# Oracle® Application Management Pack for Oracle Communications

System Administrator's Guide

Release 12.1.0.2

**E57646-02**

February 2015

ORACLE®

Oracle Application Management Pack for Oracle Communications System Administrator's Guide, Release 12.1.0.2

E57646-02

# Contents

## 3 Configuring Oracle Communications Targets



## 4 Managing Communications Applications with Enterprise Manager Cloud Control

## 5 Monitoring Billing and Revenue Management

## 9 Monitoring Oracle Communications Integrations

# Preface

This document describes how to implement and use the Application Management Pack for Oracle Communications.

## Audience

This document is intended for system administrators and other individuals who are responsible for configuring, managing and maintaining Oracle Communications applications using Oracle Enterprise Manager Cloud Control.

## Downloading Oracle Communications Documentation

Application Management Pack for Oracle Communications documentation and additional Oracle documentation, such as Oracle Database and Oracle Enterprise Manager Cloud Control documentation, is available from Oracle Help Center:

http://docs.oracle.com

## Documentation Accessibility

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

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

## Related Documents

For more information about Oracle Communications applications, see the product documentation for the respective application.

For more information about the installation, configuration, deployment, and upgrade processes using Oracle Enterprise Manager Cloud Control, see the Oracle Enterprise Manager Cloud Control Documentation.

# 1

# Understanding Application Management Pack for Oracle Communications

This chapter provides an overview of Oracle Application Management Pack for Oracle Communications.

## Overview of Application Management Pack for Oracle Communications

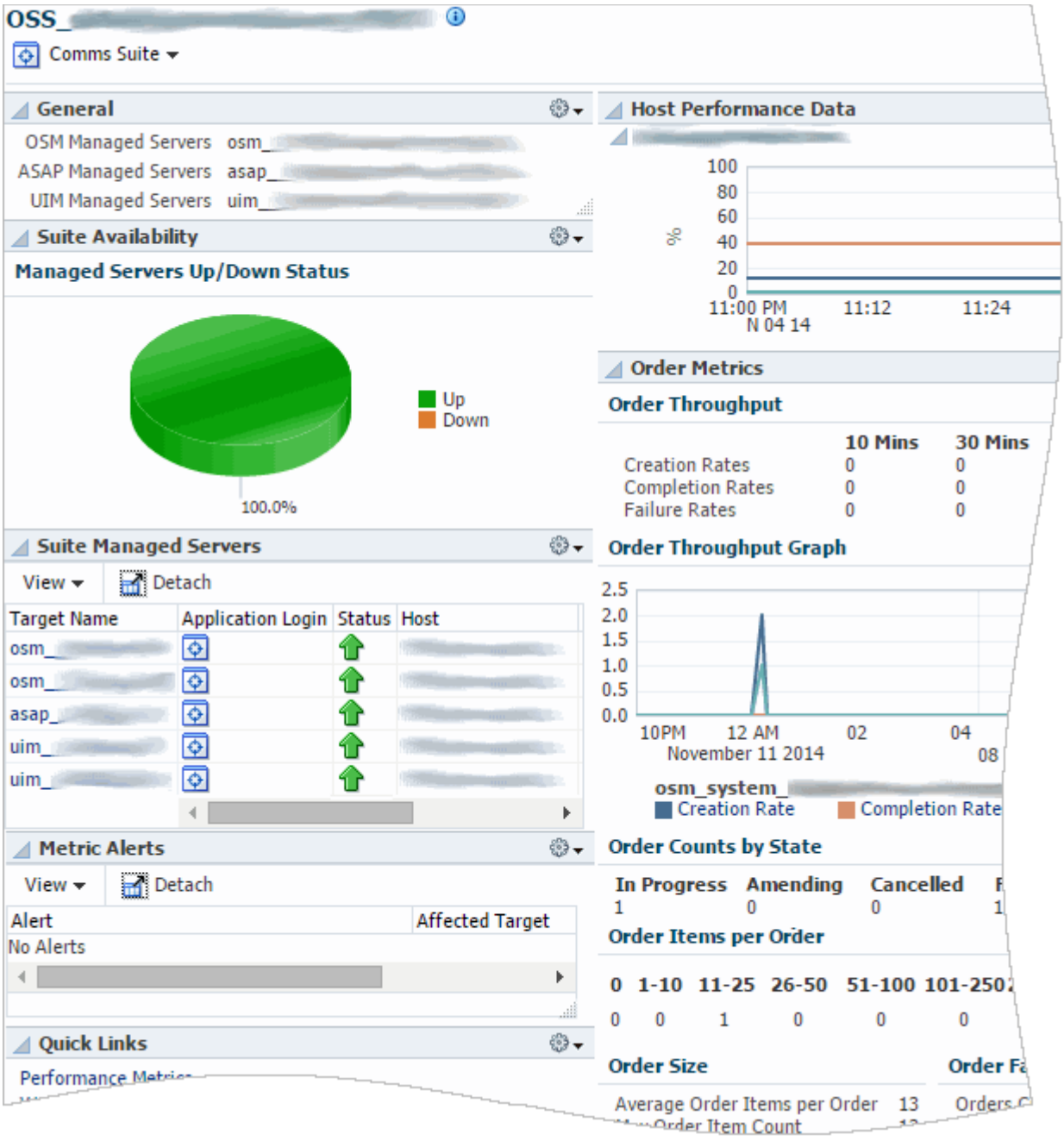
Application Management Pack for Oracle Communications consists of a plug-in for Oracle Enterprise Manager Cloud Control that provides management capabilities for supported Oracle Communications applications.

System administrators use Application Management Pack for Oracle Communications with Enterprise Manager Cloud Control to provision, configure, patch, and monitor Oracle Communications applications and solutions, allowing the deployment and maintenance of Oracle Communications applications from a centralized, Web-based console, simplifying implementations.

Figure 1–1 shows an Enterprise Manager Cloud Control home page with information from Oracle Communications operation support system (OSS) applications. This example presents a single view of information from Oracle Communications Order and Service Management (OSM), Oracle Communications Unified Inventory Management (UIM), and Oracle Communications ASAP. The home page includes application status and availability, alerts, and metrics such as hardware resource usage and order throughput.

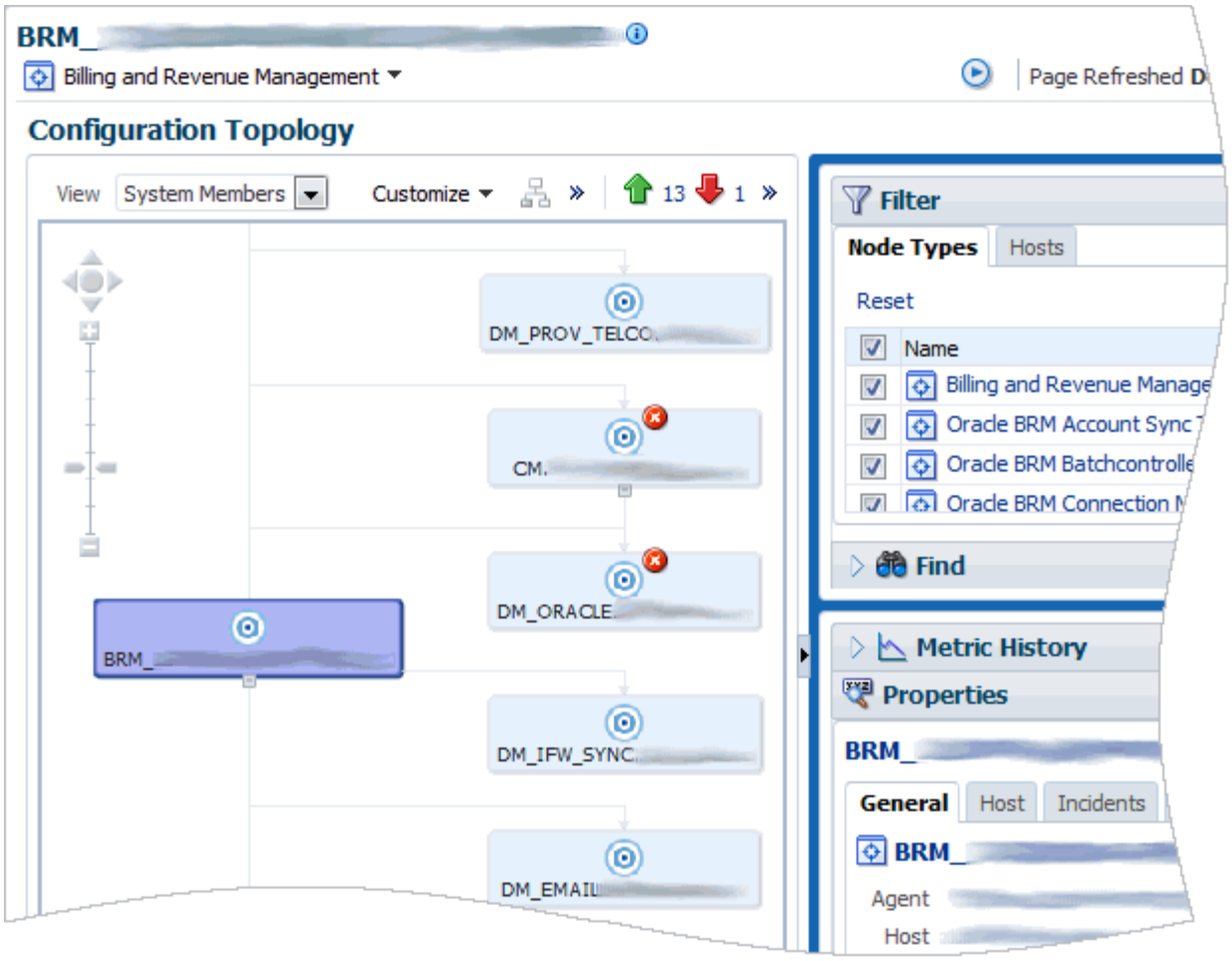
Application Management Pack for Oracle Communications also provides individual home pages for supported applications and application components.

