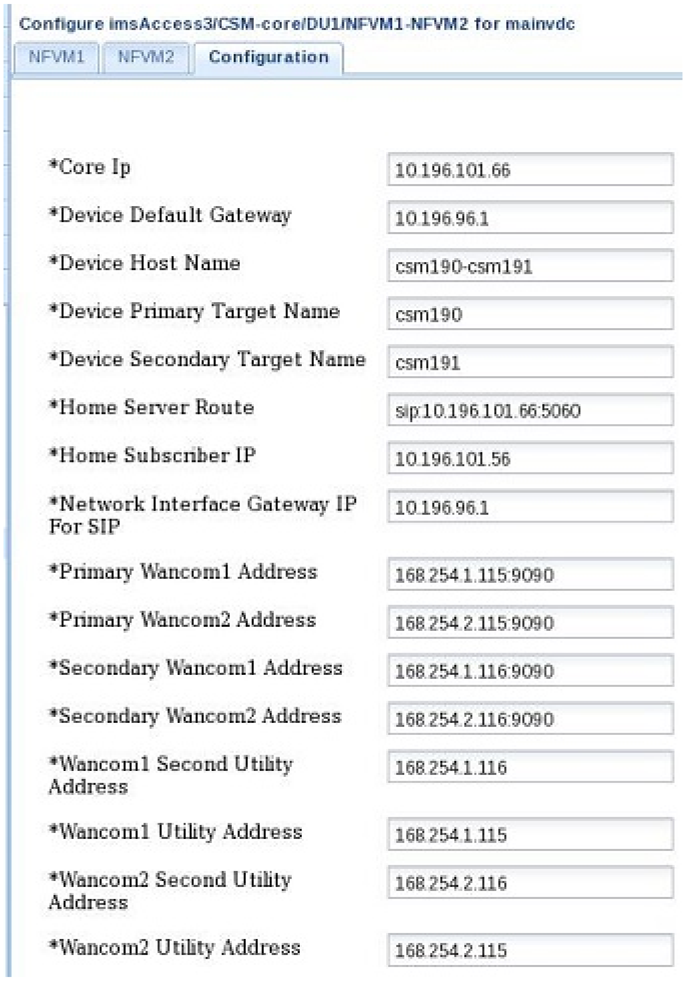
6. Click **Apply**.
7. Repeat this task to configure any remaining VDU node VM devices for the NF group.

Configure Device Specific Parameters for a DU

Device-specific support for the configuration of VDU or PDU devices is provided in Oracle Communications Application Orchestrator. This support is provided only if the device-specific configuration parameters are supported for other plugins that may not use a configuration template. The Offline Configuration is an Oracle Communications Session Element Manager plugin-specific concept has defined data-binding variables, which appear for a DU in the **Configuration** tab. If you need help configuring these data-binding variables or need a full description of the content that may appear in your configuration template, see the specific vendor plug-in user documentation that supports the targeted CNF for more information.

Note: A DU node (PDU or VDU) that has device-specific parameters cannot reach a configured state unless these device-specific parameters are defined in the **Configuration** tab.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select a CNF and click **Expand**.
3. In the **CNF details** pane, select a DU node data center VM device (For example, NFVM1), and click the **Manage** drop-down list and click **Configure**.
4. In the configure panel, click the data center VM device in the table, and click **Configure**.
5. In the **Configuration** tab, complete the fields that were defined by data-binding variables in your targeted offline configuration to configure device-specific parameters for the VM device(s) associated with the VDU or PDU node. The following figure shows an example of the **Configuration** tab populated with device-specific parameters and their specified entries:



Configure imsAccess3/CSM-core/DU1/NFVM1-NFVM2 for mainvdc

*Core Ip	10.196.101.66
*Device Default Gateway	10.196.96.1
*Device Host Name	csm190-csm191
*Device Primary Target Name	csm190
*Device Secondary Target Name	csm191
*Home Server Route	sip:10.196.101.66:5060
*Home Subscriber IP	10.196.101.56
*Network Interface Gateway IP For SIP	10.196.96.1
*Primary Wancom1 Address	168.254.1.115:9090
*Primary Wancom2 Address	168.254.2.115:9090
*Secondary Wancom1 Address	168.254.1.116:9090
*Secondary Wancom2 Address	168.254.2.116:9090
*Wancom1 Second Utility Address	168.254.1.116
*Wancom1 Utility Address	168.254.1.115
*Wancom2 Second Utility Address	168.254.2.116
*Wancom2 Utility Address	168.254.2.115

Figure 11: Configuration tab populated with device-specific parameters and entries

6. Click **Apply**.
7. Repeat this task to configure any remaining VDU or PDU node VM devices for the NF group.

Deploy and Make the CNF Operational

Once all NF group and DU parameters have been configured for a promoted CNF that is in a deployable state, the CNF (and its nodes) is deployed and made operational.

Deploy a CNF for the First Time

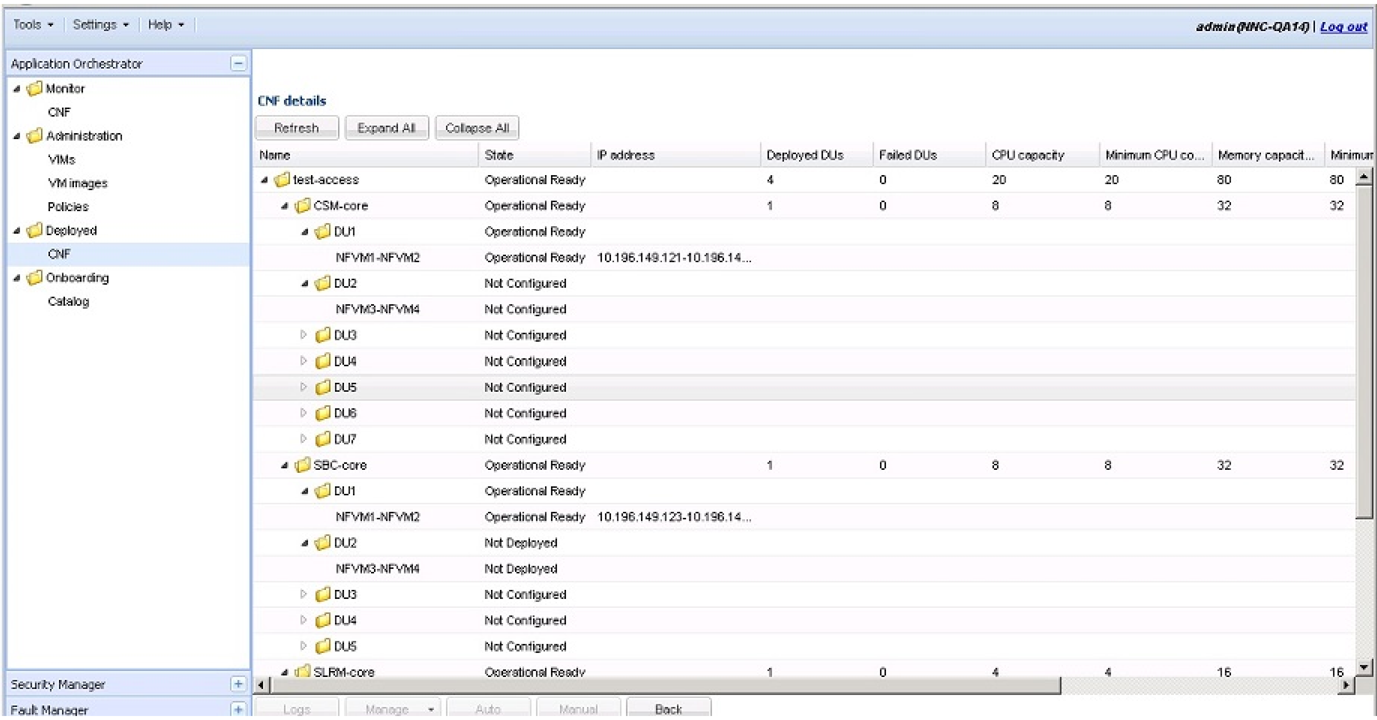
Use this task to deploy the CNF into an operational ready state in which a configured CNF made up of interdependent, linked NF groups and DUs are ready to be activated together.

1. Ensure that all required configuration parameters for the promoted CNF are configured so that it can be deployed and made operational.
2. Ensure that the CNF has the minimum number of DUs configured before the DU can be entered into a deployable state. The minimum and maximum number of DUs depends on the sizing criteria configured when staging the CNF.
3. Oracle Communications Application Orchestrator indicates at each level (CNF, NF group, DU) when a state has been reached from not configured to configured. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF** to see the state for each CNF, its NF groups, the DUs that belong to each NF group, and the NFVMs and PNFs that belong to each DU.

4. In the **Composite network functions** pane, select the CNF from the table and click **Expand**.
5. View the **State** column to learn the status of your CNF. See the *View CNF Deployment States* section in the *Staging and Promoting a CNF* chapter for more information.
6. In the **Composite network functions** pane, select the CNF and click the **Manage** > **Deploy**.
   The configured CNF is deployed when all DUs deploy, including their nodes. Once the status of the CNF and all its nodes are in the **Operational_Ready** state, the CNF is ready to become operational.
7. Click **Refresh** to check the status of the CNF, NF groups, and DUs as they deploy.

   Note: The CNF does not deploy if required configuration parameters for the promoted CNF are not configured or configured incorrectly.

8. Ensure that the CNF is deployed completely. Oracle Communications Application Orchestrator does not allow DUs to be deployed individually until the CNF to which it belongs is instantiated for the first time.
9. If your CNF, NF group(s) or DU(s) fail to deploy, do the following:
   a) Select the CNF and click **Logs** to view the log messages for the CNF. Reasons for a failure appear in the **CNF logs** dialog box. For example, if the `Please verify that 'Fast Provisioning' is disabled for Datacenter` error message appears in the CNF log dialog box, there is a problem with the provisioning of your VIM that conflicts with Oracle Communications Application Orchestrator.
   b) Check the offline configuration, VIM, or NF group parameters for any configuration problems.
   c) There may be a scenario in which any combination of DU(s) or NF group(s) fail to deploy, but others succeed to deploy into an operational ready state. In this scenario, click each failed NF group or DU, click **Undeploy**, and select the CNF and click **Redeploy**. This action can save time because you do not have to undeploy and redeploy NF group(s) or DU(s) that have already deployed into an operational ready state.
10. Once your CNF and its NF group(s) and DU(s) are deployed, they display the **Operational Ready** state as shown in the following figure.



CNF details

Name	State	IP address	Deployed DUs	Failed DUs	CPU capacity	Minimum CPU co...	Memory capacit...	Minimur
test-access	Operational Ready		4	0	20	20	80	80
CSM-core	Operational Ready		1	0	8	8	32	32
DU1	Operational Ready							
NFVM1-NFVM2	Operational Ready	10.196.149.121-10.196.14...						
DU2	Not Configured							
NFVM3-NFVM4	Not Configured							
DU3	Not Configured							
DU4	Not Configured							
DU5	Not Configured							
DU6	Not Configured							
DU7	Not Configured							
SBC-core	Operational Ready		1	0	8	8	32	32
DU1	Operational Ready							
NFVM1-NFVM2	Operational Ready	10.196.149.123-10.196.14...						
DU2	Not Deployed							
NFVM3-NFVM4	Not Deployed							
DU3	Not Configured							
DU4	Not Configured							
DU5	Not Configured							
SLRM-core	Operational Ready		1	0	4	4	16	16

