Oracle® Communications Application Orchestrator

Plug-in Guide for Session Delivery Network Elements
Release 1.1

April 2016

ORACLE

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 Oracle Legal Notices section was updated. • The About This Guide section was updated.

1

Overview

This guide is used by an administrator who wants to use the preexisting Oracle session delivery network element plug-ins for Oracle Communications Application Orchestrator and Oracle Communications Session Element Manager. Oracle Communications Session Element Manager works collaboratively with Oracle Communications Application Orchestrator to help manage Composite Network Functions (CNFs) and provide full life-cycle support for NFs.

The following diagram shows how the plug-ins fit with Oracle Communications Application Orchestrator in a network functions virtualization (NFV) architecture.

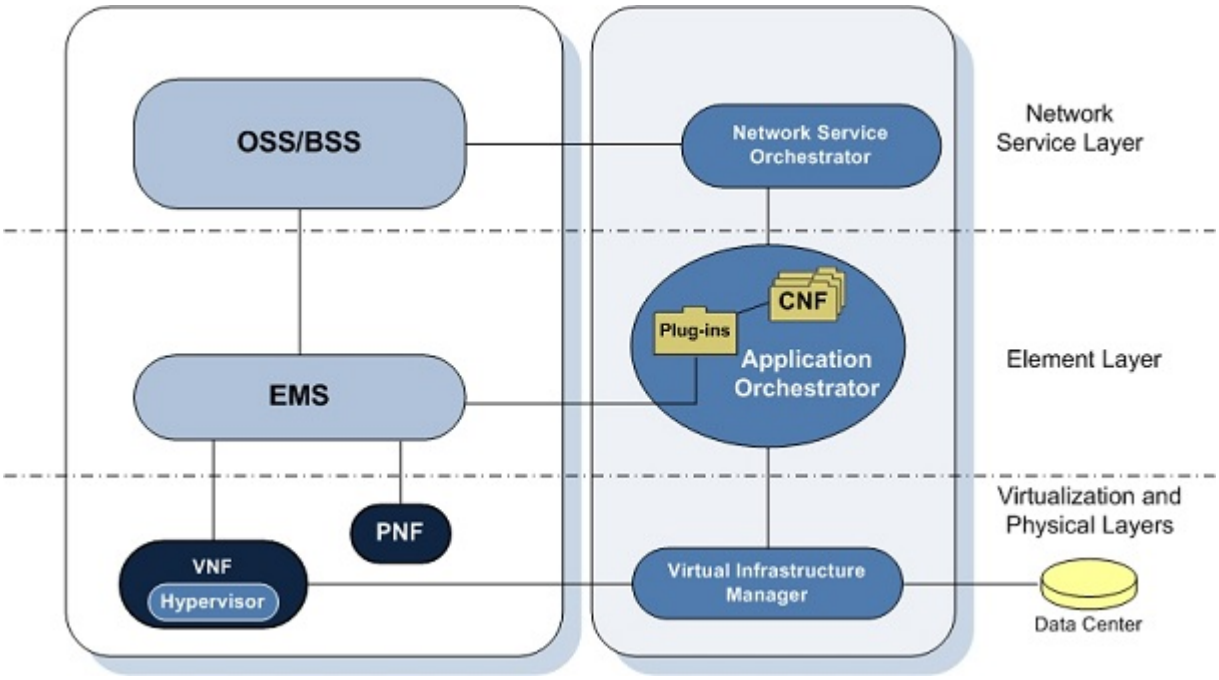


Figure 1: Oracle Communications Application Orchestrator in the network

About Application Orchestrator Plug-ins

Oracle Communications Application Orchestrator provides orchestration support for multi-vendor devices through a plug-in platform comprised of pre-existing CNFs and vendor CNFs containing Virtual Network Functions (VNFs),

Physical Network Functions (PNFs) or any combination of both, and manages the interaction of these plug-ins. Any vendor can create an EMS or CNF plug-in for the specific requirements of a device and have their devices orchestrated through Oracle Communications Application Orchestrator. Pre-existing CNFs are described in this guide. See vendor-specific plug-in documentation for more information.

2

Session Element Manager and Application Orchestrator Collaboration

Oracle Communications Session Element Manager (installed with Oracle Session Device Manager) is an EMS that can be installed with Oracle Communications Application Orchestrator.

For the purpose of managing and maintaining session delivery Network Functions (NFs), the Oracle Communication Session Element Manager can be used for collaboration with the Oracle Communication Application Orchestrator. The Oracle Communications Session Element Manager provides full life-cycle support for a PNF or VNF, which includes the configuration, loading and provisioning capabilities for devices, and performance management for session delivery network elements.