***Figure 1–1 Home Page Showing Multiple Applications in a Suite***



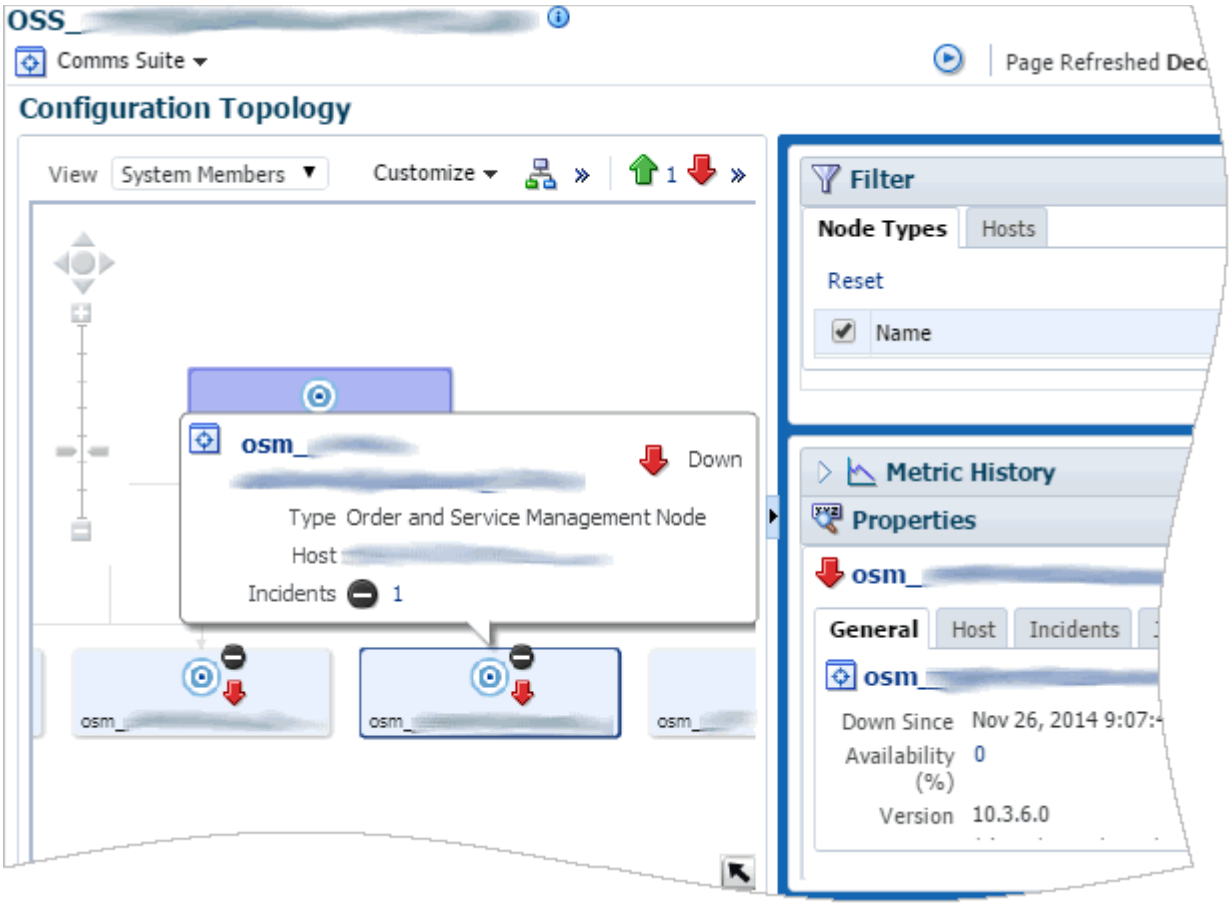

Application Management Pack for Oracle Communications displays managed Oracle Communications targets allowing you to view application, component, and host status. For example, view the topology of Oracle Communications Billing and Revenue Management (BRM) components such as the Connection Manager (CM) and Data Managers (DMs), as shown in Figure 1–2.

***Figure 1–2 BRM Topology***



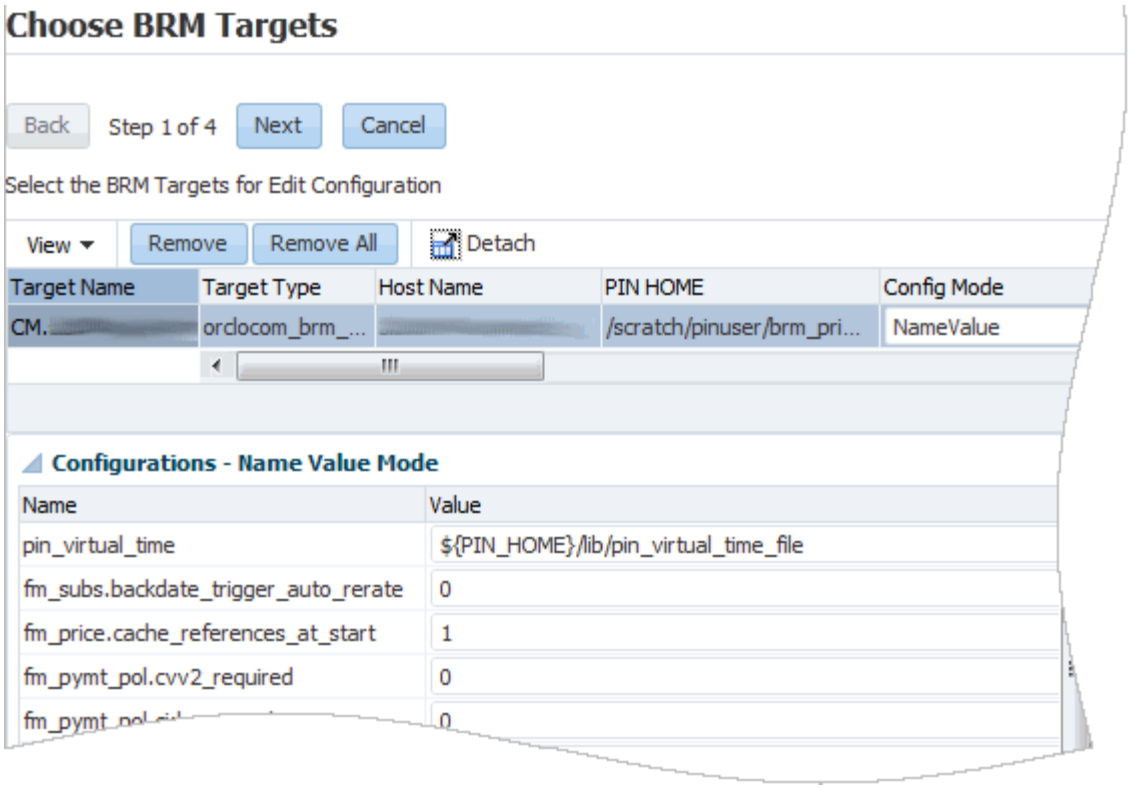

The configuration topology provides a visual representation of managed target relationships. Clicking on an element in the topology provides additional details in the Properties panel. Hovering over an element in the topology provides additional details as shown in Figure 1–3.

***Figure 1–3 Communications Suite Topology with Detail Pop-Up***




You can configure parameters for Oracle Communications applications from a single location and deploy the settings to multiple targets. Figure 1–4 shows an example of BRM parameter configuration.

***Figure 1–4 Configuring BRM Parameters***




# Key Benefits

Application Management Pack for Oracle Communications provides the key benefits that let you:

- Install, configure, and monitor Oracle Communications applications, including supported suite solutions and individual applications, from a centralized location.
- Install BRM in multischema environments with up to 9 schemas.
- Discover and monitor existing Oracle Communications applications installed independently of Application Management Pack for Oracle Communications.
- Discover and monitor Oracle Communications application infrastructure components, including Oracle Enterprise databases, Oracle WebLogic Server application servers, and Oracle Application Integration Architecture (Oracle AIA) Pre-Built Integrations.
- View graphical representations of system topology for Oracle Communications applications.
- Monitor in-depth order throughput and lifecycle metrics for OSM systems, servers, order types, and cartridges.
- Monitor and compare the compliance of OSM installations with Oracle's recommended settings
- Enforce configuration policies across multiple installations of BRM, ensuring consistent versioning and configuration.
- Recover quickly from Oracle AIA faults.
- Update and patch BRM.

- Upgrade Oracle Communications Pricing Design Center (PDC).
- Manage support requests using direct integration with Oracle Support.
- Alert system administrators when configurable operating thresholds are passed through multiple notification channels

## Supported Applications

Application Management Pack for Oracle Communications supports the installation, configuration, patching, and monitoring of the following Oracle Communications applications and versions:

- BRM version 7.5 Patch Set 10 with Patch 19921037
- Oracle Communications Elastic Charging Engine (ECE) version 11.2 Patch Set 3
- PDC version 11.1 Patch Set 6
- Oracle Communications Pipeline Configuration Center (PCC) version 1.1
- Oracle Communications Network Charging and Control (NCC) version 5.0.2
- OSM version 7.2.4.1
- UIM versions 7.2.3 and 7.2.4.1
- ASAP versions 7.2.0 and 7.2.0.3
- Oracle Application Integration Architecture Oracle Communications Pre-Built Integrations (Oracle AIA) versions 11.3 and 11.4

## Supported Suite Solutions

Application Management Pack for Oracle Communications supports the installation and configuration of the following Oracle Communications suite solutions:

- Oracle Communications Order to Cash
- Oracle Communications OSS Service Fulfillment

Highly-available versions of these suites are also supported.

## Application Management Process Flow

Implementing and using Application Management Pack for Oracle Communications requires the following process flow:

1. Installing Enterprise Manager Cloud Control and the Application Management Pack for Oracle Communications plug-in. See "Installing Application Management Pack for Oracle Communications" for more information.
2. Configuring Oracle Communications application targets, setting preferred credentials, and deploying the Oracle Management Agent to each target. See "Configuring Oracle Communications Targets" for more information.
3. Deploying the Application Management Pack for Oracle Communications Management Agent to each Enterprise Manager Cloud Control server and target host. In most cases, Management Agents for Oracle Enterprise Database and Oracle Fusion Middleware must also be deployed to targets. See "Configuring Oracle Communications Targets" for more information.

4. Managing, including installing, configuring, and updating Oracle Communications applications with Enterprise Manager Cloud Control. See "Managing Communications Applications with Enterprise Manager Cloud Control" for more information.
5. Monitoring Oracle Communications applications with Enterprise Manager Cloud Control. See "Managing Communications Applications with Enterprise Manager Cloud Control" for more information.

# Assumptions and Limitations

This section discusses product assumptions and limitations.

## Assumptions

This guide assumes the following:

- Familiarity with Enterprise Manager Cloud Control functionality.
- Proper installation and configuration of Oracle Enterprise Manager Cloud Control including the Oracle Enterprise Database.
- Supported operating systems on the target hosts where Application Management Pack for Oracle Communications installs and monitors Oracle Communications applications.
- Supported versions of Oracle Communications applications are used.
- Network connectivity between the Enterprise Manager Cloud Control host and the Oracle Communications applications targets.
- Availability and licensing of supported Oracle Communications application installers, patches, and updates.
- An understanding of the installation and configuration parameters of supported Oracle Communications applications.

## Solution Limitations

Application Management Pack for Oracle Communications has the following limitations:

### Oracle RAC Database Limitations

Provisioning of Oracle Communications applications other than BRM using Oracle Real Application Clusters (Oracle RAC) database is not supported. However, you can use the plug-in to discover and monitor existing application instances using Oracle RAC databases. Only versions of applications with official support for Oracle RAC database are discoverable.