Figure 12: CNFs in an Operational Ready State

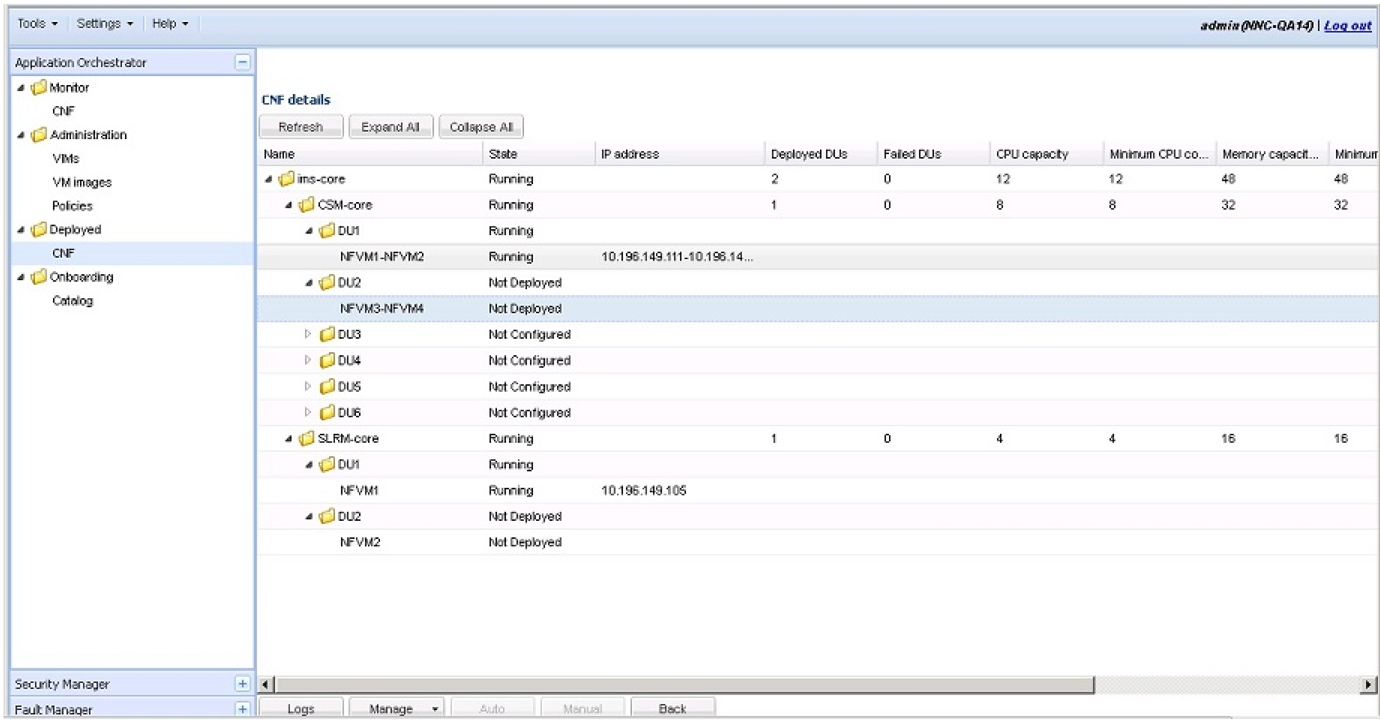
Make a Configured CNF Operational

A CNF is ready to be put into an operational state once the CNF is deployed and is in an **Operational Ready** state.

Ensure that the CNF and its NF group(s) and DU(s) are in an **Operational Ready** state before making the CNF operational.

Operationalize a CNF Manually

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select the configured CNF and click **Expand**.
3. In the **Composite Network Function details** pane, select the CNF node.
4. Click the **Manage** drop-down list and select **Set Operational**.
   Oracle Communications Application Orchestrator applies the configuration on the EMS and the CNF becomes operational. The CNF appears in **Running** state in the **Composite Network Function details** pane table as shown in the following figure.



Name	State	IP address	Deployed DUs	Failed DUs	CPU capacity	Minimum CPU co...	Memory capacit...	Minimum
ims-core	Running		2	0	12	12	48	48
CSM-core	Running		1	0	8	8	32	32
DU1	Running							
NFVM1-NFVM2	Running	10.196.149.111-10.196.14...						
DU2	Not Deployed							
NFVM3-NFVM4	Not Deployed							
DU3	Not Configured							
DU4	Not Configured							
DU5	Not Configured							
DU6	Not Configured							
SLRM-core	Running		1	0	4	4	16	16
DU1	Running							
NFVM1	Running	10.196.149.105						
DU2	Not Deployed							
NFVM2	Not Deployed							

Figure 13: Running CNFs

8

Build the Hierarchical Service Configuration

The Hierarchical Service Configuration (HSC) helps Oracle Communications Application Orchestrator automate the deployment, scaling and resizing of a CNF. The HSC must be configured before you can configure the REST API for the northbound client (such as a northbound service orchestrator (NSO)). Once the HSC and REST API are configured, the northbound client can be used to operationalize a CNF.

☞ **Note:** Oracle Communications Application Orchestrator must be able to connect to an EM to access configuration templates that the EM supports before virtual resources, network resources, and configuration parameters are provided to an external northbound service orchestrator. See your EM vendor documentation to determine if there is a need to register an external EM with the API REST callback mechanism implemented.

The HSC is a high-level template that can be configured to link a set of pre-existing configuration templates that belong to multiple NF groups together and associate their connectivity from one or more EMs. The HSC abstracts the configuration details and complexity of each NF group and provides its client (for example, an NSO) a single HSC interface for configuration information and inputs. These inputs are implicitly translated into configuration inputs for NF groups to hides any complex, confusing, or duplicated information from its client.

The northbound service orchestrator (client) application gathers configuration information from this HSC from Oracle Communications Application Orchestrator. This information includes resource criteria from the CNF descriptor of a CNF plug-in and resource requirements from the resource criteria for a CNF with a list of NF groups, connection points, end points, subnets, and virtual links.

Parameters are used to fill HSC input for the northbound service orchestrator and are defined in the HSC by a user to link or map the HSC inputs into the configuration input of each applicable NF group. The parameters that the northbound service orchestrator gathers from the HSC in Oracle Communications Application Orchestrator are obtained through a series of REST API calls with Oracle Communications Application Orchestrator. Through this series of REST API calls, the northbound service orchestrator is able to prompt Oracle Communications Application Orchestrator to deploy and operationalize a CNF.

☞ **Note:** See the *Oracle Communications Application Orchestrator REST API Guide, CNF Operations* chapter for information about configuring the external northbound service orchestrator application with the HSC REST API calls necessary for communicating with Oracle Communications Application Orchestrator.

The HSC feature also is used for CNF resource scaling and resizing events.

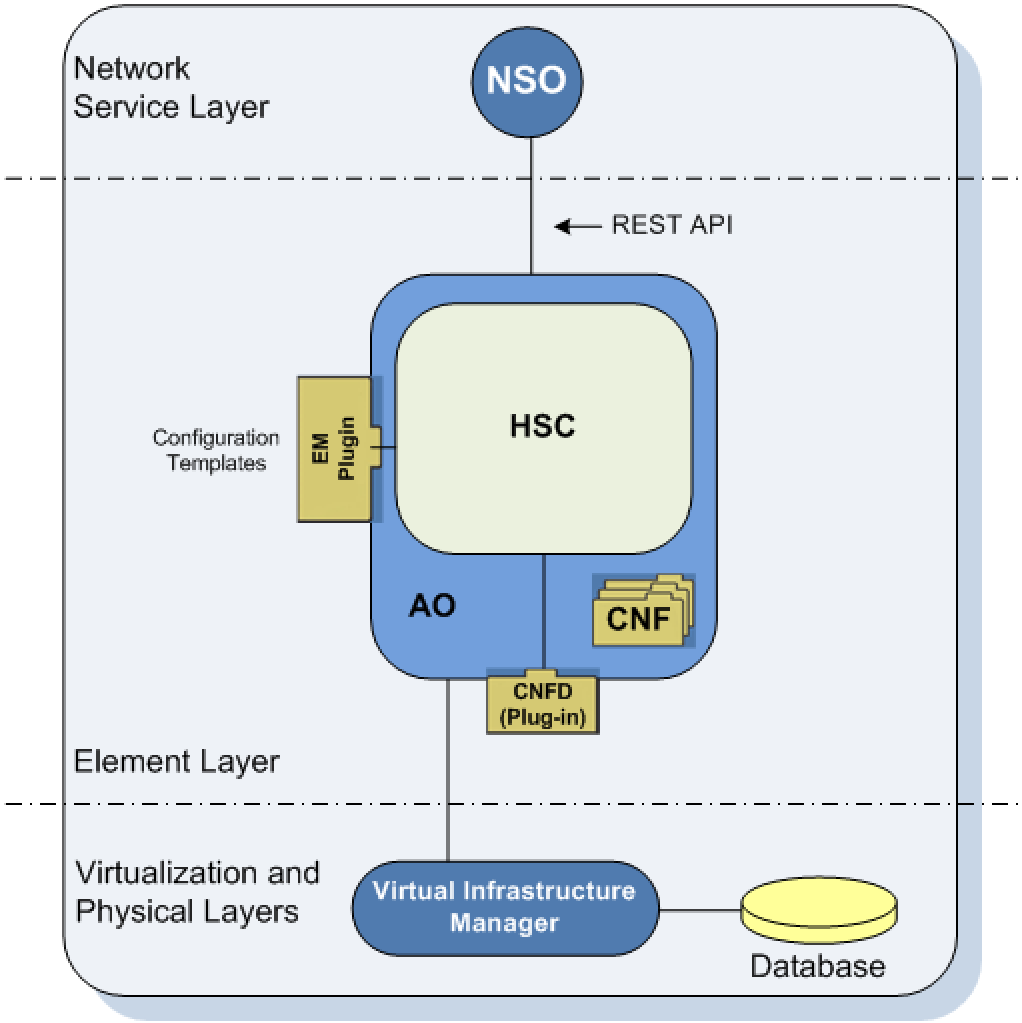


Figure 14: Northbound service orchestrator interaction with Oracle Communications Application Orchestrator and the HSC feature

HSC Data Structure Relationship to OSI Layers

The following figure shows the HSC data structure and its relationship with the OSI layers. Oracle Communications Application Orchestrator retrieves all connection points from EM plugin, which are physical interface connection points (CPs) at Layer 1/Layer 2. Virtual links (vLinks) are formed by CP associations, which are also at this layer. End points (EPs) exist from Layer 3 to 7 in their respective subnetworks, which have a one-to-one relationship with their respective connection point (CP).

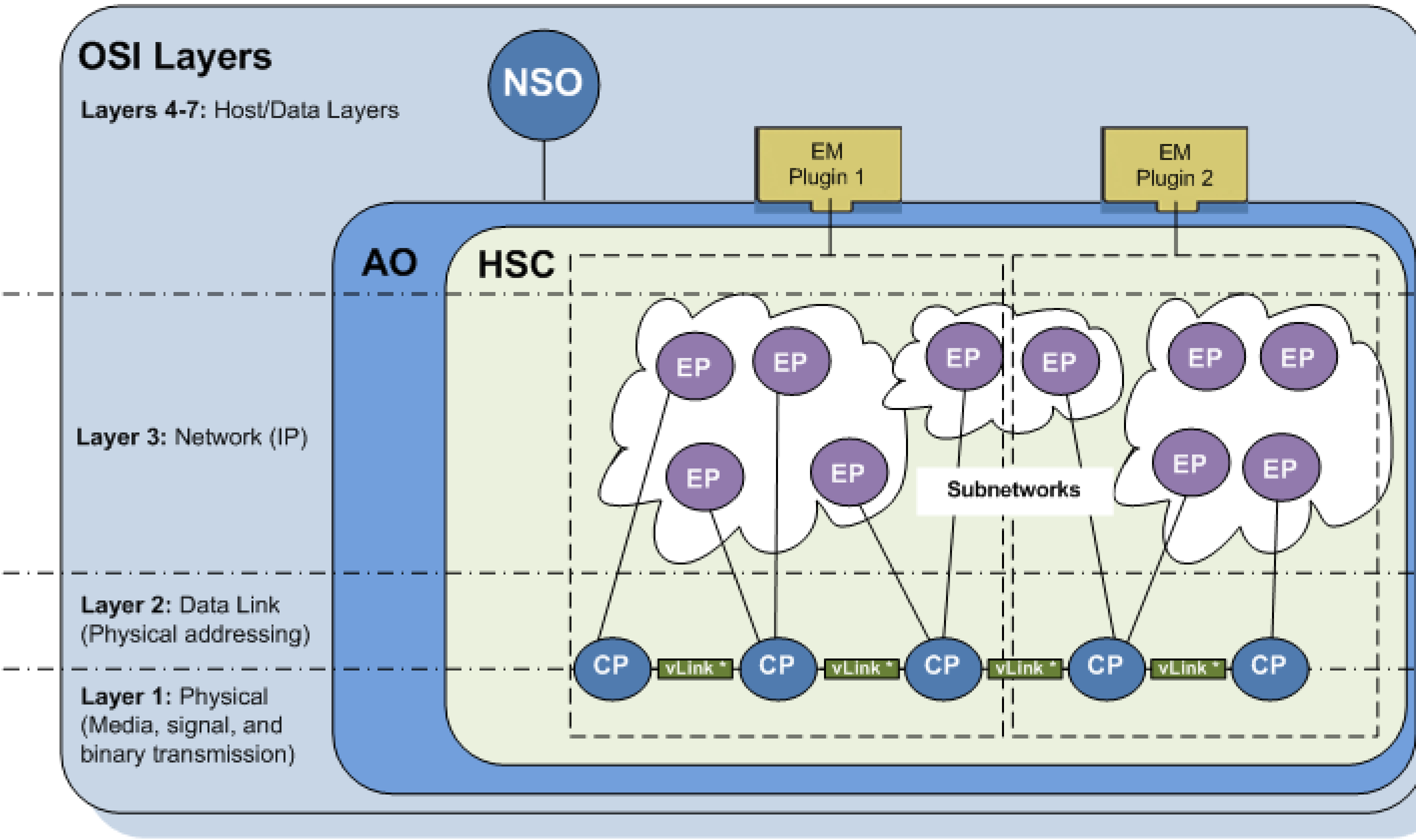

OSI Layers
Layers 4-7: Host/Data Layers
NSO
EM Plugin 1
EM Plugin 2
AO
HSC
Layer 3: Network (IP)
EP
Subnetworks
Layer 2: Data Link (Physical addressing)
Layer 1: Physical (Media, signal, and binary transmission)
CP
vLink *