Configure Session Element Manager for Application Orchestrator

The following tasks need to be completed on the Oracle Communications Session Element Manager so that it can work properly with Oracle Communications Application Orchestrator:

- Add a user group and configure the AoSystem user that Oracle Communications Application Orchestrator uses to login to Oracle Communications Session Element Manager through the REST API. See the following section for more information.
- Configure the offline configuration for your CNF(s). See the *Oracle Communications Session Element Manager User Guide* for more information.
- Add one or more device groups in the EMS for Oracle Communications Application Orchestrator to communicate with the EMS.
- Configure a Reusable Configuration Module (RCM) template on the EMS to apply a simplified configuration inputs to applicable (non-specific) devices or Network Functions (NFs). The RCM is designed so that the user does not need to know the element required for a specific task, or the configuration complexity of many attributes. For example, an RCM template might require inputs like the SIP Trunk, H.323 SIP inter-working endpoints to a session agent group (SAG), and diameter signaling router (DSR) component. See the *Oracle Communications Session Element Manager User Guide* for more information.

Add Application Orchestrator Login Parameters for Session Element Manager

The **AoSystem** user is required for Oracle Communications Application Orchestrator to communicate with Oracle Communications Session Element Manager.

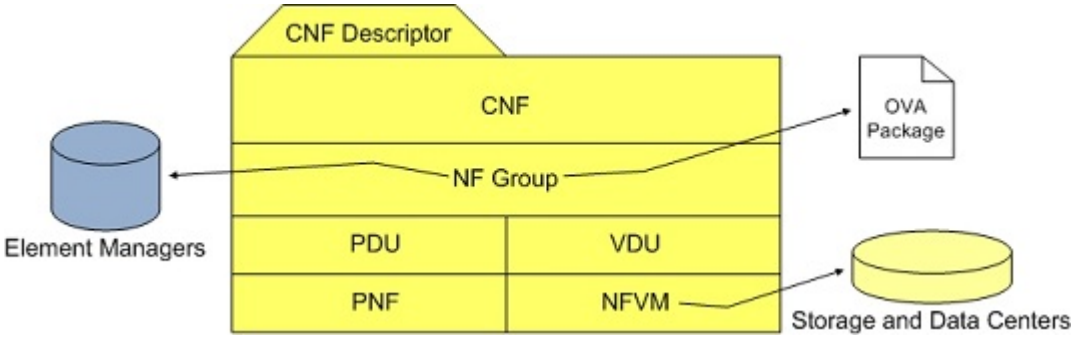
1. In **Security Manager**, create an Oracle Communications Application Orchestrator group with the **provisioners** permissions.
2. Create the explicit user name that is used by Oracle Communications Application Orchestrator to login to Oracle Communications Session Element Manager through the REST API.
3. Create your password for the **AoSystem** user.
4. Log out of Oracle Communications Application Orchestrator and log back into Oracle Communications Application Orchestrator as the **AoSystem** user.
   If you are logging into Oracle Communications Application Orchestrator for the first time, you are prompted to change the password you initially configured and enter the new password and re-enter the new password to confirm it. The next time you log into Oracle Communications Application Orchestrator, you are prompted for this new password.
5. In the login window, enter **AoSystem** in the **Username** field.
6. Enter the password that you assigned to the **AoSystem** user in the **Password** field and click **Login.**

3

Staging and Promoting a Pre-existing CNF from the CNF Catalog

You can stage any of the pre-existing session delivery network element CNFs that are available in the CNF catalog and promote a CNF that you select 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.



About Session Delivery Network Element CNF Plug-ins

Oracle Communications Application Orchestrator includes pre-existing network function (NF) descriptors in the onboarding catalog that define network function (NF) requirements for some of the following Oracle session delivery network elements:

- Oracle Communications Core Session Manager supports core session management (CSM) capabilities in network function virtualization (NFV) environments to efficiently share hardware resources across different services and customers. These capabilities include IP multi-media subsystem (IMS) call/session control functions (CSCF) and break-out gateway control function (BGCF) and their associated 3GPP interfaces.
- The Oracle Communications Session Border Controller (SBC) connects disparate IP communications networks while mitigating security threats, curing interoperability problems, and ensuring reliable communications. It protects and controls realtime voice, video, and unified communications (UC) as they traverse IP network borders.
- The subscriber-aware load balancing and route management (SLRM) mechanism is a single target for devices sending SIP messages to your IMS core over the applicable interfaces within the CSM. SLRM provides proprietary Oracle Communications load-balanced services that connect users to a group of CSMs as if they are a

single node. The load balancing functions are limited to Oracle CSM targets over the Sc diameter interface that defines the information exchange between the Oracle CSM and the SLRM .