### BRM Patch Recommendations Limitations

Application Management Pack for Oracle Communications does not support the Enterprise Manager Cloud Control patch recommendation feature. You will not see any recommended Oracle Communications applications patches. You can manually search for and apply Billing and Revenue Management patches using the administration console.

Enterprise Manager Cloud Control administration console still displays host and security related patch recommendations for targets.

### BRM Multischema Limitations

Multischema database configuration is not supported when using multiple database users (multiuser) configuration. You cannot use different database users for multiple instances of the BRM schema on the same host.

Multischema provisioning only supports BRM instances on the same host.

### PCC Limitations

Provisioning PCC with Secure Sockets Layer (SSL) is not supported.

## Directory Placeholders Used in This Guide

Table 1–1 describes the directory placeholders used in this guide.

***Table 1–1 Directory Placeholders Used in This Guide***

| Placeholder | Directory Description |
|---|---|
| *EM_home* | The directory in which Enterprise Manager Cloud Control is installed. |
| *BRM_home* | The directory in which BRM is installed. |
| *Oracle_home* | The directory in which Oracle products are installed. |
| *Database_home* | The directory in which an application's database is installed. |

# 2

# Installing Application Management Pack for Oracle Communications

This chapter describes Oracle Application Management Pack for Oracle Communications system requirements, and how to install, deploy, upgrade, and uninstall Application Management Pack for Oracle Communications.

## System Requirements

You install Application Management Pack for Oracle Communications as a plug-in on an existing Oracle Enterprise Manager Cloud Control instance. The plug-in is supported on Enterprise Manager Cloud Control version 12c Release 4.

See the Enterprise Manager Cloud Control documentation library for information about Enterprise Manager Cloud Control system requirements and installation procedures.

Enterprise Manager Cloud Control requires an Oracle Enterprise Database. See the Oracle Enterprise Database documentation for information about installing and configuring Oracle Enterprise Database.

For more information about system requirements and certified versions for Enterprise Manager, see the Enterprise Manager Base Platform certification matrix available on *My Oracle Support*.

---

**Caution:** The Oracle Management Repository for Enterprise Manager is **not** certified on Oracle Database 12*c*. For the full functionality described in this guide, the Management Repository must be configured in an Oracle Database version listed in the Enterprise Manager certification matrix.

---

This guide assumes a properly configured Enterprise Manager Cloud Control and Enterprise Database environment.

### Supported Oracle Communications Applications

Managed application targets must meet the system requirements listed in the application's documentation. For more information, see the Oracle Communications application documentation available on the Oracle Software Delivery Cloud and Oracle Technology Network at:

- https://edelivery.oracle.com

- http://www.oracle.com/technetwork/indexes/documentation/oracle-communications-185806.html

See "Supported Applications" for a list of supported Oracle Communications applications and versions.

# Installing the Application Management Pack for Oracle Communications Plug-in

Install the plug-in using one of the following methods:

- Installing the Plug-in using Enterprise Manager Self Update
- Installing the Plug-in Using an OPAR File

## Installing the Plug-in using Enterprise Manager Self Update

You install the Application Management Pack for Oracle Communications plug-in using Self Update in the Enterprise Manager Cloud Control administration console.

To install the plug-in using Self Update:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Extensibility**, and then **Self Update**.
3. Select the **Plug-in** row and click **Open**.
4. Select the row for the **Oracle Communications** plug-in.
5. Click **Download**.

The plug-in becomes deployable after the download completes. See "Deploying the Application Management Pack for Oracle Communications Plug-In" for information about deploying the plug-in.

## Installing the Plug-in Using an OPAR File

You can download the Oracle Plug-in Archive (OPAR) version of the plug-in from the Oracle Software Delivery Cloud and install the OPAR using the Enterprise Manager Command-Line Utility (EMCLI).

For information about OPAR files and EMCLI, see the Enterprise Manager Cloud Control documentation.

To install the plug-in using the OPAR file and EMCLI:

1. Download the Application Management Suite for Communications plug-in from the Oracle Software Delivery Cloud:

   https://edelivery.oracle.com

2. Copy the **12.1.0.2.0_oracle.cgbu.ocom_2000_0.opar** file to the Enterprise Manager Cloud Control host.
3. In a terminal session, navigate to the **oms/bin** directory of your Enterprise Manager Cloud Control installation.
4. Configure the EMCLI connection to the Enterprise Manager Cloud Control host using the following command:

   ```
   ./emcli setup -url=https://host:port/em -username=sysman -password=password
   -trustall
   ```

where *host* and *port* are the connection values for the Enterprise Manager Cloud Control server and *password* is the password for the sysman user.

5. Import the Application Management Suite for Communications OPAR file using the following command:

```
./emcli import_update -file=filepath/12.1.0.2.0_oracle.cgbu.ocom_2000_0.opar
-omslocal
```

where *filepath* is the absolute path to the location where the **12.1.0.2.0_ oracle.cgbu.ocom_2000_0.opar** file is located.

6. Verify the successful plug-in import:
   a. Log in to the Enterprise Manager Cloud Control administration console.
   b. From the **Setup** menu, select **Extensibility**, and then **Plug-ins**.
   c. In the Applications folder, verify that there is an **Oracle Communications** row.

See "Deploying the Application Management Pack for Oracle Communications Plug-In" for information about deploying the plug-in.

# Deploying the Application Management Pack for Oracle Communications Plug-In

After installing the plug-in, deploy it on the Enterprise Manager Cloud Control Management Server and target host agents.

## Deploying the Plug-In on the Management Server

To deploy the plug-in on the Management Server:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Set up preferred credentials for the target hosts. See "Setting Up Host Preferred Credentials" for more information.
3. From the **Setup** menu, select **Extensibility**, and then **Plug-ins**.
4. From the **Applications** folder, select the **Oracle Communications**.
5. From the **Deploy On** menu, select **Management Servers**.

   The **Deploy Plugin on Management Servers** dialog appears.
6. In the **Password** field, enter the password for the **sys** user and click **Continue**.
7. Complete the remaining steps in the dialog box.
8. Click **Deploy**.
9. Monitor the status to ensure successful deployment.
10. Install the default configuration template files. See "Installing the Default Configuration Template Files" for more information.

## Deploying the Plug-In on Management Agents

The plug-in must be deployed to each Management Agent on host targets running Oracle Communications applications. Before deploying the plug-in to a Management Agent you must add the host target to your Enterprise Manager Cloud Control instance. See "Adding Host Targets Manually and Installing the Management Agent" for information on adding host targets.

To deploy the plug-in to an Oracle Communications host target Management Agent:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Extensibility**, and then **Plug-ins**.
3. Expand **Applications**.
4. Right-click **Oracle Communications**.
5. Select **Deploy On**, and then **Management Agent**.

   The **Deploy Plug-in on Management Agent** window appears.
6. Click **Continue**.
7. Select the targets on which to deploy the plug-in.
8. Click **Continue**.
9. Confirm there are no errors indicated by the pre-requisite check.
10. Click **Next**.
11. Click **Deploy**.
12. Confirm that the Application Management Pack for Oracle Communication plug-in deploys successfully.
13. Repeat steps 1 through 12 for all Oracle Communications host targets.

For more information about the Plug-In Manager, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

# Upgrading the Application Management Pack for Oracle Communications Plug-In

You can upgrade the plug-in using the Self Update feature in Enterprise Manager Cloud Control. You must deploy the updated plug-in to the Management Server and Management Agents.

Upgrading and deploying the plug-in involves the following tasks:

1. Check whether a new version of the plug-in is available. See the discussion of checking the availability of plug-ins in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details.
2. Download the newest version of the plug-in. See "Installing the Plug-in using Enterprise Manager Self Update" for details.
3. Deploy the newest version of the plug-in to Oracle Management Service. See "Deploying the Plug-In on the Management Server" for details.
4. Deploy the newest version of the plug-in on each Management Agent. See "Deploying the Plug-In on Management Agents" for details.
5. Confirm that the newest version of the plug-in was successfully deployed as follows:
   a. Log in to the Enterprise Manager Cloud Control administration console.
   b. From the **Setup** menu, select **Extensibility**, and then **Plug-ins**.

      The Plug-ins page appears.
   c. Select the **Oracle Communications** row.

d. From the **Actions** menu, select **Information**.

   The Plug-in Information page appears.

e. On the **General** tab, confirm that the values for **Latest Available Version**, **Version Downloaded**, **Version** are all the same.

f. In the Certified Targets table, confirm that the values for **Plug-in Version** and **Plug-in Version on Management Server** are the same.

6. Install the default configuration template files. See "Installing the Default Configuration Template Files" for details.

For more information about upgrading plug-ins, see the chapter about managing plug-ins in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

For more information about Self Update, see the chapter about updating Cloud Control in *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

## Uninstalling the Application Management Pack for Oracle Communications Plug-In

To remove Application Management Pack for Oracle Communications:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Extensibility**, and then **Plug-ins**.
3. In the **Applications** folder, select **Oracle Communications**.
4. Click **Undeploy From** and undeploy the plug-in from all Management Agents.
5. Click **Undeploy From** and undeploy the plug-in from all Management Servers.

For more information, see the discussion of undeploying plug-ins in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

## Installing the Default Configuration Template Files

Application Management Pack for Oracle Communications provides parameter template files used by Enterprise Manager Cloud Control to install and configure supported Oracle Communications applications. You must install the default configuration template files provided to the Enterprise Manager Cloud Control domain.

To install the configuration templates:

1. Log in to the Enterprise Manager Cloud Control host on which you have installed and deployed the Application Management Pack for Oracle Communications plug-in.
2. Create the following directory structure in your Enterprise Manager Cloud Control instance:

   *EM_home*/**../gc_inst/user_projects/domains/GCDomain/default_xml/platform**
3. Copy the *EM_home*/**plugins/oracle.cgbu.ocom.oms.plugin_12.1.0.2.0/metadata/swlib/platform/components/default_xml.zip** to *EM_home*/**../gc_inst/user_projects/domains/GCDomain/default_xml/platform**.
4. Unzip **default_xml.zip** into the **platform** directory.

### About Provisioning Variables

The **default_xml.zip** archive includes the **platform_suite_default.xml** file. This file contains the parameters used by the Communications Suite Installation Procedure for each supported application. See the supported application installation guides for specific information on these values and their role in application installation.

Editing **platform_suite_default.xml** allows the definition of commonly used or static environmental values, such as user names and port values, in your environment. The provisioning procedure pre-populates the values used in this configuration file.