Figure 15: HSC Data Structure Relationship to OSI Layers

EM plugins are used to reduce the amount of configuration necessary to create an HSC instance by providing Oracle Communications Application Orchestrator with CPs, subnetworks, and EPs and input for all OSI layers. In typical network configurations, several EM plugins are used to provide this information to create an HSC instance. An EM allows each EM plug-in to automatically generate an HSC configuration database using the capabilities of the plugin. The more HSC data that a plugin generates, the less configuration that an HSC user needs to do manually. Due to the complexity of a typical network configuration and the number of devices used in a typical configuration, some manual configuration is necessary to create an HSC. The EM plugin is however is able to provide all or partial HSC core data for the following parameters:

- All CPs in Layer 1 and 2.
- All subnetworks (at least the VLAN information for each subnetwork) in Layer 3.
- Some or all EPs in Layer 3 (for example: network interfaces).
- Zero or more EPs in Layers 4 to 7.
- Parameters for any EPs generated automatically in any layers.

Any EPs, parameters, virtual links and their association to connection points that the EM plugin cannot provide must be entered manually by the user in Oracle Communications Application Orchestrator for an HSC.

HSC Configuration Overview

The following sections provide a brief overview for how the HSC is configured in Oracle Communications Application Orchestrator GUI, and how HSC inputs are provided later in the Oracle Communications Application Orchestrator REST API.

Configure the HSC in the GUI

Use the following steps to configure the HSC in the Oracle Communications Application Orchestrator GUI. These steps are discussed in more detail later this chapter.

1. Add an HSC.
2. Select a pre-defined CNFD for creating an HSC, and add or edit virtual link(s), connection points (CPs), and end points (EPs) for this HSC.

   Note: You cannot edit the CNFD.

Provide Values for HSC Inputs in the REST API

You must provide values for the HSC inputs in the REST API of a northbound service orchestrator (NSO) after you configure the HSC parameters in the Oracle Communications Application Orchestrator GUI. See the Oracle Communications Application Orchestrator REST API Guide for more detailed information about the steps and HSC operations described below.

1. Configure all HSC parameters in the Oracle Communications Application Orchestrator GUI.
2. Provide values for the HSC inputs in the Oracle Communications Application Orchestrator REST API for an NSO.
3. The NSO sends a request to Oracle Communications Application Orchestrator with the sizing criteria, etc.
4. Oracle Communications Application Orchestrator replies with this information.
5. The NSO responds to Oracle Communications Application Orchestrator with the sizing and payload information (for example, the subnetwork, IP addresses, etc.) learned through the HSC.
6. Use the HSC feature in Oracle Communications Application Orchestrator to operationalize a CNF.

Add an HSC

Add a unique HSC that is associated with a specified CNF descriptor (CNFD).

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**.
2. In the **Hierarchical Service Configuration** pane, click **Add**.
3. In the **Add hierarchy service configuration** pane, complete the following fields:

Name	Description
Name field	The unique name for this HSC. For example, HSCforNewEngland.
Description field	The description for how this HSC is used.
CNFD field	The CNF descriptor that identifies the CNF plug-in used by the HSC to build its configuration. If you want a list of CNFDs (plug-ins) to choose from, click the ellipsis button (**...**). In the **Select CNFD** dialog box, select the CNFD and click **Apply**.

4. Click **Apply**.
   The unique HSC is built in Oracle Communications Application Orchestrator, which is used by the northbound service orchestrator to help it work with Oracle Communications Application Orchestrator to operationalize a CNF.

Edit the HSC You Added

After a unique HSC is added and selected, it appears in the **Settings** tab on the **Edit HSC** pane as being in a **Not Configured** state. The NF groups, virtual links, connection points, end points, and subnet parameters for this HSC must be edited or added in their respective tabs, before the HSC enters a configured state where it can be used by the northbound service orchestrator and Oracle Communications Application Orchestrator to operationalize a CNF.

Edit HSC NF Group CNFD Settings

Select and edit the HSC that you added to configure all NF groups and their associated configuration settings provided by the CNF Descriptor (CNFD).

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**.
2. In the **Hierarchical Service Configuration** pane, select the HSC that you just added and click **Edit**.
3. In the **Edit HSC** pane, view the **Settings** tab that appears first among the **Virtual Links**, **Connection Points** and **End Points** tabs. Review the appropriate HSC fields:

Name	Description
Name	The (read-only) unique name of the HSC. For example, CSM-core.
Description	Enter a description for the added HSC.
State	The state of this HSC is **Not_Configured** since it is being configured for the first time.
CNFD	The device platform name on which this CNF is based. This is derived from the CNFD.
Created by	The Oracle Communications Application Orchestrator system user who created this HSC.
Create date	The date on which this HSC is created.
Last modified date	The last time this HSC was modified.

The **NF Groups** table displays the NF group(s) that belong to this HSC:

Note: The information in this table depends on the CNFD of the plugin that is used.

Name	Description
Name	The unique name of an NF group within the CNFD. For example, CSM-core.
Component type	The type of device that the NF group supports, which is supplied by the CNFD.
State	The NF group can be in a **Configured**, **Not_Configured**, or in a **Sync_Required** state. **Note:** If this is the first time that you are editing an HSC, the state of this field is in a **Not_Configured** state. HSC states are discussed in more detail later in this chapter.
Target Resync	The check boxes displayed in this column are used to resynchronize the data for each NF group with its corresponding CNF plugin for the HSC. This feature is used if any changes were made to the configuration template (for example, the offline configuration in Oracle Communications Session Element Manager). See the steps below for more information about using this feature.
Platform	The platform name of the device software for which this NF group is based. This value is supplied by the CNFD.
Software Version	The device software version for which this NF group is based, which is supplied by the selected VM image.
VM image	The VM image name. If you want to select a different available VM image name, select it from the drop-down list.
Description	The description of the NF group.

Name	Description
Registered EM	(Hidden) The name of the registered and available EM plugin used for this NF group. If you want to select a different registered EM, select it from the drop-down list. The EM type(s) are defined for an NF group in the CNFD.

4. In the **NF Groups** table, select an NF group, and click **Edit**.
5. In the **Edit HSC's NF group** pane, complete the fields that you want to edit:

Name	Description
Name field	(Read-only) The NF group name.
Component type field	(Read-only) The NF group device type.
Description field	The description of the NF group.
EM type field	(Read-only) The EM type used for this NF group. For example: OCSEM.
Registered EM drop-down list	Select an EM that is registered with Oracle Communications Application Orchestrator. Select **None** if your implementation of a plugin does not require an EM.
Platform field	(Read-only) The platform name of the device software for which this NF group is based. This value is supplied by the CNFD.
VM image drop-down list	The default VM image name. Select a different VM image name if necessary.
Software Version field	The device software version for which this NF group is based, which is supplied by the selected VM image.
Template drop-down list	Click **Load** to load the configuration template associated with this NF group.
State field	Displays the synchronization status of the NF group.

6. In the **Notification messages** section, you can click **Add** to add a notification message and configure its parameters or select an existing notification message and click **Configure** to edit its parameters.
7. In the **Add notification message** or **Configure notification message** dialog box, complete the following fields:

Name	Description
Target component type drop-down list	Select a pre-populated component type for the notification message sent to the EM.
Condition drop-down list	The scaling condition for which the notification message is sent to the EM. For example, **ScaleUp**.
Name field	The scaling notification metadata message name created by the EM and learned by Oracle Communications Application Orchestrator from the RMS NM template configured in the EM. For example, **CSMAdded**.

Note: The fields in the **Add notification message** or **Configure notification message** dialog box may be different depending on the CNFD of the plugin that you are using.

8. Click **OK**.
9. (Optional) Click the **Target Resync** check box for each NF group to resynchronize all NF group data with their respective CNF plugins or click **Check All** to check all NF groups.

   Note: Click **Uncheck All** if you want to uncheck all NF groups.

10. Click **Resync** if your NF group is in a **Sync_Required** state or if you targeted other NF groups for synchronization before going to the next tab.

The state of a synchronized NF group displays as **Sync_Completed**. Any auto-generated CPs, EPs, or data variables of the configuration template are synchronized and saved to the database. Any differences between the last synchronization and the resynchronization are updated to the HSC database.

11. Click **Apply**.
    The NF group data for the HSC is saved, and the **Virtual Links** displays.

Add a Virtual Link

This task is used to add a virtual link between two or more connection points that are created dynamically between two end points on top of a physical infrastructure. A virtual link is made at layer 1 and 2 of a network. This virtual link is associated to a connection point (CP) to construct a model of how devices connect to the network.

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**.
2. In the **Hierarchical Service Configuration** pane, select the HSC that you just added and click **Edit**.
3. In the **Edit HSC** pane, click the **Virtual Links** tab.
4. If virtual links are being configured for the first time, the table is empty. Click **Add** to add a virtual link.
5. In the **Add virtual link** dialog box, complete the following fields:

Name	Description
Name field	The unique name of this virtual link within this HSC.
Description field	The user-defined description of the virtual link.

Edit the Description of a Virtual Link

This task is used to view a virtual link and edit its description if necessary.

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**.
2. In the **Hierarchical Service Configuration** pane, select the HSC that you want to edit and click **View**.
3. In the **Edit HSC** pane, click the **Virtual Links** tab.
4. Select a virtual link from the table and click **View** to edit the description for a virtual link.
5. In the **Edit virtual link** dialog box, view the fields and edit the **Description** field if necessary:

Name	Description
Name field	The unique name of this virtual link within this HSC.
Link Type field	The link type appears as either **Virtual** or **Physical**.
Description field	The user-defined description of the virtual link.
QoS check boxes	(Read only) The following fields show the service (QoS) policy for endpoints over the virtual link: • Bandwidth (MB) • Latency • Jitter • Packet loss • Out-of-Order Delivery Error • Low throughput • Errors

Edit Connection Points to Virtual Links

This task is used to edit layer 2 connection points for a logical entity, such as NF groups, to their respective virtual links.

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**.

2. In the **Hierarchical Service Configuration** pane, select the HSC that you just added and click **Edit**.
3. In the **Edit HSC** pane, click the **Connection Points** tab.
4. Click **Edit**.
5. In the **Edit connection points** dialog box, view the following fields and edit a virtual link for an NF group and the description of the CP if necessary:

Name	Description
NF group field	The read-only (component) type of NF group to which a CP belongs. For example, SLB-core
Geo Segment field	The read-only (static) name of the geo segment used to group the CPs and end points (EPs) in different locations for the purpose of providing geographical redundancy for them. The EM populates this field for each CP. The values for this field are either **Preferred** or **Fault_Tolerant**.
Interface Name field	The read-only (static) name of the interface NIC. For example, M01, S0P1, wancom0. The configuration template uses the static NIC reference as the interface name in a one-to-one pairing. **Note:** For Oracle Communications Session Element Manager plug-ins, the interface name can be configured in the offline configuration to be any valid string entered by user for the name attribute in the **Physical Interface** element.
NIC reference field	(Hidden) This field applies only to Oracle Communications Session Element Manager plug-ins. The read-only (static) name of the physical NIC. For example, there are eight predefined static physical interfaces: S0P0, S0P1, S1P0, S1P1, wancom0, wancom1, wancom2, spare.
Description field	The description of the CP and for what it is used.
Associated virtual link drop-down list	Select a virtual link name to associate with an NF group.