When you choose **Onboarding** > **Catalog**, you see the following window:

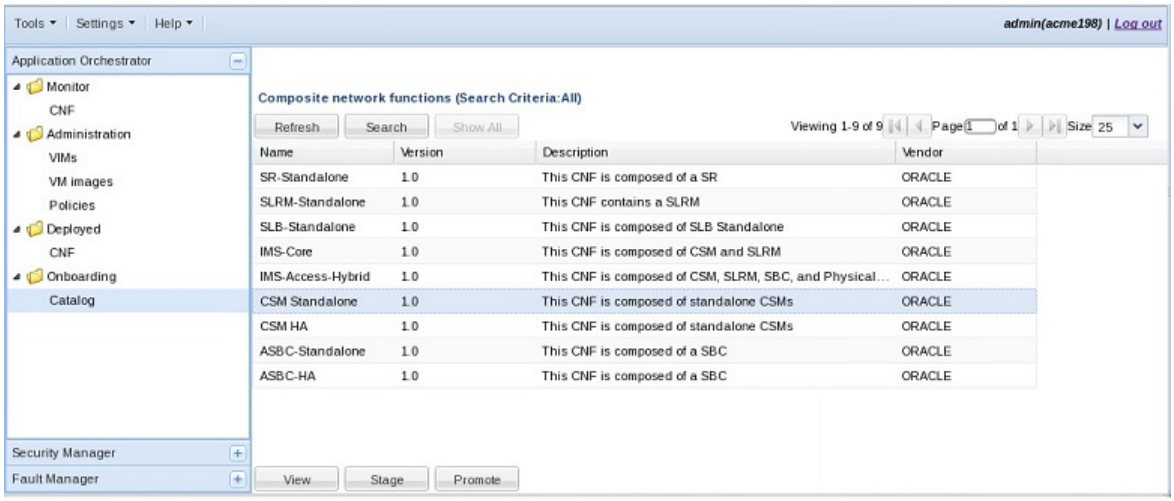


Figure 2: Oracle Communications Application Orchestrator Pre-existing Plug-ins

The following table describes the pre-existing CNFs that were included with the Oracle Communications Application Orchestrator in the **Composite network functions** table:

Note: The supported component types are associated with each plug-in and are selected when you add a VM application image to Oracle Communications Application Orchestrator.

Plug-in	Description	Supported Component Types
ASBC-Standalone	This CNF is composed of access standalone Oracle Communications Session Border Controllers.	• **SBC**
ASBC-HA	This CNF is composed of access high availability Oracle Communications Session Border Controllers.	• **SBC** • **Peering_SBC**
CSM Standalone	This CNF is composed of standalone Oracle Communications Core Session Manager.	**CSM**
CSM HA	This CNF is composed of high availability Oracle Communications Core Session Manager.	**CSM**
IMS-Core	This CNF is composed of the core IP multi-media Subsystem (IMS), which consists of a CSM, SLRM.	• **CSM** • **SLRM** • **USM**
IMS-Access-Hybrid	This CNF is composed of access-hybrid IMS, which consists of a CSM and SLRM running on virtual machines (VMs) with an access SBC and SLB running on physical devices to provide a hybrid solution.	• **CSM** • **SLRM** • **SLB** • **SBC** • **USM** (Oracle Communications Unified Session Manager)
SLB-Standalone	This CNF is composed of physical standalone Oracle Communications Session Load Balancer.	**SLB**

Plug-in	Description	Supported Component Types
SLRM-Standalone	This CNF is contains subscriber-aware load balancing and route management (SLRM) mechanisms.	**SLRM**
SR-Standalone	This CNF is composed of virtual standalone Oracle Communications Session Routers.	• **Transaction_SR** • **Session_SR**

Stage a Session Delivery Network Element 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 the users wants 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: This configuration provides an example of the resource criteria for the fields that represent Oracle Communications Session Delivery Network Element plug-ins.

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.

Name	Description
Minimum Subscribers field	The minimum number of subscribers.
Maximum Subscribers field	The maximum number of subscribers.
Minimum Registrations per Second field	The minimum number of registrations.
Maximum Registrations per Second field	The maximum number of registrations.
Sizing Model drop-down list	Select from the following staging (sizing) model based on the hardware required for VM resource usage: • **Small** • **Medium** • **Large**

4. Click **OK**.
   Oracle Communications Application Orchestrator automatically stages the CNF and the staged CNF appears in the **Staged CNFs** table.

4

Configure the CNF for Session Delivery Network Elements

The tasks in this chapter are used to configure specific networking parameters for an NF group belonging to the promoted Oracle Communications session delivery network element CNF so that it can be put in a deployable state.