The following example shows the configurable *db_name* **value** parameter for a Billing and Revenue Management database SID in the **platform_suite_default.xml** file:

```
<parameter mandatory="true" name="DATABASE_SID" value="db_name"
category="orclocom_brm" basic="true" type="DBRegister">
      <label locale="en" value="Database SID"/>
</parameter>
```

Make a copy of the edited **platform_suite_default.xml** file and save it in a secure location.

## Creating the Oracle Communications Folders for BRM Installers

If you are provisioning Billing and Revenue Management, you must create the **CommSuiteProvisioning** and **BRMComponents** folders in the Enterprise Manager Cloud Control Software Library to store installers used during the provisioning procedure.

To create the folders:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Enterprise** menu, select **Provisioning and Patching**, and then **Software Library**.
3. From the **Actions** menu, select **Create Folder**.
4. In the **Name** field, enter **CommsSuiteProvisioning**.
5. Click **OK**.
6. Select the **CommsSuiteProvisioning** folder.
7. From the **Actions** menu, select **Create Folder**.
8. In the **Name** field, enter **BRMComponents**.
9. Click **OK**.

## Enabling Application Management Pack for Oracle Communications Logging

Enable java logging for Application Management Pack for Oracle Communications in Enterprise Manager Cloud Control by updating the **logging.xml** file located in the following directory on your Enterprise Manager Cloud Control Management Server host:

*EM_home***/gc_inst/user_projects/domains/GCDomain/config/fmwconfig/servers/EMGC_OMS1**

To enable logging:

1. Log in to the Management Server host as a user with permissions to modify the Enterprise Manager Cloud Control configuration.
2. Change directory to *EM_home*/**gc_inst/user_projects/domains/GCDomain/config/fmwconfig/servers/EMGC_OMS1**.
3. Open the **logging.xml** file with a text editor.
4. Add a new entry for the Application Management Pack for Oracle Communications log handler. Use the following example as a guide:

```
 <log_handler name='comms-ams-handler'
class='oracle.core.ojdl.logging.ODLHandlerFactory'
filter='oracle.dfw.incident.IncidentDetectionLogFilter'>
   <property name='path'
value='${domain.home}/servers/${weblogic.Name}/sysman/log/comms-ams.log'/>
   <property name='maxFileSize' value='10485760'/>
   <property name='maxLogSize' value='104857600'/>
   <property name='encoding' value='UTF-8'/>
   <property name='useThreadName' value='true'/>
   <property name='supplementalAttributes' value='J2EE_APP.name,J2EE_
MODULE.name,WEBSERVICE.name,WEBSERVICE_PORT.name,composite_instance_
id,component_instance_id,composite_name,component_name'/>
  </log_handler>
```

5. Add a new entry for a logger referring to the log handler created in step 4. Use the following example as a guide:

```
<logger name='oracle.communications.platform.em' level='NOTIFICATION'
useParentHandlers='false'>
   <handler name='comms-ams-handler'/>
  </logger>
```

   Set the logging level by editing the **level** value in the logger entry. For example, the following logger entry provides trace logging of all messages:

```
<logger name='oracle.communications.platform.em' level='TRACE:32'
useParentHandlers='false'>
   <handler name='comms-ams-handler'/>
  </logger>
```

   Setting the logging level to **TRACE:32** produces large amounts of logging data and should only be used for resolving issues with your Application Management Pack for Oracle Communications environment. See the chapter about logging in *Oracle Enterprise Manager System Administrator's Guide* for more information on setting logging levels.
6. Save the changes made to **logging.xml** and exit the editor.

You are not required to restart the Enterprise Manager Cloud Control Management Server to activate changes to logging configuration.

# 3

# Configuring Oracle Communications Targets

This chapter discusses configuring new and existing Oracle Communications targets in Oracle Enterprise Manager Cloud Control for use with Oracle Application Management Pack for Oracle Communications.

## Understanding Oracle Communications Targets

You provision, configure, and monitor Oracle Communications applications on hosts set up as managed targets in Enterprise Manager Cloud Control. Enterprise Manager Cloud Control also manages non-host targets. Managed non-host targets consist of applications and their components, and infrastructure such as Oracle Enterprise Databases and Oracle WebLogic Server domains.

An Oracle Management Agent runs on each host where one or more targets exist. The Enterprise Manager Cloud Control Management Server communicates with the Management Agent performing operations including application provisioning, configuration, and monitoring. You must install the Management Agent on any host you plan on using with Application Management Pack for Oracle Communications.

For more information about managed targets see the chapter about discovering and monitoring targets in *Oracle Enterprise Manager Cloud Control Administrator's Guide* available at:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/discovery.htm

## Setting Up Host Preferred Credentials

Application Management Pack for Oracle Communications uses preferred credentials for authentication between the Management Server and managed host targets. You set either default credentials for target types or target-specific credentials that are stored in the Enterprise Manager Cloud Control repository. Executing procedures and administrative tasks on host targets from the Management Server, such as provisioning applications and starting Oracle WebLogic Server domains, uses preferred credentials.

To set up host preferred credentials:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Security**, and then **Preferred Credentials**.
3. Select **Host** under **Target Type** in the table.
4. Click **Manage Preferred Credentials**.
5. Do one of the following:

- To set default preferred credentials, click **Set** under **Default Preferred Credentials**.
- To use target preferred credentials, click **Set** under **Target Preferred Credentials**.

You can also set up target preferred credentials when adding a new managed host.

See the discussion of preferred credentials in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for more information about preferred credentials.

## Ensuring Correct Preferred Credentials Permissions on Host Targets

Remote procedures and administrative tasks launched from the Management Server execute on target hosts. You must set the necessary file and directory permissions on target hosts for the users that perform actions on the target host. This ensures that commands and scripts execute properly on target hosts.

For example:

- A WebLogic Server domain on a target host may be deployed in a mounted file share physically located on a third host. The user that starts this domain must exist on the third host and have execute permissions in the mounted file share to run the start scripts.
- The BRM user must have full permissions on the directory where the agent is installed, and the agent user must have at least read and execute permission on the directory where BRM is installed. See "Setting Permissions on BRM Hosts" for more information about setting BRM permissions.

Ensure that the preferred credentials you create for the managed hosts in your environment exist on accessed hosts and have the needed permissions in the file locations where your applications may be installed.

# Adding Host Targets Manually and Installing the Management Agent

To manually add a host to Enterprise Manager Cloud Control and install the Management Agent on the new host:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Add Target**, and then **Add Targets Manually**.
3. From the Instruction options, select **Add Host Targets.**
4. Click **Add Host**.
5. In the **Add Host Targets: Host and Platform** wizard, click **Add**.
6. In the **Host** field, enter the new target's host name.
7. From the **Platform** menu, select the correct operating system platform.
8. Click **Next**.
9. In the **Installation Base Directory** field, enter an installation base directory for the new target. This specifies the directory on the target host where you want the software binaries, security files, and inventory files of the Management Agent to be copied.
10. In the **Instance Directory** field, enter an instance directory on the new target. This specifies the directory on the target host where Management Agent configuration files are stored.

11. Select a **Named Credential** for Management Agent installation on the new target. See "Setting Up Host Preferred Credentials" for more information on setting up host credentials.
12. Confirm the **Privileged Delegation Setting** and **Port**, as well as any **Optional Details** needed in your installation.
13. Click **Next**.
14. Confirm the value in the **Host Information** field and click **Deploy Agent**.
15. Confirm that the Management Agent is properly installed and the new target is now visible in the administration console.

> **Note:** To see database associations in the topology view for Oracle Communications applications, you must add the host on which the database resides to Enterprise Manager Cloud Control and install a Management Agent on the host.

For detailed information on installing the Management Agent, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide* at:

http://docs.oracle.com/cd/E24628_01/install.121/e22624/install_agent.htm

### Setting Permissions on BRM Hosts

For BRM targets, after installing the Management Agent on the BRM host, you must set specific permissions that correspond to the credentials you use in Enterprise Manager for monitoring BRM. These permissions allow you to use Enterprise Manager Cloud Control to perform actions on BRM components and run scripts located in the directory where the Management Agent is installed.

To set the required BRM permissions:

1. On the BRM host operating system, add the agent user and the BRM host user to the same user group.
2. Give BRM user read, write, and execute permissions for the directory where the Management Agent is installed.
3. Give the agent user read and execute permissions for the directory where BRM is installed.
4. Run the **root.sh** script in the directory where the Management Agent is installed.

## Adding Oracle Communications Targets

You add Oracle Communications targets after their hosts obtain managed status and receive a Management Agent. You must also deploy the Application Management Pack for Oracle Communications plug-in to each Management Agent before performing discovery.

Add Oracle Communications application targets using guided or automatic discovery. Table 3–1 shows which type of discovery Application Management Pack for Oracle Communications supports for each application target.

*Table 3–1 Types of Discovery for Oracle Communications Targets*

| Type of Discovery | Target |
|---|---|
| Automatic | Oracle Communications Elastic Charging Engine (ECE)<br>Oracle Communications Billing and Revenue Management (BRM)<br>Oracle Application Integration Architecture (AIA) Oracle Communications Pre-Built Integrations (Oracle Communications Integration target type)<br>Oracle Communications Network Charging and Control (NCC)<br>Oracle Communications Order and Service Management (OSM)<br>Oracle Communications Unified Inventory Management (UIM)<br>Oracle Communications ASAP |
| Guided | BRM<br>OSM<br>UIM<br>ASAP |

When you discover operations support systems (OSS) targets such as OSM, UIM, and ASAP, Enterprise Manager Cloud Control automatically discovers their WebLogic Server domains as well. The domain appears in the application's topology view and you can monitor the domain on the domain's home page.

Use the following methods for adding non-host Oracle Communications targets to your Enterprise Manager Cloud Control Management Server:

- Discovering Targets Automatically
- Discovering and Rediscovering Targets Using Guided Discovery
- Adding Existing Oracle Communications Applications Using Monitoring Properties

Before discovering Oracle Communications application targets, obtain information about the application instances, such as installation locations, user credentials, and database and server connection details, from your system administrator.

## Discovering and Rediscovering Targets Using Guided Discovery

Application Management Pack for Oracle Communications provides a guided discovery module for discovering existing targets on managed hosts for the following Oracle Communications applications:

- BRM
- OSM
- UIM
- ASAP

You must rediscover BRM targets after provisioning or uninstalling an individual BRM component, editing the BRM configuration files, or patching BRM.

### Rediscovering BRM Targets Using Guided Discovery

Rediscovering a BRM target ensures that Enterprise Manager Cloud Control accurately reflects any changes made to the BRM system.

Rediscover a BRM target in the same way as you discover a new target, as described in "Discovering Targets Using Guided Discovery", ensuring that you do the following:

- When you enter information in the **Application Information** fields, use the same values as the existing BRM target.
- Select the **Overwrite existing BRM Targets** option before clicking **Submit**.
- Confirm that Enterprise Manager Cloud Control has updated the BRM targets with the latest information.