6. Click **Apply** and **Continue** to confirm your changes.
7. In the success dialog box, click **OK**.

Configure End Points

End points (EPs) are specified for logical layer 3 through 7 device EPs on the network. An EP contains a collection of configuration input parameters, which are categorized by type (that is, IP, netmask, gateway, etc).

An EM can allow an EP to be shared within a configuration template or across different templates so that this EM can discover what data is shared with it for a northbound client application.

Add Endpoints to a Subnetwork

You can add an end point (EP) to an existing subnetwork.

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**.
2. In the **Hierarchical Service Configuration** pane, select the HSC that you just added, and click **Edit**.
3. In the **Edit HSC** pane, click the **End Points** tab.
4. In the **Subnetwork** table, select a subnetwork.
   The empty **End point** table is populated with EPs associated with the selected subnetwork.
5. Below the populated **End Point** table, click **Add** to add an endpoint.
6. In the **Add end point** dialog box, complete the following fields:

Name	Description
Name field	The name of the new EP.
Description field	The description of this EP.
Exposure drop-down list	Select **Internal** or **External** to indicate whether the EP is internal or external to the subnetwork (CNF).
NF Group drop-down list	Select the name of the NF group to which this EP belongs. You can select the name of the NF group provided by the plug-in or **SHARED-BY-GROUPS**. The **SHARED-BY-GROUPS** option allows the EP to be configured so that a parameter with same name can point to multiple parameters in a single configuration template or across configuration templates used by different NF groups.
Geo Segment drop-down list	Select the name of the Geo segment to which this EP belongs (**Preferred** or **Fault Tolerant**). The Geo segment is used to group the CPs and EPs in different physical locations for the purpose of geographical redundancy.
Subnetwork field	The subnetwork ID to which this EP belongs.

7. Click **Apply**.
   The parameter that you configured appears in the **Config parameters** table.
8. Click **Apply**.

Edit Subnetwork End Points

In Oracle Communications Application Orchestrator, each subnetwork has one or more end points (EPs) that contain configuration parameters that describe the properties and characteristics of its EP(s) and the way these EP(s) map to targeted NF group configuration template variables. Use this task to edit the EPs of a defined subnetwork.

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**.
2. In the **Hierarchical Service Configuration** pane, select the HSC that you just added and click **Edit**.
3. In the **Edit HSC** pane, click the **End Points** tab. The **Subnetwork** and **End Point** tables display. The **Subnetwork** table depends on the state of the CPs being associated to a virtual link. Each CP association operation may result in addition of a new subnet to the table automatically, and each CP dissociation operation may result in the deletion of an existing subnet automatically.
   a) A dash (—) in the subnetwork table indicates that the subnetwork is undefined because the EPs belonging to it are undefined. To assign any undefined EPs to a subnetwork, select the subnetwork entry with a dash by selecting its row.
   b) Alternately, you may want to edit a defined subnetwork to edit its EP(s). Select the subnetwork entry that you want to edit.

   The **Subnetwork** table contains the following columns.

Name	Description
Name field	The name of the virtual link.
Vlan field	The VLAN number that is pre-defined for this subnet by its configuration template. For Oracle Communications Session Element Manager, the VLAN number is pre-defined by the Offline Configuration.
# of EPs field	The number of EPs created in this subnetwork.

   The empty **End point** table is populated with EPs associated with the selected subnetwork.
4. Select an EP from the **End points** table.
5. In the **Edit EP** dialog box, view and complete the following fields:

Name	Description
Name field	The name of the EP. The EP name is determined by the specific plugin. For example, a plug-in might use prefix NF-group-name/given-name, where the given name is the actual network interface name and VLAN number from the configuration.
Description field	The description of this EP.
Auto Generated field	(Read-only) Indicates whether this EP is auto-generated by the element manager (EM) (**True**) or by the user (**False**).
Exposure drop-down list	Select **Internal** or **External** to indicate whether the EP is internal or external to the subnetwork (CNF).
NF Group field	The name of the NF group to which this EP belongs. • If the **SHARED-BY-GROUPS** parameter was selected from the **NF Group** drop-down list when this EP was added, this field can be edited. • If the EP belongs to this NF Group only, this field is read-only.
Geo Segment field	(Read-only) The name of the Geo segment to which this EP belongs (**Preferred** or **Fault Tolerant**). The Geo segment is used to group the CPs and EPs in different physical locations for the purpose of geographical redundancy. The EM populates this field for the auto-generated EPs. User-created EPs are populated manually by a user.
Vlan field	(Read-only) The VLAN number that is pre-defined for the subnet by its configuration template. For Oracle Communications Session Element Manager, the VLAN number is pre-defined by the Offline Configuration.
Subnetwork field	(Hidden) The subnetwork ID to which this EP belongs.
Parent CP	(Hidden) The parent CP to which this EP belongs. **Note:** Some EPs that are not IP or connection-related may not have a parent CP.

6. Next click **Add**.
7. In the **Add parameter** dialog box, add a configuration parameter for your EP by completing the following fields:

Name	Description
Param name:	Select the unique parameter that you want to use with this EP. If there is no name to select, specify the name of this parameter.
Param type	Select the type of parameter this EP is using. For example, IPv4, IPv6, Mac, SubnetGateway, etc.
NF group	(Read-only) Indicates the NF group to which this EP belongs.
Template name field	(Read-only) The configuration template that you are using that maps to this variable. For example, If you are using Oracle Communications Session Element Manager, the offline configuration template might be CSM_Standalone_SlrmLink.
Variable type drop-down list	Select **Template** or **Bootparameter** for the type of variable that you are using for this EP. Either variable is required to place the NF group to be in a **Configured** state. • If you select **Template**, this drop-down list is populated with data variables from the target configuration template.

Name	Description
	• If you select **Bootparameter**, this drop-down list is populated with a specific boot parameters list.
Variable name drop-down list	Click **Load** to load a list of variables based on the variable type you specified and select the variable that you want.
Description field	The description of the parameter that you configured.

8. Click **Apply**.
   The parameter that you configured appears in the **Config parameters** table.
9. Click **Apply**.

User Actions for HSC Status Conditions

You can check the main status of one or more HSCs (configured or not configured) in the main HSC pane. To find specific information about the status of NF group(s) belonging to an HSC that is in a **Not Configured** state, you can edit the HSC to view NF group information in the **Settings** tab to decide what actions you need to do in order to get this HSC into a **Configured** state.

The following flow diagram describes the different status scenarios for HSC NF groups:

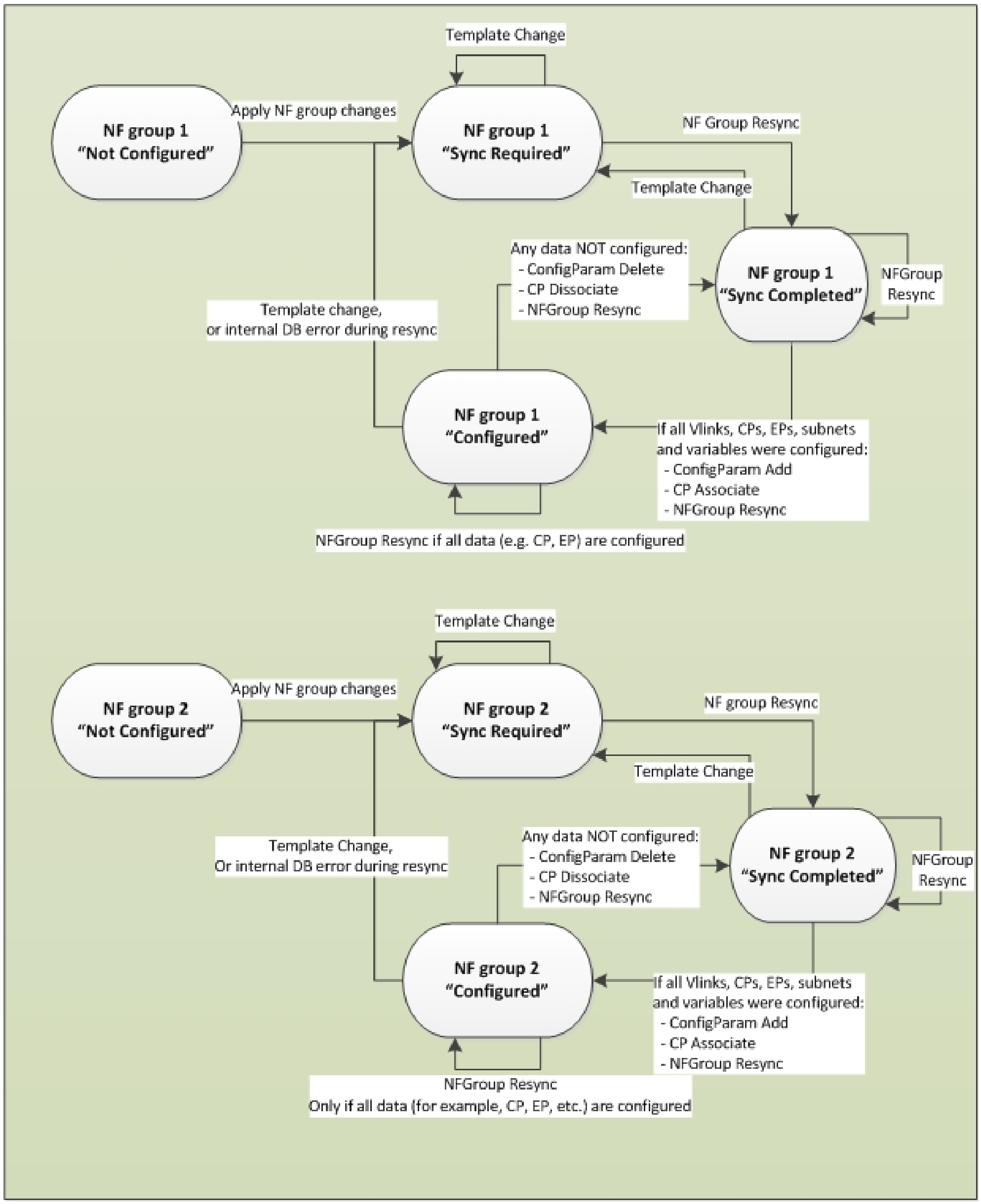


Figure 16: HSC NF group status scenarios

The following table describes the different GUI actions taken to transfer an NF group from one state to another:

NF Group State: From	NF Group State: To	Action
Not Configured	**Sync Required**	Enter and apply the following required NF group fields: • Registered EM • VM image • Template
Sync Required	**Sync Completed**	Resynchronize the NF group once the following data is obtained from the EM plugins and saved to the database: • Connection points (CPs)

NF Group State: From	NF Group State: To	Action
		• End points (EPs) • Subnetwork information
Sync Completed	**Configured**	The NF group is in a configured state when: • All CPs of the NF group are associated to a vLink. • All EPs of the NF group are properly configured. For example, the subnetwork field must be populated. • All template and boot parameter variables from the NF group are mapped to configuration parameters.
Configured	**Sync Completed**	Resynchronize the NF group if the following parameters are not configured: • Connection points (CPs) • End points (EPs) • All template and boot parameter variables are mapped from the target NF group.
Configured	**Configured**	Resynchronize the NF group if the following parameters are configured: • Connection points (CPs) • End points (EPs) • All template and boot parameter variables are mapped from the target NF group.
Configured	**Sync Required**	Resynchronize the NF group if the EM configuration template changed (which can occur when an EM registers), or there was an internal DB error during resynchronization.

Check the HSC Deployment Status

The HSC deployment status can be checked to determine if an HSC is deployed to form a CNF by a northbound client application, such as an NSO. If this is the case, the cnfName field of the HSC is populated and implies that the HSC deployment status is Deployed. If the cnfName field is empty, a new HSC or an HSC that is undeploying, the deployment status is Not Deployed.