Configure the Oracle Communications Session Element Manager

Use this task to configure Oracle Communications Session Element Manager so that it can manage the configuration of the DUs. The fields and values described in this task represent the Oracle Communications Session Element Manager implementation with a standalone Oracle Communications Session Border Controller. If you are configuring a different pre-existing CNF, some of the fields and values described below may be different.

1. Expand the **Application Orchestrator** slider and choose **Deployed** > **CNF** to navigate to the **Deployed CNF** table.
2. Choose a CNF from the **Deployed CNF** table and click **Expand**.
3. In the CNF detailed view, choose 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.
EM reference field	The name of the Oracle Communications Session Element Manager device. For example: **MyOCSEM**.

Name	Description
Last modified	Displays the last time EM parameters were created or modified for the CNF NF group.
OCSDM Base URL field	The base URL used to access the EMS device. Port 8080 is for HTTP and Port 8443 is for HTTPS. For example: **https://myems:8443**
OCSDM User name field	Enter **AoSystem**. The AoSystem user name is used by Oracle Communications Application Orchestrator to log into Oracle Communications Session Element Manager through the REST interface. See the "Add Application Orchestrator Login Parameters for Session Element Manager" section of the *Session Element Manager and Application Orchestrator Collaboration* chapter for more information on configuring the AoSystem user.
OCSDM Password field	The password for the AoSystem user that is used by Oracle Communications Application Orchestrator to log into Oracle Communications Session Element Manager through the REST interface. See the "Add Application Orchestrator Login Parameters for Session Element Manager" section of the *Session Element Manager and Application Orchestrator Collaboration* chapter for more information on configuring the AoSystem user password.
Device user password field	This password is required for external connections to the NF using the user account.
Confirm device 'admin' password field	Reenter the administrator-level password.
Device admin password field	This password is required for external connections to the NF using the *admin* account.
Device configuration password field	The protected configuration password on the NF device. This password is required so that the EMS can access configuration mode on the NF device.
Confirm device 'configuration' password field	Reenter the configuration-level password.
Device group drop-down list	Click **Load** to load one or more EMS device groups. A device group is chosen so that all NFs deployed in this NF group are associated with this device group.
Offline Configuration drop-down list	Click **Load** to load one or more offline configuration templates. The configuration templates are filtered to be appropriate for the VM image chosen, the NF software version targeted, and the resilience policy defined for this NF group. Selecting a configuration template assigns this template as the golden master for all the NF instances that are deployed in this group.
SNMP community name	The SNMP community name that the NF device uses.
Use Device Cluster check box	The check box is always selected by default. All NF device instances belong to a device cluster in the EMS, which maintains configuration synchronization between all members. We recommend that this check box always be selected. If the check box is unselected, then the NF device instances do not belong to a cluster and the configuration and management is the responsibility of the provisioner. Click **Load** to retrieve existing available device clusters or enter a new device cluster name that the EMS ensures gets created.

Name	Description
Device cluster name field	The name of the device cluster.
License entitlements field	This field displays the license entitlements needed by some of the session delivery NFs to enable features on the device. The **Load** button loads the entitlements if required. The entitlements are discussed in the following rows.
Capacity field	The valid value is zero.
FEATURE_ACCOUNTING check box	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for RADIUS, an accounting, authentication, and authorization (AAA) system.
FEATURE_IPV6	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for licensed use of IPv6 addresses.
FEATURE_SAG	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for session agent group name resolution for resolving addresses found in Session Initiation Protocol (SIP) contact headers.
FEATURE_QOS	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for quality of service (QoS) based routing.
FEATURE_SESSION_RECORDING	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for session recording server (SRS) operation to receive replicated media and record signalling.
FEATURE_IWF	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for inter-working function (IWF) to interconnect SIP networks with H.323 networks.
Routing	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for session routing and load balancing for SIP and H.323 services.
Policy Server	Check the check box if you want to enable the Oracle Communications Session Border Controller feature for Diameter-bsed external policy servers.
Last modified	Displays the last time EMS parameters were created or modified for the CNF NF group.

5. 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 in this task are specific to the Oracle Communications Session Element Manager.

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 choose **Deployed** > **CNF**.
2. In the **Deployed CNF** table, choose the CNF and click **Expand**.

3. In the CNF detailed view, choose 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. Choose a data center and click **Configure**.
6. In the **Configure common DU settings** dialog box, complete the following fields:

Name	Description
Default Gateway field	The default gateway IP address for the network on which the DUs are located so that the data center has connectivity to all the DUs belonging to this NF group.
Netmask field	The subnetwork mask for the DU network.
Vlan field	The VLAN number. The default is zero. Zero indicates that there is no VLAN.

7. Click **OK**.
8. In the the **DU** tab, click **Apply**.