When you rediscover the target, Enterprise Manager Cloud Control rediscovers the entire BRM suite of targets and components.

If you have configured automatic discovery for BRM, you are not required to rediscover BRM after provisioning or uninstalling components.

### Discovering Targets Using Guided Discovery

To discover and promote existing Oracle Communications application targets:

1. Back up existing Oracle Communications applications configurations files, such as **pin.conf** and **pin_ctl.conf** for BRM or **oms-config.xml** for OSM.
2. For BRM, confirm the variables listed in Table 3–2 are correctly set in the **pin_ctl.conf** file for your environment. This file is located in the *BRM_home*/**bin** directory on your BRM server, where *BRM_home* is the directory where BRM is installed.

   See the section about customizing the **pin_ctl** utility environment variables in *Oracle Communications Billing and Revenue Management System Administrator's Guide* for more information on setting the required variables.

***Table 3–2 Required pin_ctl.conf Variables for Guided Discovery***

| Variable | Description |
|---|---|
| NLS_LANG | The database language used in the BRM database. |
| ORACLE_HOME | The home directory of the Oracle database used by BRM. |
| TNS_ADMIN | The directory in which the **tnsnames.ora** file referencing the database used by BRM is located. |
| PIN_LOG_DIR | The BRM directory in which logs are stored. Set **PIN_LOG_DIR** to:<br>`BRM_home/var` |
| LD_LIBRARY_PATH | Set **LD_LIBRARY_PATH** to:<br>*Oracle_home*`/lib64:`*Oracle_Home*`/lib:`*Database_Home*`/lib:`<br>*Database_home*`/rdbms/lib:$LD_LIBRARY_PATH` |
| LD_LIBRARY_PATH_64 | Set **LD_LIBRARY_PATH_64** to:<br>*Oracle_home*`/lib64:`*Oracle_home*`/lib:`*Database_home*`/lib:`<br>*Database_home*`/rdbms/lib:$LD_LIBRARY_PATH` |
| PATH | Set **PATH** to:<br>*Oracle_Home*`/bin:$PATH` |
| EVENT_HANDLER_PORT | For BRM Pipeline only.<br>Set **EVENT_HANDLER_PORT** to the port to which the Pipeline Manager Event Handler listens. |

3. Ensure that the Application Management Pack for Oracle Communications plug-in is deployed on the application host.
4. Log in to the Enterprise Manager Cloud Control administration console.
5. From the **Setup** menu, select **Add Target**, and then **Add Targets Manually**.

   The Add Targets Manually page appears.
6. From the Instruction options, select **Add Targets Using Guided Process**.
7. From **Target Types**, select one of the following:
   - For OSM, UIM, or ASAP targets, select **Oracle Communications OSS Applications Discovery**.
   - For BRM, select **Oracle Communications Billing and Revenue Management Discovery**.
8. Click **Add Using Guided Process**.
9. In the **Choose Targets** wizard, click **Add**.
10. Select the host on which the existing application is installed, and then click **Select**.
11. Select one of the following check boxes for the application to discover:
    - **OSS** (OSM, UIM, and ASAP)
    - **BRM**

    You cannot discover both OSS and BRM targets at the same time.
12. Under Application Information, do one of the following:
    - To discover OSS targets, from the **SelectApplication** list, select the applications to discover. You can select more than one option.
    - To discover BRM targets, from the **Select Product Type** list, select **PortalBase** or **Pipeline**.
13. Enter the information for the environment in the **Domain Configuration** and **Application Information** fields.

    Table 3–3 describes the BRM discovery fields.

***Table 3–3 BRM Discovery Fields***

| Fields | Description |
|---|---|
| PipelineIFWhome or Portalbase Pinhome | The path to the directory in which BRM is installed. |
| ThirdPartyLocation | The path to the directory in which the BRM Third Party package is installed. |
| DatabaseHome | The path to the Oracle Enterprise Database client package directory located on your BRM server. |
| TNS_ADMIN | The path to the directory on your BRM host in which the **tnsnames.ora** file pointing to your database is located. |
| BRM Pin User | The BRM host user. |
| BRM Pin Password | The BRM host password. |

*Table 3–3 (Cont.) BRM Discovery Fields*

| Fields | Description |
|---|---|
| BRM Registry File Name | For Pipeline targets only, the names of the registry files, such as **wireless.reg** or **wirelessRealtime.reg**.<br>To discover both pipeline and real-time pipeline targets, enter both registry files separated by a comma. For example:<br>`wireless.reg,wirelessRealtime.reg` |

Table 3–4 describes the OSS discovery fields.

*Table 3–4 OSS Discovery Fields*

| Field | Description |
|---|---|
| EM Repository Owner | The user name of the Enterprise Manager repository owner. |
| EM Repository Owner Password | The password of the Enterprise Manager repository owner. |
| WebLogic Hostname | The host name of the domain on which the OSS products are deployed. |
| WebLogic Port | The port number of the host on which the OSS products are deployed. |
| WebLogic Admin User | The administrator user name with which to connect to the WebLogic Server host. |
| WebLogic Admin Password | The administrator password with which to connect to the WebLogic Server host. |
| JMX Protocol | The connection protocol to use when connecting to the WebLogic server. |
| ASAP Environment ID | The unique identifier for your ASAP environment. This field appears when you select ASAP from the **SelectApplication** list. |

14. (Optional) To rediscover the BRM base target after provisioning or uninstalling an individual BRM component, editing BRM configuration, or patching BRM:

    Select the **Overwrite existing BRM Targets** option.

15. (Optional) To register most types of database for monitoring and topology view:

    a. Select the **Register DB** option.

    b. Provide the connection details and user credentials for the database. If you are discovering multiple OSS products, enter the database details for each product.

    If you are discovering BRM and your database is an Oracle Real Application Clusters (Oracle RAC) database, do not select the **Register DB** option. Instead, you must associate the database after discovering the BRM and Oracle RAC targets. See "Associating Oracle RAC Database Targets with BRM Targets" for more information.

16. (Optional) To create a logical group or add the target to an existing logical group:

    a. Select the **Enable Logical Grouping** option.

    b. Do one of the following:

    – Create a new logical group by entering a unique logical group name.

- Add the target to an existing logical group by clicking **Browse** and selecting an existing logical group.

17. Click **Submit**.
18. Confirm that the existing application installation is added by verifying that the new targets are now visible in the Enterprise Manager Cloud Control administration console. Some applications result in a single target addition while others may include more than one target.

    See "Monitoring Oracle Communications Application Targets" for information on how to view newly discovered targets.
19. Perform the appropriate post-discovery tasks for the target, as described in "Post-Discovery Tasks".

For general information about discovering existing hosts and promoting targets, see the discussion of automatically discovering and monitoring targets in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

## Discovering Targets Automatically

Enterprise Manager Cloud Control can automatically discover unmanaged hosts on your network by using IP scanning or discovery modules. Once you have discovered unmanaged hosts, you can promote them to managed status. Promoting a host to managed status installs a Management Agent on the host, allowing Enterprise Manager Cloud Control to perform additional functions on the new target, including automatic discovery of applications.

Application Management Pack for Oracle Communications provides discovery modules used for automatically discovering the following target types on managed hosts:

- ECE running on Oracle Coherence
- BRM
- Oracle Communications Integration (AIA)
- NCC
- OSM
- UIM
- ASAP

Automatic discovery involves the following tasks:

- For ECE and Integration targets:
  - ECE Pre-Discovery Tasks
  - Integrations Pre-Discovery Tasks
- For all targets:
  - Configuring Automatic Discovery
  - Running Automatic Discovery On Demand
  - Viewing Automatic Discovery Errors
  - Promoting Discovered Targets
- For BRM targets on Oracle RAC databases:

– Associating Oracle RAC Database Targets with BRM Targets

### ECE Pre-Discovery Tasks

Before configuring automatic discovery for ECE targets:

1. Discover and promote the Coherence clusters on which ECE is running.

   For more information about adding existing ECE Coherence clusters to Enterprise Manager Cloud Control, see the discussion of discovering Coherence targets in the *Getting Started with Management Pack for Oracle Coherence* chapter in *Oracle Enterprise Manager Cloud Control Getting Started with Oracle Fusion Middleware Management*.

2. Enable the Coherence Management Pack as follows:

   a. Log in to the Enterprise Manager Cloud Control administration console.

   b. From the **Setup** menu, select **Management Packs**, and then **Management Pack Access**.

   c. Under **View Options**, select **All Targets**.

   d. From the **Pack Access** options, select **Pack Based Batch Update**.

   e. Enable the **Management Pack for Oracle Coherence** by selecting the pack and moving it to the **Selected Packs** window.

   f. Click **Apply**.

### Integrations Pre-Discovery Tasks

Before configuring automatic discovery for Integration targets:

1. Discover and promote the SOA application and infrastructure targets on which the integration is deployed.

   See the discussion of managing Oracle SOA in *Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide* for more information about discovering SOA targets.

2. Ensure that you have set the preferred credentials for the WebLogic Server domain on which the integration is deployed. See "Setting Up Host Preferred Credentials" for more information.

### Configuring Automatic Discovery

To configure managed hosts to run automatic discovery:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Add Target**, and then **Configure Auto Discovery**.

   The Setup Discovery page appears.

3. Click the **Targets on Hosts** tab.
4. Highlight the host on which you want to discover targets. For ECE, this is a Coherence target host.
5. Click **Discovery Modules**.
6. From the **Enabled** column, select the type of target you want to discover.

   You can select more than one type of target at once.

7. For all Oracle Communications target types except NCC, click **Edit Parameters**. NCC does not have any editable parameters.
8. For NCC targets, skip this step.

   For all other targets, enter the parameters for the application you want to discover.

   Table 3–5 describes the fields for ECE.

***Table 3–5 ECE Automatic Discovery Fields***

| Field | Description |
|---|---|
| Agent EMD URL | The main URL of the Management Agent on the target host. |
| ECE Home | The path to the directory in which ECE is installed. |
| JMX Port | The JMX port number of the ECE management node. |
| Hostname | The host name of the ECE management node. |
| Service Name | The service name of the ECE management node. |

Table 3–6 describes the fields for BRM.

***Table 3–6 BRM Automatic Discovery Fields***

| Field | Description |
|---|---|
| Portalbase Pinhome | The path to the directory in which BRM is installed. |
| ThirdPartyLoc | The path to the directory in which the BRM third-party package is installed. |
| TNS_ADMIN | The path to the directory on your BRM host in which the **tnsnames.ora** file that points to your database is located. |
| Oracle Client Directory | The Oracle home directory containing access libraries and binaries, corresponding to the 64-bit client. |
| Pipeline InstallLoc | The directory where BRM pipeline is installed. |
| Pipeline RegistryFile | The path to the BRM pipeline registry file. |

Table 3–7 describes the fields for OSS products.