The following table describes HSC deployment status, HSC state, user access for HSC provisioning, NF group resynchronization permission, NF Group change permissions (configuration template, VM image, and registered EM), and whether or not a description is allowed to be entered by a user for the HSC:

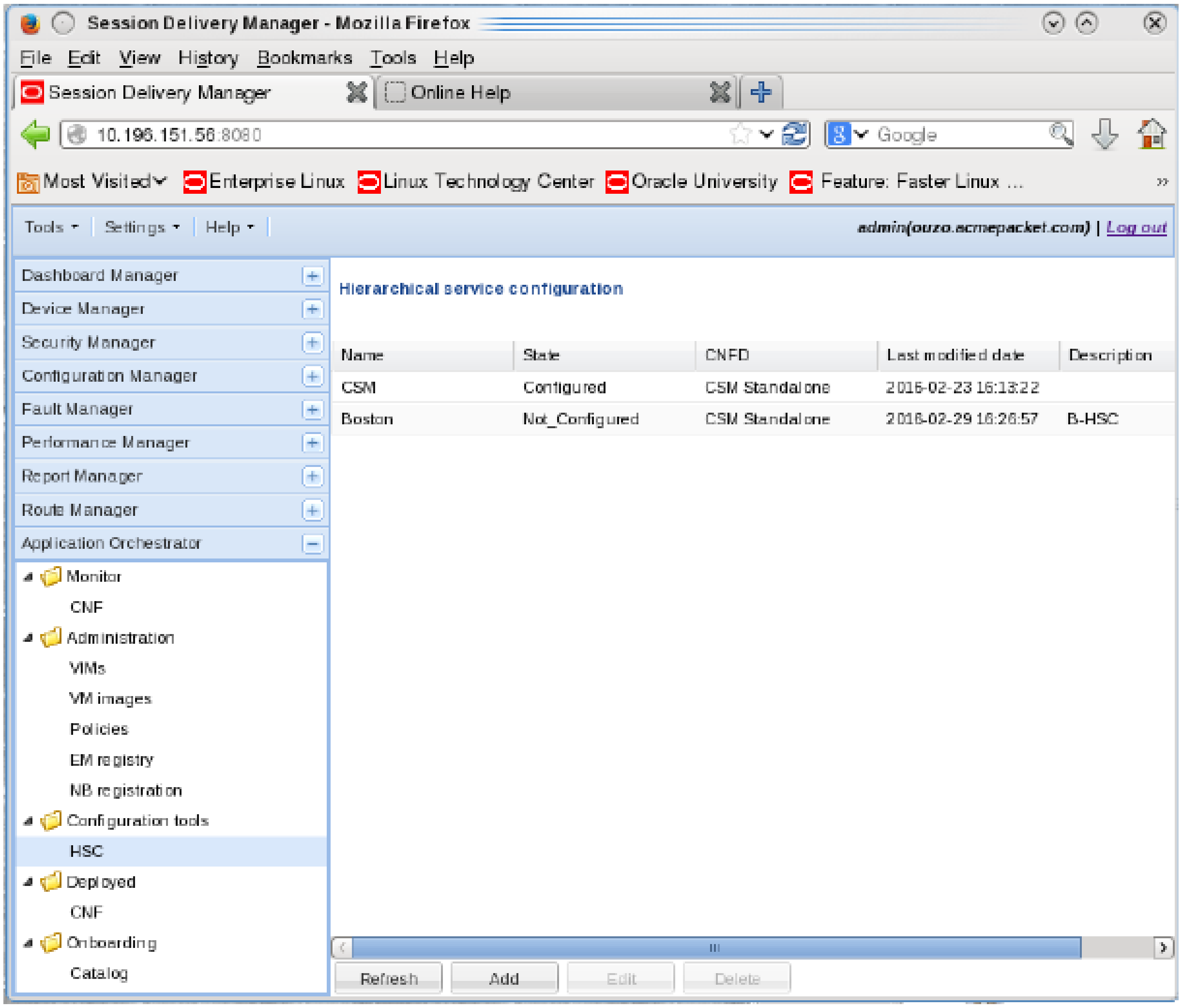
Deployment Status	HSC State	User Access	NF Group Resync	NF Group Change	HSC Description
Not Deployed	Not Configured	READ_WRITE	Allow	Allow	Allow
Not Deployed	Configured	READ_WRITE	Allow	Allow	Allow
Deployed	Not Configured	READ_WRITE	Allow	Not Allow	Allow
Deployed	Configured	READ_ONLY	Allow	Not Allow	Allow

Check the HSC Configuration Status

Once the HSC is configured in Oracle Communications Application Orchestrator and the Oracle Communications Application Orchestrator REST API is configured for a northbound service orchestrator to access, you can check the status of your HSC configuration.

1. Expand the **Application Orchestrator** slider and select **Configuration tools** > **HSC**. In the Hierarchical service configuration pane, following columns display.
2. In the **Hierarchical service configuration** pane, view the following columns to review the status of the HSC(s) that you configured:

Name	Description
Name column	The HSC name.
State column	The current state of the HSC, which is either **Not_Configured** or **Configured**.
CNFD column	The name of the **CNFD** that is used by this HSC.
Last modified date column	The date and time of last HSC modification.
Description column	The HSC description entered by user.
Created by column	(Hidden) The name of the logged in user who created this HSC.
Create date column	(Hidden) The date and time of HSC creation.
CNF Name column	(Hidden) The name of the CNF that was created from a deployed HSC.



Name	State	CNFD	Last modified date	Description
CSM	Configured	CSM Standalone	2016-02-23 16:13:22	
Boston	Not_Configured	CSM Standalone	2016-02-29 16:26:57	B-HSC

Figure 17: HSC pane

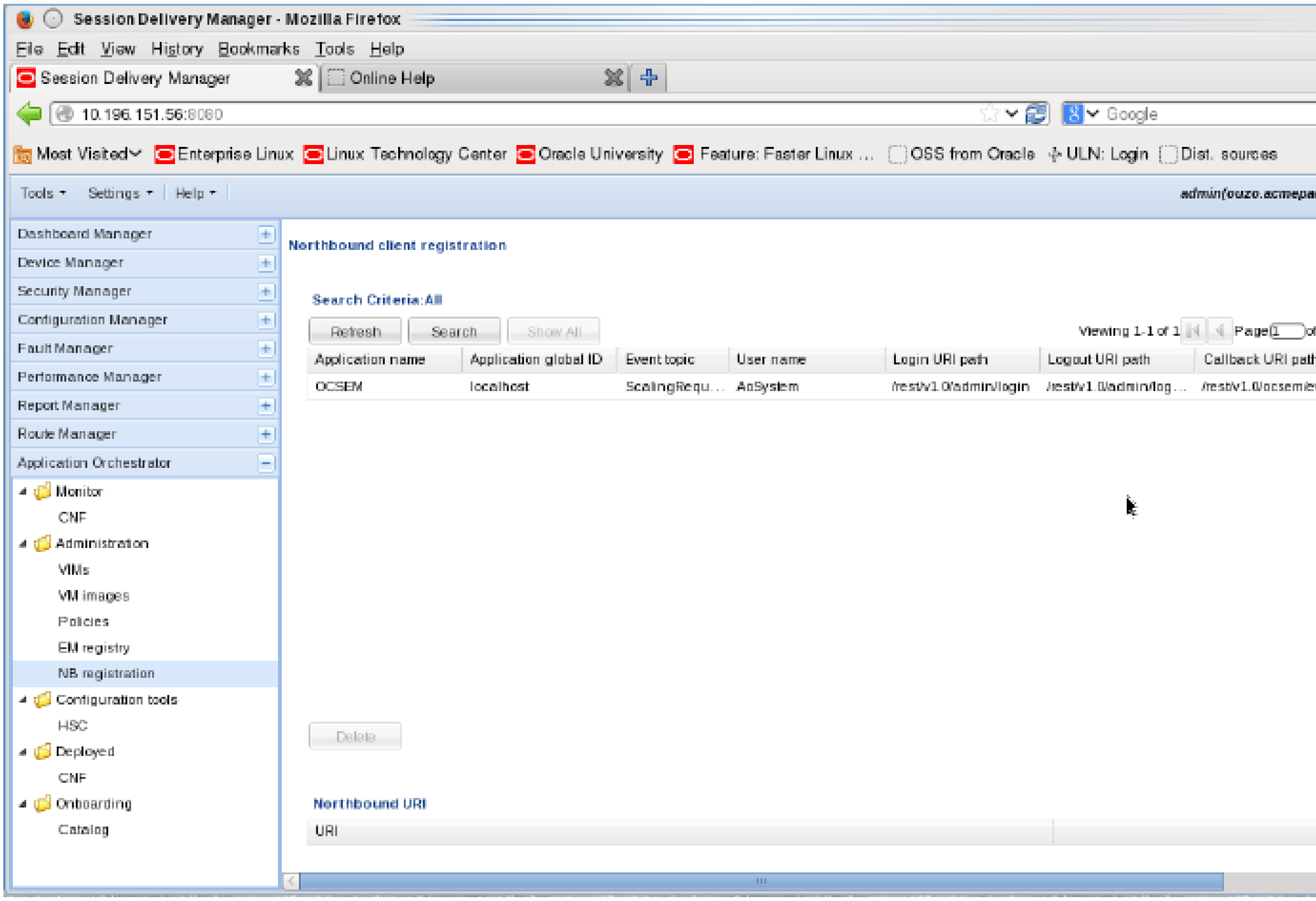
Check if the Northbound Client is Registered

Use this task to check if your northbound client, such as a northbound service orchestrator (NSO) or element manager (EM), that is registered with Oracle Communications Application Orchestrator.

1. Expand the **Application Orchestrator** slider and select **Administration** > **NB registration**.
2. In the **Northbound client registration** table, view the following columns to display the northbound client(s) registered with Oracle Communications Application Orchestrator.

Name	Description
Application name column	The northbound client application name that is registering the event topic. For example NSO, OCSEM, etc.
Application global ID column	Unique ID (or name) that the northbound client used to register. If the northbound client is a cluster, the unique ID can be the cluster ID or name. The Oracle Communications Application Orchestrator uses this ID to ensure that only one client in the cluster is notified when an event occurs.
Event topic column	The event topics that the northbound client utilizes. For example, ScalingRequest, Scaling, StateChange, etc.

Name	Description
User name column	The Oracle Communications Application Orchestrator user name, which is the **AoSystem** user.
Login URI path column	The login uniform resource identifier (URI) resource used to log into the Oracle Communications Application Orchestrator REST API. For example: `https:// OCAO_ipaddress:8443/rest/v1.0/admin/login`
Logout URI path column	The logout uniform resource identifier (URI) resource used to log into the Oracle Communications Application Orchestrator REST API. For example: `https:// OCAO_ipaddress:8443/rest/v1.0/admin/logout`
Callback URI path column	This is the URI that the northbound client is used to implement the REST API to allow the OCAO to send the event. The intention to use list here is to allow users to register all the northbound clients that are in the same cluster once. Uses can also use this API to register each northbound client individually
Object ID	(Hidden) The SNMP object identifier (OID) that uniquely identifies the northbound client in the MIB hierarchy.



Northbound client registration

Search Criteria:All

Application name	Application global ID	Event topic	User name	Login URI path	Logout URI path	Callback URI path
OCSEM	localhost	ScalingRequ...	AoSystem	/rest/v1.0/admin/login	/rest/v1.0/admin/log...	/rest/v1.0/ocsem/e

Northbound URI

URI

Figure 18: Northbound client registration pane

3. View the Northbound URI table to view a list of URI calls associated with the selected northbound client.

9

Manage DU Deployments

Once a CNF is activated and running after its deployment, you can undeploy or deploy DUs on an individual basis for administrative reasons before a CNF is deployed and made operational.

Note: When a CNF is deployed, the minimum number of DUs for each NF group are deployed.

Deploy a DU

Ensure that all required NF group and DU parameters are configured before deploying the DU.

Note:

When a CNF is deployed, DUs belonging to this CNF are automatically deployed. If you undeploy a DU, you can only (re)deploy DUs after the CNF to which they belong has been deployed for the first time.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select the CNF and click **Expand**.
3. In the **CNF details** pane, select the DU node you want to deploy.
4. Ensure that Manual mode is enabled (the Manual button is grey). If the **Manual** button is activated, click **Manual** to enter Manual mode so the DU can be deployed.
5. Click the **Manage** drop-down list and select **Deploy**.
   The DU is in a deployed state.

   Note: If the required configuration parameters for the deployed DU are not configured or configured incorrectly, an error message displays and the DU cannot become operational when the CNF is activated.
6. Deploy the CNF and make the CNF operational. See *Deploy and Make the CNF Operational* chapter for more information.

Undeploy a DU

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the **Deployed CNF** table, select the CNF and click **Expand**.
3. In the **CNF details** pane, select the DU node you want to deploy.
4. Ensure that Manual mode is enabled (the Manual button is grey). If the **Manual** button is activated, click **Manual** to enter Manual mode so the DU can be undeployed.

5. Click the **Manage** drop-down list and choose **Undeploy**.
   The DU is in an undeployed state.

10

Monitor Application Orchestrator System Information

Real-time KPI thresholds, device status and performance information can be monitored in Oracle Communications Application Orchestrator for CNFs.

Monitor Active CNFs

1. Expand the **Application Orchestrator** slider and select **Monitor** > **CNF** to display state, capacity and performance information for an NF group, its DUs and physical or virtual devices associated with each DU.
2. In the **Monitor CNF groups** table, you can use the following tree table buttons display information about the active CNFs.

   In this global table, the following columns display for the running CNFs and their current states.

Name	Description
Name column	The CNF name.
Deployment state column	The deployment state for each CNF. See the *View CNF Deployment States* in the *Staging and Promoting a CNF* chapter for more information.
Health state column	The overall reported health of the CNF. The following health states are shown below: • Two dashes (- -) indicate that health data continues to be collected for one or more DUs. • **Healthy**—All DUs are in a healthy state and are reachable on the network. • **Impaired**—One or more DUs are unreachable on the network or have otherwise encountered an error which impacts the total DU capacity, or resiliency.
Capacity state column	The overall reported capacity. The following capacity states are shown below: • **Reducible**—The capacity of the NF group can be satisfied by fewer DUs than are currently deployed (all NF group KPIs are in a reducible state). • **Good**—The capacity of the NF group is satisfied by the number of DUs that are currently deployed (one or more NF group KPIs are in the **Good** state, and no KPIs are in **Warning** or **Critical** states).

Name	Description
	• **Warning**—The capacity of the NF group is satisfied by the number of DUs that are currently deployed, but one or more KPIs have exceeded a warning capacity limit. Additional DUs may be required in the near future in order to bring total NF group capacity back into a **Good** state range. • **Critical**—The capacity of the NF group may no longer be satisfied by the number of DUs that are currently deployed. One or more KPIs have crossed a critical threshold boundary indicating that additional DUs are required immediately.
CPU capacity column	The current use and total resource allocation of the CPU for the CNF. The CPU capacity is the current number of CPU cores in use.
Memory capacity column	The current resource allocation and total memory resource allocation of the CNF. For example, 40 GB of disk might be allocated to a VM, but the VM may only be using 1 GB of that 40 GB.
Disk capacity column	The current resource allocation and total disk resource allocation for the CNF.

Monitor NF Groups

1. Expand the **Application Orchestrator** slider and select **Monitor** > **CNF** to display state, capacity and performance information for an NF group, its DUs and physical or virtual devices associated with each DU.
2. To view an NF group for a CNF, select the CNF from the **Monitor CNFs** pane and click **Monitor**.
3. In the **Monitor NF groups for CNF** pane, following information appears in the table:

Name	Description
Name column	The NF group name.
Deployment state column	The deployment state for each NF group. See the *View CNF Deployment States* in the *Staging and Promoting a CNF* chapter for more information.
Health state column	The overall reported health of the NF group. The following health states are shown below: • Two dashes (- -) indicate that health data continues to be collected for one or more DUs. • **Healthy**—All DUs are in a healthy state and are reachable on the network. • **Impaired**—One or more DUs are unreachable on the network or have otherwise encountered an error which impacts the total DU capacity or resiliency.
Capacity state column	The overall reported capacity. The following capacity states are shown below: • **Reducible**—The capacity of the NF group can be satisfied by fewer DUs than are currently deployed (all NF group KPIs are in a reducible state). • **Good**—The capacity of the NF group is satisfied by the number of DUs that are currently deployed (one or more NF group KPIs are in the **Good** state, and no KPIs are in **Warning** or **Critical** states). • **Warning**—The capacity of the NF group is satisfied by the number of DUs that are currently deployed, but one or more KPIs have exceeded a warning capacity limit. Additional DUs may be required in the near future in order to bring total NF group capacity back into a Good range.

Name	Description
	• **Critical**—The capacity of the NF group may no longer be satisfied by the number of DUs that are currently deployed. One or more KPIs have crossed a critical threshold boundary indicating that additional DUs are required immediately.
CPU capacity column	The current use and total resource allocation of each NF group.
Memory capacity column	The current use and total resource allocation of the memory for each NF group.
Disk capacity column	The current use and total resource allocation of the storage for each NF group.

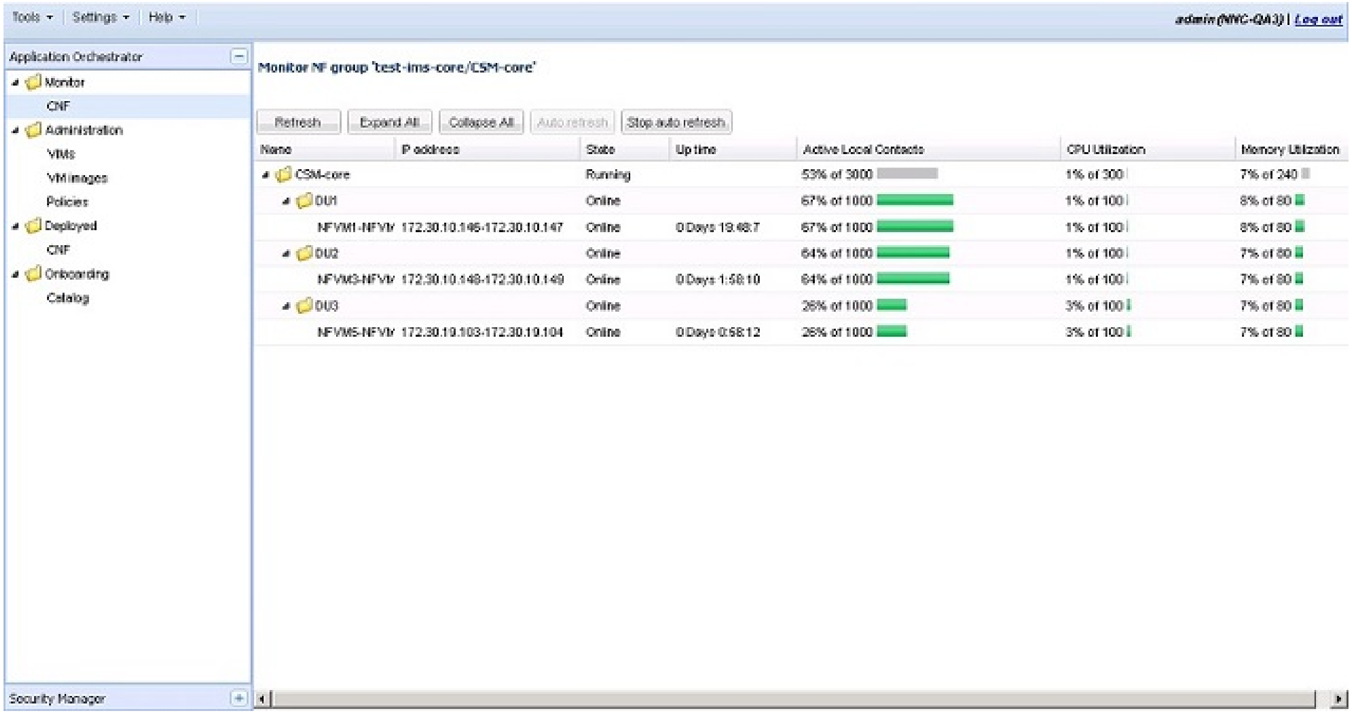
Monitor VDUs and PDUs

1. Expand the **Application Orchestrator** slider and select **Monitor** > **CNF** to display state, capacity and performance information for DUs and physical or virtual devices associated with each DU.
2. Select the CNF from the **Monitor CNFs** pane and click **Monitor**.
3. To view VDU and PDU information for the NF group of a CNF, select the DU or DU node and click **Monitor**.

Name	Description
Name column	The PDU, VDU or NFVM device name.
Deployment state column	The deployment state for each VDU or PDU. See the *View DU and DU node Deployment States* in the *Staging and Promoting a CNF* chapter for more information.
Health state column	The overall reported health of the VDU or PDU. The following health states for a DU and DU node are shown below: • Two dashes (- -) indicate that health data continues to be collected for the DU or DU node. • **Online (DU)**—All DU nodes are in an online state (accepting new traffic). • **Online (DU node)**—All NF devices belonging to the DU node are in an online state (accepting new traffic). • **Offline (DU)**—One or more DU nodes are offline (not accepting new traffic). Although some DU nodes may be online, the entire DU is considered to be in an offline state. • **Offline (DU node)**—One or more NF devices belonging to a DU node are offline (not accepting new traffic). Although some NF devices may be online, the entire DU node is considered to be in an offline state. • **Impaired (DU)**—One or more DU nodes are unreachable on the network or have otherwise encountered an error which impacts the total DU node capacity or resiliency. • **Impaired (DU node)**—One or NF devices are unreachable on the network or have otherwise encountered an error which impacts the total capacity. • **Unreachable (DU)**—All DU nodes are unreachable on the network. • **Unreachable (DU node)**—All NF devices belonging to the DU node have become unreachable on the network.
CPU capacity column	The current use and total resource allocation of the CPU for the NF group, PDU, VDU or VM device. A threshold must be configured for this KPI so that data populates this column.

Name	Description
Memory capacity column	The current use and total resource allocation of the memory for the NF group, PDU, VDU or VM device. A threshold must be configured for this KPI so that data populates this column.
Disk capacity column	The current use and total resource allocation of the memory for the NF group, PDU, VDU or VM device. A threshold must be configured for this KPI so that data populates this column.

The following figure shows an example of an active CNF that is composed of core IP multi-media Subsystem (IMS) Oracle Communications Session Routers and SLRMs.



Monitor NF group 'test-ims-core/CSM-core'

Name	IP address	State	Up time	Active Local Contacts	CPU Utilization	Memory Utilization
CSM-core		Running		53% of 3000	1% of 300	7% of 240
DU1		Online		67% of 1000	1% of 100	8% of 80
NFVM1-NFVM	172.30.10.146-172.30.10.147	Online	0 Days 19:48:7	67% of 1000	1% of 100	8% of 80
DU2		Online		64% of 1000	1% of 100	7% of 80
NFVM3-NFVM	172.30.10.148-172.30.10.149	Online	0 Days 1:58:10	64% of 1000	1% of 100	7% of 80
DU3		Online		26% of 1000	3% of 100	7% of 80
NFVM5-NFVM	172.30.19.103-172.30.19.104	Online	0 Days 0:58:12	26% of 1000	3% of 100	7% of 80

Figure 19: DU information for the NF group of an active CNF

Note: The auto-refresh interval is set to 15 seconds by default. Devices are polled for performance information every 5 minutes.

11

Fault Manager

Fault manager is used to view events, alarms and trap event settings. Events and alarm information is based on the Oracle® standard and proprietary Management Information Bases (MIBs). All SNMP traps generated from nodes are managed by Oracle Communications Application Orchestrator. Both alarms and event trap notifications are generated when a bad (fault) event or alarm occurs on a node.

To receive notifications, ensure that SNMP communities and the MIB contact and trap receiver information is configured on your OSS/BSS system in order to receive fault notifications.

If you want more specific information about events, alarms, and MIBs that is not covered in this chapter, see the *Oracle Communications Core Session Manager MIB Reference Guide*.

Alarm and Event Configuration Tasks

The following sections describe the **Alarms** table and **Events** table, with their accompanying features. The **Events** table shows a one to one correspondence with all device traps and generated server events. The **Events** table maintains the precise history of all events created and recorded. The **Alarms** table summarizes the **Events** table by showing the most recent update for the specific categories, failed resources, and devices in each row. There may be several events generated in the **Alarms** table that correlate to events for a failed resource type for a device into one entry where the last known state and time is shown.

Manage How Alarms are Displayed

1. Expand the **Fault Manager** slider and select **Events**.
2. Glide your mouse over a column and click the drop-down list that appears next to any column heading.
3. Click the down arrow to display the menu.
4. Click **Sort Ascending** to sort the data in ascending order, or click **Sort Descending** to sort the data in descending order.
5. Click **Columns** sub-drop-down list to access a list of column names to edit.
6. Check a marked checkbox next to a column to hide it, or click an empty checkbox next to a column to display it.
7. In the alarms pane, select an alarm that you want to view and click **View**.

   Note: Alternatively, you can double-click the alarm.