***Table 3–7 OSS Product Automatic Discovery Fields***

| Field | Description |
|---|---|
| WebLogic Host Name | The host on which the OSS product is deployed. |
| WebLogic Port | The port number of the host on which the OSS product is deployed. |
| WebLogic User Name | The user name with which to connect to the WebLogic Server host. |
| WebLogic Password | The password with which to connect to the WebLogic Server host. |
| T3/T3s Protocol | The connection protocol to use when connecting to the WebLogic server. |
| Deployment Names | A colon-separated list of the types of OSS products to discover. The default value is **oms:asap:oracle.communications.inventory**. |
| Comms Plugin Version | The version of Application Management Pack for Oracle Communications that you are using. |

Table 3–8 describes the fields for Integration targets (Oracle AIA).

***Table 3–8 Integrations Automatic Discovery Fields***

| Field | Description |
|---|---|
| SOA WebLogic Admin Server Host Name | The host name of the WebLogic Server administration server. |
| SOA WebLogic Admin Server Port | The port number of the WebLogic Server administration server. |
| SOA WebLogic Protocol (t3/t3s) | The connection protocol to use when connecting to the WebLogic server. |
| SOA WebLogic Admin Server User Name | The user name with which to connect to the WebLogic Server host. |
| SOA WebLogic Admin Server Password | The password with which to connect to the WebLogic Server host. |

These fields are not immediately validated. The discovery module uses the values to contact the Management Agent on the specified host when attempting to add the target and reports any validation errors at that time.

9. Click **OK** in the Edit Parameters window.
10. Click **OK**.

    The list of managed hosts appears.

### Running Automatic Discovery On Demand

By default, automatic target discovery runs once daily. You can set a discovery interval to suit your environment, as described in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

You can also run automatic discovery on demand at any other time you want to discover targets.

To run automatic discovery on demand:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Add Target**, and then **Configure Auto Discovery**.
3. Click the **Targets on Hosts** tab.
4. Select a row from the list of managed host targets.
5. Click **Discover Now**.

   A confirmation dialog box appears.
6. Click **Yes**.

   The **Targets on Hosts** tab appears.

If the discovery succeeded, a green check mark appears beside the date and time in the **Most Recent Ended On** column. You can promote the targets as described in "Promoting Discovered Targets".

If the discovery failed, a red and white X appears beside the date and time in the **Most Recent Ended On** column. Follow the steps in "Viewing Automatic Discovery Errors" to help you resolve the error and then retry the automatic discovery.

### Viewing Automatic Discovery Errors

To view failed automatic discoveries and get more details about automatic discovery errors:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Add Target**, and then **Configure Auto Discovery**.
3. Click the **Targets on Hosts** tab.
4. From the **Most Recent Ended On** column, click the date and time link for the failed discovery.

   The diagnostic details for that host appear.
5. From the **Error** column, click an error link for more details.

   The full error text appears. For example:

   ```
   Failure ::Wrong Directories for the host entry example.com : InstallLocation -
   /brm_home/installation
   ```

Use the information provided in the error text to help you resolve the automatic discovery failure. In the example above, you would provide the correct installation directory in the Edit Parameters dialog box for the BRM discovery module of the **example.com** host.

### Promoting Discovered Targets

After automatically discovering targets, promote them so that you can monitor and manage them. For ECE, you must promote each cluster and node found by automatic discovery.

To promote discovered targets:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Setup** menu, select **Add Target**, and then **Auto Discovery Results**.

   The Auto Discovery Results page appears
3. Click the **Targets on Hosts** tab.
4. Select the row of the automatically discovered targets that you want to promote.

   **Note:** Oracle ECE Cluster target types include **BRM** in the target name. Oracle ECE Node target types include the name of the host and the name of the ECE node in the target name.
5. Click **Promote**.

   The Promote *target_type* Target(s) page appears.
6. For BRM and NCC targets, skip this step.

   For ECE, OSS, and Integrations targets, enter the required credentials and properties for the target.

   Table 3–9 describes the required fields for ECE.

*Table 3–9 ECE Promotion Fields*

| Field | Description |
|---|---|
| Monitoring Username | The user name for the ECE monitoring user. |
| Monitoring Password | The password for the ECE monitoring user. |
| Bulk Operations MBean | The name of the bulk operations MBean. |
| Cluster Name | The name of the ECE cluster. |
| Communication Protocol | The cluster communications protocol. |
| ECE Installation Directory | The path to the directory where ECE is installed. |
| ECE Version | The version of ECE. |
| JMX Remote Port | The ECE target's JMX remote port. |
| Machine Name | The host on which the ECE target runs. |
| Service Name | The service used for performing remote management. |
| Service URL | The service URL used for remote management. |

Table 3–10 describes the required fields for OSS targets:

*Table 3–10 OSS Promotion Fields*

| Property | Description |
|---|---|
| EM repository Owner | The user name of the Enterprise Manager repository owner. |
| EM repository Owner Password | The password of the Enterprise Manager repository owner. |
| WebLogic Admin Password | The password of the WebLogic Server administrator account. |
| ASAP Environment ID | The unique identifier for your ASAP environment. This field appears when you are promoting an ASAP target. |

Table 3–11 describes the required fields for Integration targets (AIA).

*Table 3–11 Integration Promotion Fields*

| Property | Description |
|---|---|
| EM Admin/Sysman User-name | The user name of the Enterprise Manager administrator. |
| EM Admin/Sysman Password | The password of the Enterprise Manager administrator. |
| SOA Home | The path to the directory in which SOA is installed. |
| Communications Integration Home (Pre-built/AIA Home) | The path to the directory in which the Oracle AIA pre-built integrations are installed. |
| Host-Name | The host name of the database.<br>Enter values for this field under both Communications Integration and SOA database details. |
| Port | The port number of the database.<br>Enter values for this field under both Communications Integration and SOA database details. |

*Table 3–11 (Cont.) Integration Promotion Fields*

| Property | Description |
|---|---|
| SID | The unique identifier of the database.<br>Enter values for this field under both Communications Integration and SOA database details. |
| User-Name | The user name of the database user.<br>Enter values for this field under both Communications Integration and SOA database details. |
| Password | The password of the database user.<br>Enter values for this field under both Communications Integration and SOA database details. |
| System User-Name | The user name of the database system user.<br>Enter values for this field under both Communications Integration and SOA database details. |
| System Password | The password of the database system user.<br>Enter values for this field under both Communications Integration and SOA database details. |

7. For NCC, OSS, and Integrations targets, skip this step.

   For BRM targets, edit the monitoring credentials:

   a. Click **Specify Common Monitoring Credentials**.

   b. Select an existing credential name or create a new one.

   c. In the **Credential Details** table, enter the username and password for the BRM user for whom you set permissions in "Setting Permissions on BRM Hosts".

   d. Click **Save**.

      The credentials for all BRM targets in the list of targets to be promoted are saved.

8. (Optional) To register most types of database for monitoring and topology view, do one of the following:

   - For NCC, ECE, and OSS targets, and BRM targets without an Oracle RAC database:

     a. Select the **Register DB** option.

     b. Provide the connection details and user credentials for the database.

   - For BRM with an Oracle RAC database, do not select the **Register DB** option. Instead, associate the database manually after discovering both BRM and Oracle RAC targets. See "Associating Oracle RAC Database Targets with BRM Targets" for more information.

   - For Integration targets:

     a. Under **Communication Integration Database Detail** or **SOA Database Detail**, select the **Register DB for Monitoring** option.

        You can register the Oracle AIA database only, the SOA Database only, or both.

     b. Provide values for the **System User-Name** and **System Password** fields.

9. For Integrations targets, skip this step.

(Optional) For all other target types, to create a logical group or add the target to an existing logical group:

a. Select the **Enable Logical Grouping** option.

b. Do one of the following:

- Create a new logical group by entering a unique logical group name.
- Add the target to an existing logical group by clicking **Browse** and selecting the logical group.

10. Click **Promote**.

    The target is promoted to managed status. You can view the target on the All Targets page.

11. Perform the appropriate post-discovery tasks for the target, as described in "Post-Discovery Tasks".

## Post-Discovery Tasks

For some Oracle Communications applications you must perform additional tasks before you can monitor them correctly. The following tasks apply to certain targets:

- Adding BRM Components to the pin_ctl.conf File: For BRM targets.
- Configuring SNMP for BRM Pipeline Targets: For BRM Pipeline and Real-Time Pipeline targets.
- Associating Oracle RAC Database Targets with Application Targets: For application targets installed on Oracle RAC databases.
- Adding the UIM Database Password to the Communications Suite Target: For UIM targets in a Communications suite.
- Configuring Compliance for an OSM Cluster: For OSM targets in a clustered environment.

### Adding BRM Components to the pin_ctl.conf File

You may have installed BRM components that do not appear in the **pin_ctl.conf** file. Before you can use Enterprise Manager Cloud Control to start or stop these components, you must add them to **pin_ctl.conf**.

If you do not know whether you installed components that do not appear in **pin_ctl.conf**, you can check using the following procedure.

To add components to **pin_ctl.conf**:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the BRM target home page, as described in "Viewing Home Pages".
3. In the Components Installed region, review the list of installed components.
4. On the host where BRM is installed, open the following file:

   *BRM_home*`/bin/pin_ctl.conf`

5. Search for the following line:

   ```
   1 dm_oracle
   ```

6. Compare the list of components to the list in the Components Installed region of the BRM target home page in Enterprise Manager Cloud Control.

7. Add a line for any components that appear in the Components Installed region but do not appear in the **pin_ctl.conf** file.

   For example, if DM_AQ and DM_PROV_TELCO components appear in the Components Installed region, add the following lines:

   ```
   1 dm_oracle
   1 dm_prov_telco
   1 dm_aq
   start_dm_aq cpidproc:dm_aq: cport:port
   ```

   where *port* is the port on which the Oracle Advanced Queueing Data Manager listens.

   **Note:** The target name column of the Components Installed region includes host information with the component name. Do not include the host in **pin_ctl.conf**.

8. Save and close the file.

### Configuring SNMP for BRM Pipeline Targets

After discovering BRM Pipeline and Real-Time Pipeline targets, configure Simple Network Management Protocol (SNMP). For more information about using SNMP with BRM, see the discussion of using the SNMP Instrumentation protocol to monitor and control BRM components in *Oracle Communications Billing and Revenue Management System Administrator's Guide*.