8. In the **Alarm detail** dialog box, view the following fields:

Name	Description
Annotation	The user-defined note pertaining to this alarm.
Acknowledged by	The user that acknowledged the alarm.
Time	The date and time this alarm was generated in hours, minutes, and seconds.
Modified time	The date and time the alarm was last modified.
Description	A short description of the alarm.
Source	The exact descriptive source of the alarm.
Source IP	The IP address from which this alarm was generated.
Failed resource	The resource responsible for this alarm.
Type	The type of trap associated with this alarm. For example, TrapRelayMonitor.
System up time	Length of time the system has been operational in hours, minutes, and seconds.
Severity	One of the following user-defined severity levels can display for a system alarm: **Note:** The number indicates the numerical severity level. • (0) EMERGENCY—The system is unusable. • (1) CRITICAL—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. The default color code is red. • (2) MAJOR—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but ceases to function. The default color code is salmon. • (3) MINOR—Error conditions exist. The functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. The default color code is orange. • (4) WARNING—Warning conditions exist. Some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly. The default color code is light yellow. • (5) NOTICE—Normal, but a significant condition exists. The default color is lime green. • (6) INFO—Informational messages are appearing. The default color code is yellow-green. • (7) TRACE—Trace messages appear. The default color is lime green. • (8) DEBUG—Debugging messages appear. The default color is lime green. • (9) DETAIL—Detailed messages appear. The default color is lime green.
Trap Name	The exact name of the trap associated with this alarm. For example, apNNCTrapRelayAliveNotification.
Trap Category	The category to which the alarm belongs. For example, NNC.
Source Group ID	(Hidden) The identity of the source group associated with this alarm.
Object ID	(Hidden) The object identifier (OID) associated with this alarm.

Manage How Events are Displayed

1. Expand the **Fault Manager** slider and select **Events**.
2. Glide your mouse over a column and click the drop-down list that appears next to any column heading.
3. Click the down arrow to display the menu.
4. Click **Sort Ascending** to sort the data in ascending order, or click **Sort Descending** to sort the data in descending order.
5. Click **Columns** sub-drop-down list to access a list of column names to edit.
6. Check a marked checkbox next to a column to hide it, or click an empty checkbox next to a column to display it.
7. In the events pane, select an event that you want to view and click **View**.

   Note: Alternatively, you can double-click the event.

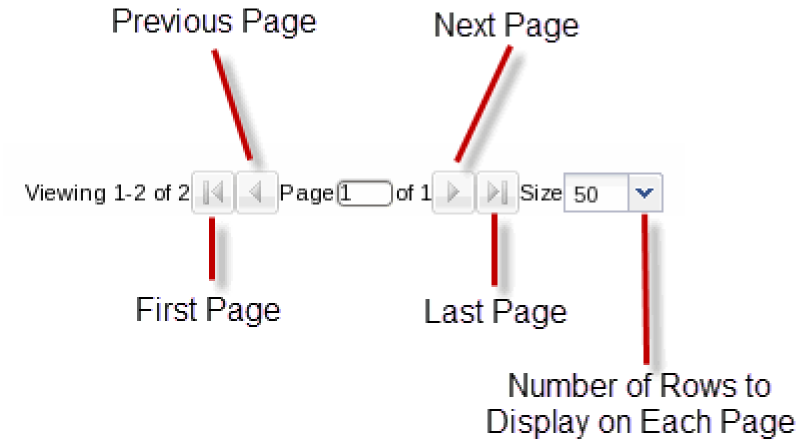
8. In the **Event detail** dialog box, view the following fields:

Name	Description
Time	The date and time this event was generated in hours, minutes, and seconds.
Description	A short description of the event.
Severity	One of the following user-defined severity levels can display for a system event: **Note:** The number indicates the numerical severity level. • (0) EMERGENCY—The system is unusable. • (1) CRITICAL—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. The default color code is red. • (2) MAJOR—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but ceases to function. The default color code is salmon. • (3) MINOR—Error conditions exist. The functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. The default color code is orange. • (4) WARNING—Warning conditions exist. Some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly. The default color code is light yellow. • (5) NOTICE—Normal, but a significant condition exists. The default color is lime green. • (6) INFO—Informational messages are appearing. The default color code is yellow-green. • (7) TRACE—Trace messages appear. The default color is lime green. • (8) DEBUG—Debugging messages appear. The default color is lime green. • (9) DETAIL—Detailed messages appear. The default color is lime green.
Default Severity	The system-defined severity level for this event.
Source	The exact descriptive source of the event.
Source IP	The IP address from which this event was generated.
Failed resource	The resource responsible for this event.

Name	Description
Type	The type of trap associated with this event. For example, TrapRelayMonitor.
Trap Name	The exact name of the trap associated with this event. For example, apNNCTrapRelayAliveNotification.
Trap Category	The category to which the event belongs. For example, NNC.
System up time	Length of time the system has been operational in hours, minutes, and seconds.
Source Group ID	(Hidden) The identity of the source group associated with this event.
Object ID	(Hidden) The object identifier (OID) associated with this event.

Navigate Multiple Fault Manager Pages

1. Expand the **Fault Manager** slider and choose from the following options:
   - **Events**
   - **Alarms**
2. At the top right area of the **Events** or **Alarms** pane, click the navigation icons to display the desired first page, previous page, next page, and the last page, etc.



Manage the Page View for Events and Alarms

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the alarms or events pane, you can select from the following actions:

Name	Description
Refresh button	Click to refresh the data in the table.
Show all button	Click to show all current alarms or events.

Search for Alarms or Events by Specifying a Criteria

You can search for events and alarms by specifying one, some, or all of the search selection criteria. For example, you can select alarms for a specific IP address during a specified date-time range.

1. Expand the **Fault Manager** slider and select from the following options:

- **Events**
- **Alarms**

2. In the alarms or events pane, click **Search**.
3. In the **Filter search** dialog box, complete the following fields:

Name	Description
Date from field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The chosen date to filter event data begins at 12:00 AM (midnight) on the specified date.
Date to field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The date you select ends at 11:59:59 PM.
Source device field	The source name for this device.
Source IP field	The IP address for this source device.
Trap name drop-down list	Select the trap name.
Type drop-down list	Select the alarm type.
Severity drop-down list	Select the severity level for this alarm.

Change the Number of Alarms or Events in a Table

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. At the top of the events or alarms pane, click the **Size** drop-down list.

   Note: By default, 50 table items are displayed.
3. Click the appropriate value.

Save Alarms or Event Data to a File

You can save event or alarm data in the content area to a comma-separated values (CSV) file that stores table data (numbers and text) in plain-text form.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the events or alarms pane, click **Save to file**.
3. In the save dialog box, select either to open the file or save the file.

   Note: If you save the file, the file is saved to your browser's default download location.
4. Click **OK**.

Delete Alarms or Events

The appropriate administrator privileges must be assigned to delete alarms or events.

Note: Deleting an alarm in Oracle Communications Application Orchestrator has no affect on the node because the node is unaware that Oracle Communications Application Orchestrator displayed the alarm or deleted it from the alarms table.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the alarms or events table, click the alarm or event that you want to remove and click **Delete**.
3. In the **Delete** dialog box, click **Yes** to confirm the deletion of the alarm or event.

Specify a Criteria to Delete Alarms and Events

The appropriate administrator privileges must be assigned to delete alarms or events.

Use this task to specify one or more criterion for deleting alarms or events from Oracle Communications Application Orchestrator.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the events or alarms pane, click **Delete by criteria**.
3. In the **Delete event** dialog box, complete the following fields:

Name	Description
Please specify the delete choice field	Click to select either **Delete all** or **Delete by criteria**.
Date from field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The chosen date to filter event data begins at 12:00 AM (midnight) on the specified date.
Date to field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The date you select ends at 11:59:59 PM.
Source device field	The source name for this device.
Source IP field	The IP address for this source device.
Trap name drop-down list	Select the trap name.
Type drop-down list	Select the alarm type.
Severity drop-down list	Select the severity level for this alarm or event.

4. Click **OK**.

Configure When Event and Alarm Data is Cleared

1. On the main menu, click **Settings** > **Faults** > **Fault configuration**.
2. In the **Fault configuration** dialog box, complete the following fields:

Name	Description
***Clear events older than (days)** field	The number of days events are retained in the database before the events are cleared. The default value is seven days. Zero indicates no event data is cleared
***Clear alarms older than (days)** field	The number of days alarms are retained in the database before the alarms are cleared. The default value is 14 days. Zero indicates no alarm data is cleared.

Name	Description
***Duplicate trap filter interval (minutes)** field	The number of minutes for when duplicate traps are cleared for events and alarms.

3. Click **OK**.
4. In the success dialog box, click **OK**.

Alarm Specific Configuration Tasks

Alarms play a significant role in determining the overall health of the system. An alarm is triggered when a condition or event happens within the hardware or software of a system (node). Alarms contain an alarm code, a severity level, a textual description of the event, and the time the event occurred. The following sections describe how to configure the way alarms display in Oracle Communications Application Orchestrator.

Configure the Auto Refresh Period for Alarm Data

1. Expand the **Fault Manager** slider and select **Alarms**.
2. Click **Auto refresh**.
3. In the **Auto refresh** dialog box, enter the number of seconds to refresh alarm data in the **Refresh Interval(secs)** field.
4. Click **OK**.

   Note: If you want to stop the auto-refresh function, click **Stop Auto Refresh**.

Add a Comment to an Alarm

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, click the alarm to which you want to add a comment and click **View**.
3. In the **Alarm detail** dialog box, click **Edit**.
4. Add your comments about this alarm in the **Description** field.
5. Click **OK**.

Enable Alarm Acknowledgement

The appropriate administrator privileges must be assigned to acknowledge alarms.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to acknowledge and click **Acknowledge**.
3. In the **Acknowledge** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.
5. Click the alarm to view an updated **Alarm detail** dialog box with the **Acknowledged by** and **Last modified** fields updated.
6. Click **OK**.

Disable Alarm Acknowledgement

The appropriate administrator privileges must be assigned to unacknowledge alarms.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to unacknowledge and click **Unacknowledge**. The Acknowledge dialog box appears.
3. In the **Unacknowledge** dialog box, click **Yes**.

4. In the **Info** dialog box, click **OK**.

Clear an Alarm

The appropriate administrator privileges must be assigned to clear alarms.

Note: Clearing an alarm in Oracle Communications Application Orchestrator has no affect on the node because the node is unaware that Oracle Communications Application Orchestrator displayed the alarm or changed its severity to clear.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to clear and click **Clear**.
3. In the **Clear** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.

Override Default Severity Levels for Alarm Trap Conditions

1. Expand the **Fault Manager** slider and select **Trap event setting**.
2. In the **SNMP Trap OID** dialog box, click the alarm trap you want to change from the **Trap Descriptor** scroll-down list.
   The information for the alarm trap appears in the **Severity Mapping** table below.
3. In the **Severity Mapping** table, click the **Current severity** column cell of the trap condition row that you want to modify.
4. In the drop-down list of severity levels, click the severity you want to apply. The new level appears in the Current Severity column.

   Note: The **Default severity** column serves as a reference point and continues to show the default severity setting for the trap condition.
5. Click **Apply**.
6. In the Information dialog box, click **OK**.

Audible Alarms

The audible alarms system allows you to set off an audible sound when an activated alarm is triggered.

Alarm events are updated during each refresh cycle of the alarms table. Search functionality is disabled when audible alarms are active. The audible alarms cease to function upon exiting the Fault Manager navigation bar slider.

Audio Files

The Audible Alarms application comes with five alarm sounds (one for each severity). You may replace these files with your own as long as the new.wav files retain the same filenames. The files are located in the following directory:

```
<installed directory>\ACMEConsole\audibleAlarms
```

The filenames appear as:

- Audio_Emergency.wav
- Audio_Critical.wav
- Audio_Major.wav
- Audio_Minor.wav
- Audio_Warning.wav

Enable and Configure Audible Alarms

1. On the main menu, click **Settings** > **Alarms** > **Audible Alarms**
2. In the **Audible Alarms** dialog box, click the check box next to the severity categories that you want to enable an audible alarm. The categories are **Emergency**, **Critical**, **Major**, **Minor**, and **Warning**.
3. Click **OK**.

4. On the Oracle Communications Application Orchestrator navigation bar, select **Fault Manager** > **Alarms**
5. Click **Start Audible Alarm**.
   The button toggles to **Stop Audible Alarm**.

6. If you want to shut down the audible alarms application, click **Stop Audible Alarm**.
   The button toggles to **Start Audible Alarm**.

Change the Default Severity Alarm Colors

1. On the main menu, click **Settings** > **Alarms** > **Alarm Colors**
2. In the **Alarm colors** dialog box, click the **Color** drop-down list next to the severity category and its default color.
3. In the pop-up color palette, click the new color that you want for the alarm.
4. Repeat the previous two steps if you want to configure more severity alarm colors.
5. Click **OK**.
6. In the success **Information** dialog box, click **OK**.