To configure SNMP, do the following for each BRM Pipeline and Real-Time Pipeline target:

1. Install the SNMP software as described in *Oracle Communications Billing and Revenue Management Installation Guide*.
2. Start the SNMP master agent with the following command:

   ```
   master_agent -l Master_agent_port -x AgentX_port &
   ```

   where *Master_agent_port* is the port for the SNMP server and *AgentX_port* is the port for the SNMP agent
3. Open the following file:

   ```
   Pipeline_home/conf/wireles.reg
   ```

   where *Pipeline_home* is the directory where the BRM Pipeline target is installed
4. In the **Instrumentation** section, under **SnmpServer**, edit the value for the **Port** entry to match the value you used for *AgentX_port* when you started the master agent. For example:

   ```
   Instrumentation
     {
     SnmpServer
     {
       Port = AgentX_port
   ```

5. Save and close the file.
6. Log in to the Enterprise Manager Cloud Control administration console.

7. From the **Targets** menu, select **All Targets**.
8. In the Target Type tree, select **Oracle BRM Pipeline** or **Oracle BRM RTP**.
9. From the list of targets, right-click the name of the BRM Pipeline target for which you are configuring SNMP.
10. From the context menu, select **Target Setup,** and then **Monitoring Credentials**.
11. In the **SNMP AgentX Port** field, enter the port that you used for *AgentX_port* when you started the master agent.
12. In the **SNMP Master Agent Port** field, enter the port that you used for *Master_agent_port* when you started the master agent.
13. Click **OK**.

    The home page for the BRM Pipeline target appears.
14. In the Summary region, click **ReStart**.

## Associating Oracle RAC Database Targets with Application Targets

When your Oracle Communications application targets are installed on Oracle RAC databases, you must perform additional tasks before you can view the Oracle RAC database details on the application target's topology page. These tasks are different for BRM and OSS products.

### Associating Oracle RAC Database Targets with BRM Targets

To associate an Oracle RAC database with a BRM target:

1. In any order, do the following:
   a. Discover the Oracle RAC database target as described in the discussion of discovering cluster database targets in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
   b. Discover the BRM target as described in "Adding Oracle Communications Targets". During discovery or while promoting automatically discovered targets, do not select the **Register DB** option.
2. On the BRM target home page, click **AssociateRACDB**.
3. Confirm that the database was successfully associated by viewing the BRM target's topology page. See "Viewing Topology" for more information about topology pages.

### Associating Oracle RAC Database Targets with OSS Targets

To associate an Oracle RAC database target with an OSS target:

1. In any order, do the following:
   a. Discover the Oracle RAC database target as described in the discussion of discovering cluster database targets in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
   b. Discover the OSS target as described in "Adding Oracle Communications Targets". During guided discovery or while promoting automatically discovered targets, select the **Register DB** option and provide the required database credentials.

2. Confirm that the database was successfully associated by viewing the BRM target's topology page. See "Viewing Topology" for more information about topology pages.

### Adding the UIM Database Password to the Communications Suite Target

To add the UIM database password to the communications suite target:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the UIM target home page, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Target Setup**, and then **Monitoring Configuration**.
4. In the **UIM DB User Password** field, enter the database password for UIM.
5. Click **OK**.

### Configuring Compliance for an OSM Cluster

If you are monitoring compliance for OSM targets in a clustered environment, you must configure coherence remote management, which allows you to specify one server as the MBean server that manages all other servers.

You configure coherence remote management by adding and setting system properties for the OSM managed servers that you have discovered.

To configure coherence remote management:

1. Go to the directory of the domain where OSM is deployed, for example:

   `/u01/Oracle/Middleware/`*`user_projects`*`/domains/`*`OSM_Domain`*

2. Open the startup script for the single OSM managed server that you want to designate as the MBean server.
3. Add and set the following properties:

   ```
   -Dtangosol.coherence.management.remote=true
   -Dtangosol.coherence.management=all
   ```

4. Save and close the file.
5. Open the startup script for any other OSM managed server.
6. Add and set the following properties:

   ```
   -Dtangosol.coherence.management.remote=true
   -Dtangosol.coherence.management=none
   ```

7. Save and close the file.
8. Repeat steps 5 to 7 until you have updated the startup scripts for all managed servers that you have discovered.

## Adding Existing Oracle Communications Applications Using Monitoring Properties

You can manually add existing installations of supported versions of Oracle Communications applications or components as managed non-host targets by specifying the target host type and monitoring properties.

The plug-in supports the following Oracle Communications application target types for property monitoring:

- ASAP Target
- NCC SLC Target
- NCC SMP Target
- NCC VWS Target
- OSM Target
- Oracle BRM Account Sync Tool
- Oracle BRM Batchcontroller Process
- Oracle BRM Connection Manager
- Oracle BRM Connection Manager Master Process
- Oracle BRM Connection Manager Proxy
- Oracle BRM DM AQ
- Oracle BRM DM Invoice
- Oracle BRM DM LDAP
- Oracle BRM DM Prov Telco
- Oracle BRM DM-EAI
- Oracle BRM DM-EMAIL
- Oracle BRM DM-FUSA
- Oracle BRM DM-TAXWARE
- Oracle BRM DM-VERTEX
- Oracle BRM DMO
- Oracle BRM DMTT
- Oracle BRM Diameter Gateway
- Oracle BRM EAI JS Component
- Oracle BRM Formatter Process
- Oracle BRM Pipeline
- Oracle BRM REL
- Oracle BRM RTP
- Oracle BRM SNMP Process
- Oracle BRM UEL
- Oracle ECE Cluster
- Oracle ECE Node
- UIM Target

To manually add existing Oracle Communications applications or processes:

1. Add the server host of each application or process instance as a managed host and install the Management Agent. See "Adding Host Targets Manually and Installing the Management Agent" for more information.

2. Deploy the Application Management Pack for Oracle Communications plug-in to the Management Agent. See "Deploying the Application Management Pack for Oracle Communications Plug-In" for more information.
3. Log in to the Enterprise Manager Cloud Control administration console.
4. From the **Setup** menu, select **Add Target**, and then **Add Targets Manually**.
5. Select **Add Targets by Specifying Target Monitoring Properties.**
6. From **Target Types**, select the Oracle Communications application or process.
7. Click the magnifying glass to search for the monitoring agent running on the host where the Oracle Communications application or process is running. The **Search and Select: Targets** window appears.
8. Select the Management Agent running on the Oracle Communications application or process host.
9. Click **Select**.
10. Click **Add Manually...**.
11. Provide the required parameters for the target type. Obtain these values from the installed Oracle Communications application or component environment. See the documentation for the application or component for more information.
12. Click **OK** to add the new target.
13. Confirm that the new target is now visible in the Enterprise Manager Cloud Control administration console.

# Preparing New Hosts for Application Provisioning

This section describes the steps needed to prepare a new host for Oracle Communications application provisioning. You must prepare a host for an Oracle Communications application before initiating provisioning from Enterprise Manager Cloud Control. This involves the following steps:

- Ensuring Proper Application System Requirements
- Installing Required Software
- Adding a Host to Enterprise Manager Cloud Control

## Ensuring Proper Application System Requirements

The managed host must meet the application's hardware and software requirements. See the product's installation guide for more information.

Hardware and Software requirements vary depending on the type of installation you are performing. For example, development and testing systems require lower minimum technical requirements compared to production systems. However, all managed hosts must meet the minimum requirements.

## Installing Required Software

Most Oracle Communications applications require foundational software, such Oracle Enterprise Database or Oracle WebLogic Server, before installation. Required software can exist on the same host you are provisioning an Oracle Communications application on or on a remote host. Consult the installation guides for these

requirements. Foundational software configuration details, such as host names, credentials, and port numbers may be required for provisioning.

You can install foundational software on any host, then use discovery to promote the hosts to managed target status. This enables monitoring components such as Enterprise Database and WebLogic Server domains in Enterprise Manager Cloud Control along side Oracle Communications applications.

### Adding a Host to Enterprise Manager Cloud Control

Add the new host to Enterprise Manager Cloud Control and install a Management Agent on the host either manually or with discovery. See "Adding Oracle Communications Targets" for more information.

## Downloading Oracle Communications Application Installers

You must download supported versions of Oracle Communications applications before installing them on managed hosts in Enterprise Manager Cloud Control. The Communications Suite Installation Procedure copies the installers onto the target host during the installation process.

Obtain the installer packages for supported products from the Oracle Software Delivery Cloud at:

`https://edelivery.oracle.com`

See "Supported Applications" for a list of supported Oracle Communications applications and versions.

Place the installers in a shared network location accessible by the Enterprise Manager Cloud Control host and the managed targets on which Oracle Communications applications will be installed.

For BRM, you must upload the installers into the **BRMComponents** folder in the Software Library. See "Creating the BRM Source Components" for more information on uploading BRM components.

> **WARNING: Do not change names of the BRM installation packages. The provisioning procedure does not support custom file names for the installation packages.**

See "Provisioning and Upgrading Applications" for more information on the installation procedure.

# 4

# Managing Communications Applications with Enterprise Manager Cloud Control

This chapter describes how to manage Oracle Communications applications using Oracle Application Management Pack for Oracle Communications with Oracle Enterprise Manager Cloud Control.

## Overview

Application Management Pack for Oracle Communications provides management capabilities for the following Oracle Communications applications:

- Oracle Communications Billing and Revenue Management (BRM)
- Oracle Communications Elastic Charging Engine (ECE)
- Oracle Communications Pricing Design Center (PDC)
- Oracle Communications Pipeline Configuration Center (PCC)
- Oracle Communications Network Charging and Control (NCC)
- Oracle Communications Order and Service Management (OSM)
- Oracle Communications Unified Inventory Management (UIM)
- Oracle Communications ASAP
- Oracle Application Integration Architecture (Oracle AIA) Oracle Communications Pre-Built Integrations

See "Supported Applications" for supported Oracle Communications application versions.

## Supported Actions

You perform a variety of actions in Enterprise Manager Cloud Control, including discovering, provisioning, patching, upgrading, and monitoring applications.

Actions supported vary by application. Not all actions are supported by all applications. Table 4–1 lists supported actions for each application.

See "Supported Applications" for information about supported Oracle Communications applications and versions.

*Table 4–1 Supported Application Management Pack for Communications Actions*

| Action | BRM | ECE | PDC | PCC | NCC | OSM | UIM | ASAP | Oracle AIA |
|---|---|---|---|---|---|---|---|---|---|
| Discover | Yes | Yes | No | Yes | Yes | Yes | Yes | Yes | Yes |
| Provision | Yes | No | Yes | Yes | No | Yes | Yes | Yes | No |
| Start and Stop Processes | Yes | No | No | No | No | No | No | No | No |
| Patch | Yes | No | No | No | No | No | No | No | No |
| Upgrade | No | No | Yes | No | No | No | No | No | No |
| Monitor | Yes | Yes | No | No | Yes | Yes | Yes | Yes | Yes |
| View/Edit Configuration | Yes | No | No | No | No | No | No | No | No |
| Manage Alerts | Yes | Yes | Yes | No | No | Yes | Yes | Yes | Yes |
| View Topology | Yes | Yes | No | No | No | Yes | Yes | Yes | Yes |
| Manage Compliance | No | No | No | No | No | Yes | No | No | No |

## Discovering Applications

Discovery enables adding already installed Oracle Communications applications in your environment to Enterprise Manager Cloud Control. Application Management Pack for Oracle Communications provides automatic and guided discovery modules for supported Oracle Communications applications and components running on managed host targets. After discovery, you promote new Oracle Communications targets to a managed status.