Application Orchestrator Event Types

Expand the **Fault Manager** slider and select **Trap event setting** to view or change the severity setting of the following Oracle Communications Application Orchestrator-specific event types that are associated with syslog messages.

Note: The **ap-ocao.mib** file is dedicated for Oracle Communications Application Orchestrator event notification.

Type	Associated Traps	Description
CapacityPlanner_DUAvailbility	apOCAONFcDUAvailabilityFailure	Notifies when a scale-out operation fails because there is not an available DU for the network function (NF) component group (For example, a CNF).
	apOCAONFcDUAvailabilityFailure Clear	Clears a notification for the latest scale-out attempt after previous failures (for example, the notification clears when a DU is available).
DUDeploymentStatus	apOCAONFcDeploymentFailure	Notifies when the deployment of an NF component fails.
	apOCAONFcDeploymentFailureCle ar	Clears a notification of a prior NF component deployment failure.
NBI	apOCSDMServerHeartbeatReachabl e	Notifies the availability of the Oracle Communications Application Orchestrator server or server cluster from the northbound interface through periodic monitoring.

Fault Email Notifications

Oracle Communications Application Orchestrator can trigger automatic email notifications when reporting alarms for certain severities. You can configure the appropriate email addresses that match each alarm severity.

Configure Email Notifications for Fault Occurrences

With appropriate administrator privileges assigned, you can assign fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.
2. In the **Fault email recipients** dialog box, click **Add**.
3. In the **Add email** dialog box, complete the following fields:

Name	Description
***Email address** field	The recipient email address attached to the alarm severity.
Severity drop-down list	Select the severity level for this email notification. The levels are **Emergency**, **Critical**, **Major**, **Minor**, **Notice**, **Warning**, **Info**, **Trace**, **Debug**, and **Unknown**.
Notify on clear check box	Check the check box to send a fault notification on all clear events. This option is only available for the following severity levels: **Emergency**, **Critical**, **Major**, and **Minor**.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. In the **Fault email recipients** dialog box, the configured email address appears in the table. Click **OK**.

Delete Fault Email Notifications

With appropriate administrator privileges assigned, you can delete fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.
2. In the **Fault email recipients** dialog box, select the email address you want to remove and click **Delete**.
3. In the **Delete** dialog box, click **Yes**.
4. In the success dialog box, click **OK**.
5. In the **Fault email recipients** dialog box, the email address no longer appears in the table. Click **OK**

Edit Fault Email Notifications

With appropriate administrator privileges assigned, you can edit fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.
2. In the **Fault email recipients** dialog box, select the email address you want to edit and click **Edit**.
3. In the **Edit email** dialog box, edit the following fields:

Name	Description
***Email address** field	The recipient email address attached to the alarm severity.
Severity drop-down list	Select the severity level for this email notification. The levels are **Emergency**, **Critical**, **Major**, **Minor**, **Notice**, **Warning**, **Info**, **Trace**, **Debug**, and **Unknown**.
Notify on clear check box	Check the check box to send a fault notification on all clear events. This option is only available for the following severity levels: **Emergency**, **Critical**, **Major**, and **Minor**.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. In the **Fault email recipients** dialog box, the edited email address appears in the table. Click **OK**

Configure Application Orchestrator External Trap Receivers

Note: Before you configure Oracle Communications Application Orchestrator external trap receivers, you must configure an external server to be the receiver of these traps.

Add External Trap Receivers

An external trap receiver is a device that you use as the SNMP trap destination, instead of the device where Oracle Communications Application Orchestrator is installed. When you configure the external trap receiver, you enter its address and port. The combination of IP address and port must be unique for each configured trap receiver.

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, click **Add**.
3. In the **Add trap receiver** dialog box, complete the following fields:

Name	Description
***IP address** field	The IP address of the server receiving traps.
***UDP port** field	The port number for the server receiving the traps or retain the default value of **162**.
***Community string** field	The name of the SNMP community to which the server receiving traps belongs or retain the default value **public**.
SNMP version drop-down list	The version of SNMP. SNMP Version 2 (**V2**) is chosen by default.
Forward enabled check box	Check the check box if you want to allow the trap to be forwarded to a client.
Severity level drop-down list	Select from the following trap severity levels: • **Indeterminate**—The trap severity cannot be determined because of the nature of the information contained in the trap. • **Critical**—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. • **Major**—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but it ceases to function. • **Minor**—Error conditions exist. Functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. • **Warning**—Warning conditions exist. There are some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly.
Format field	Select from the following trap formats: • **OC SDM** radio button—*Oracle Communications Session Delivery Manager* format. • **OC SDM traps** check box is pre-selected for *Oracle Communications Session Delivery Manager* traps. • **ITU X.733** radio button—International Telecommunication Union Alarm Model format defined in recommendation X.733.

Name	Description
	• **OC SDM traps** check box is pre-selected for *Oracle Communications Session Delivery Manager* by default. You can un-check this check box. • **SBC traps** check box—Oracle Communications Session Border Controller traps. **Note:** If this check box is checked, you can specify that traps for the device can be forwarded to the destination. If the **Select devices** radio button is chosen, you can select a device from the **Managed devices** box and click the **Add** arrow button to add the trap device to the **Selected trap source devices** box. You can remove a trap device by selecting it and clicking the **Remove** arrow button.

4. Click **OK**.
   The new trap is added to the table in the **Trap receivers configuration** dialog box.

Synchronize an External Trap Receiver to Validate the Health of a Device

Use this task to configure alarms or events on the Oracle Communications Application Orchestrator to be resent (forwarded) out of the northbound interface to the connected destination trap receiver (device) in order to synchronize the alarms or events so that the health of the connected device can be determined.

Note:

You must add an external trap receiver device before doing this task.

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, select the trap receiver that you want to edit and click **Sync**.
3. In the **Trap receiver alarm synchronization** dialog box, complete the following fields:

Name	Description
Synchronization from radio button	Click the **Event** radio button or **Alarm** radio button to resend events or alarms to the connected destination trap receiver.
Minimum severity level drop-down list	Select from the following security levels to send all existing events or alarms with this severity level or higher to its destination trap receiver: • **Indeterminate**—Clear all events and synchronize from when they were cleared. • **Critical**—Send critical events or alarms. • **Major**—Send major and critical events or alarms. • **Minor**—Send minor, major, and critical events or alarms. • **Warning**—Send warning, minor, major, and critical events or alarms. • **Clear**—Clear all alarms and synchronize from when they were cleared.
Date and time from: fields	Click the calendar icon to select the synchronization start date and time.
Date and time to: fields	Click the calendar icon to select the synchronization end date and time.

4. Click **OK**.

Add the Heartbeat Trap to Monitor Server Availability

The heartbeat trap (apOCSDMServerHeartbeatReachable) can be manually started and stopped to periodically monitor the availability of the Oracle Communications Application Orchestrator from the northbound interface. This heartbeat trap is sent (forwarded) out of the northbound interface as an event (INFO) to the connected destination trap receiver of a management device. A problem can be detected by the management device if no heartbeat trap is received by its trap receiver during the specified interval due to either the failure of a single server or server cluster, or if SNMP administrative changes affected the connectivity between the server and management device.

Note:

You must add an external trap receiver device to Oracle Communications Application Orchestrator before doing this task.

The heartbeat trap is disabled by default. Use the following steps to specify the heartbeat trap send interval, and initiate the sending or termination of a heartbeat trap.

1. On the main menu, click **Settings** > **Faults** > **Heartbeat Traps**.
2. In the **Configure heartbeat SNMP trap interval** dialog box, complete the following fields:

Name	Description
Interval (minutes) drop-down list	Select the number of minutes to send the heartbeat trap. The range increments in 5 (default), 10, 15, 30 and 60 minutes.
Start field	(Read-only) The time the last heartbeat trap was started.
Stop field	(Read-only) The time the last heartbeat trap was stopped.
Trap time stamp field	(Read-only) The time stamp for when the last heartbeat trap was sent.

3. Click **Apply** to update the interval change.
4. Click **Start** to send the heartbeat trap. The heartbeat trap is sent at the interval that you specify.
5. Click **Stop** to terminate the heartbeat trap.
6. Click **Refresh** to see the most current trap time stamp information for exactly when the last heartbeat trap was sent.

Edit External Trap Receivers

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, select the trap that you want to edit and click **Edit**.
3. In the **Edit trap receiver** dialog box, edit the fields described in the *Add External Trap Receivers* section and click **OK**.

Delete External Trap Receivers

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, choose the trap that you want to delete and click **Delete**.
3. In the confirmation dialog box, click **Yes**.
4. In the success dialog box click **OK**.
   The trap is removed from the table in the **Trap receivers configuration** dialog box.

A

Guidelines for Provisioning Your VIM

The guidelines in this appendix can help you to provision your VIM so that it can be added and configured in Oracle Communications Application Orchestrator.

Guidelines for Provisioning Oracle OpenStack

Use the following guidelines to provision Oracle Openstack VIMs.

- Use the following links to find OpenStack user documentation:
  - *Oracle OpenStack for Oracle Linux Release 1*
  - *Oracle OpenStack for Oracle Linux Release 2*
- Oracle Communications Application Orchestrator uses the following services:
  - **Keystone**—An identity management system responsible for user and service authentication. Keystone is capable of integrating with third-party directory services and the Lightweight Directory Access Protocol (LDAP).
  - **Nova**—A computing service responsible for creating instances and managing the life cycle of these instances, and managing the chosen hypervisor to which it is connected.
  - **Neutron**—A network service responsible for creating network connectivity and network services. It is capable of connecting with vendor network hardware through plug-ins. Neutron comes with a set of default services implemented by common tools. Network vendors can create plug-ins to replace any one of the services with their own implementation, adding value to their users.
  - **Glance**—An image service responsible for managing images uploaded by users. Glance is not a storage service, but it is responsible for saving image attributes, and making a virtual catalog of the images.
- Use Neutron for networking. Networks should be *flat provider* networks, backed by Openvswitch or LinuxBridge networking agents. Use **`firewall_driver = neutron.agent.firewall.NoopFirewallDriver`**, and disable **`iptables`** on compute nodes when testing initial connectivity. **`iptables`** can be used later after configuring security groups.
- Oracle Communications Application Orchestrator uses **Domain**, **Project**, and **User** fields for authentication. Enable multi-domain support, or use **default** for Domain.
- Oracle Communications Application Orchestrator does not support floating IPs currently. A floating IP address is a service provided by Neutron that does not use any DHCP service or is not configured statically within the guest VM.
- When a new virtual machine (VM) is deployed, Oracle Communications Application Orchestrator looks for an existing *flavor* virtual hardware template in OpenStack that matches the required CPU, memory, and disk allocations. If one does not exist, Oracle Communications Application Orchestrator attempts to create a flavor

template. This requires the OpenStack user to have the Nova permission: **`compute_extension:flavormanage`**. Have an administrator add the required *flavor* hardware template, or add this permission to the Nova **`json.policy`** file for the OpenStack user.

OpenStack Configuration Drive Requirements and Guidelines

To use Configuration Drive with libvirt, XenServer, or VMware, you must first install the genisoimage package on each compute host, or instances do not boot properly. Use the mkisofs_cmd flag to set the path where you install the genisoimage program. If genisoimage is in same path as the nova-compute service, you do not need to set this flag.

Guidelines for Provisioning vCloud Director 5.5

Use the following guidelines and the *vCloud Director User's Guide* to provision the vCloud Director 5.5 VIM.

- The vCloud user must have the **Catalog Author** permissions or higher.
- Organization Virtual Data Centers (Org vDCs) registered with Oracle Communications Application Orchestrator must have **Fast Provisioning** disabled.
- Org vDCs registered with Oracle Communications Application Orchestrator should use the *allocation pool* resource allocation model, with 100 percent of allocated resources with a certain percentage guaranteed. Other allocation models can result in poor performance because of the over-provisioning of resources.
- Use the following anti-affinity rules for HA pairs:
    - Direct access to the vCenter server that provides resources for the underlying vCloud provider vDC is required.
    - The vCenter user must have permissions to create an anti-affinity DRS rule on the Cluster where the VMs are deployed.
    - The Cluster must be backed by *shared* storage, or the DRS rule can fail to move live, running virtual machines from one host to another while maintaining continuous service availability (vMotion).
    - When configuring the Oracle Communications Application Orchestrator VIM Datacenter, make sure to select a vCloud storage profile that contains only shared storage volumes.

      Note: This vCloud storage profile must be configured in advance by a vCloud administrator.