See "Adding Oracle Communications Targets" for information about adding existing Oracle Communications targets to your Enterprise Manager Cloud Control instance.

## Provisioning and Upgrading Applications

You provision and upgrade supported Oracle Communications applications, components and suite configurations using the Communications Suite Installation Procedure in Enterprise Manager Cloud Control.

The procedure requires an understanding of the installation parameters of each application and assumes that all prerequisites for installing those applications are met. See "Preparing New Hosts for Application Provisioning" for more information about ensuring application hosts are ready. See "About Providing Valid Installation Parameter Values" for information about required values for installation parameters.

You can provision one or more applications using a single Communications Suite Installation Procedure execution. For example, you can provision Oracle Communications applications that form the Order to Cash solution at the same time.

The Communications Suite Installation Procedure supports:

- Provisioning application suites. See "About Provisioning Application Suites".
- Provisioning highly-available suites and clustered applications. See "About Provisioning Highly-Available Suites and Clustered Applications".
- Upgrading PDC. See "Upgrading PDC".
- Provisioning all supported applications. See "Provisioning Applications and Suites" and "Provisioning BRM".

The Communications Suite Installation Procedure requires that application and component hosts exist as managed host targets in your Enterprise Manager Cloud Control environment. See "Understanding Oracle Communications Targets" for information about adding new and existing hosts as managed targets.

**Note:** On Oracle Real Application Clusters (Oracle RAC) databases, the Communications Suite Installation Procedure supports provisioning BRM only.

## About Providing Valid Installation Parameter Values

The values that you provide for the installation parameters during the Oracle Communications Installation Procedure are required by the Oracle Communications application installer for the selected application. Typically, you enter these values during the installation interview process for the application you are installing.

You must use values that respect the validations performed by the application installer. For example, if a product does not allow a user name and password to be the same or requires special characters in the password, you must use values that meet those requirements.

The Communications Suite Installation procedure validates that you have provided values for all required fields, but it does not immediately validate the content of the values. You will not be notified that you have used invalid values until after the procedure fails.

See the specific Oracle Communications application product installation guides for information about the parameters and their required values.

## About Provisioning Application Suites

Oracle Communications application suites, such as the Order to Cash solution suite, provide cross-application functionality. Provision supported applications suites using the Communications Suite Installation Procedure.

You can provision the following application suites on both a single server meeting the minimum technical requirements for multi-application installation or across distributed high-availability hosts:

- Order to Cash suite:
  - OSM
  - UIM
  - ASAP
  - BRM
  - PDC
  - PCC
- OSS Service Fulfillment suite:
  - OSM
  - UIM
  - ASAP

You provision a suite in the same way as other targets, as described in "Provisioning Applications and Suites".

After provisioning applications suites, you must manually deploy solution cartridges. For information about deploying cartridges for the individual applications, see:

- *Oracle Communications Order and Service Management Cartridge Guide for Oracle Application Integration Architecture*
- *Oracle Communications Unified Inventory Management Installation Guide*
- *Oracle Communications ASAP Installation Guide*

## About Provisioning Highly-Available Suites and Clustered Applications

You can provision supported Oracle Communications applications in the following high-availability and cluster configurations:

- A highly-available OSS fulfillment suite
- A highly-available Order to Cash suite
- An OSM cluster with multiple nodes
- A UIM cluster with multiple nodes

You provision highly-available or clustered targets in the same way as other targets, as described in "Provisioning Applications and Suites".

By default, the Communications Suite Installation Procedure includes OSM and UIM clusters with two nodes. You can add more nodes using the **Configure** button as described in "Provisioning Applications and Suites".

## Upgrading PDC

Upgrading PDC involves the following steps:

1. Perform the following tasks as described in the discussion of pre-installation tasks for the PDC patch installation in *Oracle Communications Pricing Design Center Installation and System Administration Guide:*
   a. Shut down the current PDC instance.
   b. Back up your existing PDC installation.
   c. Install the recommended BRM version or patch.
   d. Install the recommended version of JRE/JDK.
   e. Upgrade WebLogic Server to the recommended version.
   f. Enable the SSL Port for the WebLogic Server domain and ensure that the domain's state is **Release Configuration**.
   g. Upgrade Oracle Application Development Runtime to the recommended version.
2. Set the path to the JAVA_HOME environment variable as described in "Setting the Java Home Path for PDC".
3. Provision PDC as described in "Provisioning PDC".

### Setting the Java Home Path for PDC

To set the Java home path for PDC:

1. Go to the *MW_Home*/**user_projects/domains/bin** directory, where *MW_Home* is the directory in which the Oracle Middleware components are installed.
2. Open the **setDomainEnv.sh** file in a text editor.
3. Search for the following line:

   ```
   JAVA_HOME="
   ```

4. Edit the value to match the absolute path to the directory where you installed the version of Java required by the version of PDC to which you are upgrading.

   For example:

   ```
   JAVA_HOME="/pinhome/pin136/opt/portal/7.5/ThirdPartyApps/jre/1.7.0"
   ```

5. Save and close the file.
6. Restart the administration server.

### Provisioning PDC

Provision PDC as described in "Provisioning Applications and Suites" and, when specifying the domain parameters under **ADMIN Configuration**, ensure that you select the **Do you want to upgrade PDC** option.

## Provisioning Applications and Suites

This section describes provisioning the following Oracle Communications application types:

- Order to Cash and OSS Fulfillment suites
- OSM single nodes and OSM clusters
- UIM single nodes and UIM clusters
- ASAP
- PCC
- PDC

See "Provisioning BRM" for information about provisioning BRM:

To provision an Oracle Communications application or suite:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Enterprise** menu, select **Provisioning and Patching**, and then **Procedure Library**.

   The Deployment Procedure Manager page appears.
3. In the **Select** column, select the **Communications Suite Installation Procedure** option.
4. Click **Launch**.

   The Communications Suite Provisioning page appears.
5. Under Choose Targets, click **Add** to select the types of Oracle Communications targets to provision.

   The System Types dialog box appears.
6. Select the check box for each type of system to provision.

You can provision multiple system types at a time, but you cannot provision multiple operations support system (OSS) system types unless they are included in a suite. For example, you can select a PCC target and an OSM target, but if you select an invalid combination, such as an OSM target and an ASAP target, an error is displayed when you click **OK** and you cannot proceed.

To provision multiple OSS system types included in a suite, select one of the OSS Fulfillment Suite or Order to Cash Suite options.

7. Click **OK**.

   The selected systems are added to the **Choose Targets** table, which displays each system's components.

   For applications that require an Oracle WebLogic Server installation, an **ADMIN** row is automatically added for specifying the WebLogic Server installation used for provisioning.

   For highly-available suites and application clusters, a **PROXY** row is automatically added for each OSM and UIM cluster.

8. (Optional) You can save your provisioning configuration as a custom system. This is useful when you plan to provision multiple instances of the same application on multiple targets or for backing up configurations for reuse at a later time.

   To save a provisioning procedure configuration as a custom system:

   a. Click **Save**.

      The Custom System Name dialog box appears.

   b. In the **Name** field, enter a name for the configuration.

   c. Click **OK**.

9. For targets that require an Oracle WebLogic Server domain, do the following:

   a. Select the **ADMIN** row.

   b. From the menu in the **Target Name** column, select the host of the administration server from which to provision the target.

      The table is updated with the **Free RAM**, **RAM**, **Free Storage** and **Storage** values for the selected host.

   c. In the Host Configurations region, under ADMIN Configuration, enter values for the required fields.

   d. (Optional) For PDC targets, to upgrade PDC, select the **Do you want to upgrade PDC** option.

10. For highly-available suites and cluster applications, do the following:

    - (Optional) To add more cluster nodes or proxies:

      a. Select a UIM or OSM cluster row.

      b. Click **Configure**.

      c. Select **Add Application** or **Add Proxy**.

         A row for the application or proxy is added to the table under the cluster.

    - Specify the port for the WebLogic Server proxy:

      a. Select the **PROXY** row.

      b. From the menu in the **Target Name** column, select the host for the proxy.

For highly-available and cluster environments intended for demonstrations and development, you can use the same host for the administration server, the proxy server, and the application.

The table is updated with the **Free RAM**, **RAM**, **Free Storage** and **Storage** values for the selected host.

c. In the Host Configurations region, in the **WebLogic Proxy Server Port** field, enter the port for the WebLogic Server proxy.

11. For PDC targets, do the following:

a. Select the **PDC BRM PACK** row.

b. In the Host Configurations region, under PDC BRM PACK Configuration, enter values for the required fields.

Selecting **Support Migration** is optional. The **Migration Username** and **Migration User Password** fields are required only if you select the **Support Migration** option.

c. (Optional) Select the **Support Migration** option and enter values for all of the **Migration** fields.

12. For each component in the Choose Targets table that you have not yet configured, do the following:

a. Select the component's row.

b. From the menu in the component's **Target Name** column, select the host on which to provision the component.

The table is updated with the **Free RAM**, **RAM**, **Free Storage** and **Storage** values for the selected target host.

---

**Note:** For OSS applications, the provisioning procedure uses the hosts that you select for the application rows as managed servers in the WebLogic Server domain. The procedure installs the applications from the administration server host, not the managed server hosts. As a result, the application home directories are located on the administration server host.

---

c. In the **Host Configurations** region, enter values for all required fields.

---

**Note:** For PDC targets, the **PDC Managed Server SSL Port** field is required. During installation, Secure Sockets Layer (SSL) is enabled by default for the WebLogic servers used by PDC. If you do not want to use SSL, you can disable it in the WebLogic Server Administration Console. See the WebLogic Server documentation for more information about using SSL.

---

13. Click **Next**.

14. Provide the preferred credentials for the target host. See "Setting Up Host Preferred Credentials" for more information.

15. Under **Schedule**, specify when the installation procedure should run.

16. Click **Next**.

17. Under **Review**, verify your provisioning configuration by checking the summary provided, and then click **Finish**.

    **Tip:** You can view the status of the provisioning process in the **Procedure Activity** tab. Click the procedure name in the **Run** column to view the procedure's status. To update the status, click **Refresh**. The Procedure Steps table displays all of the provisioning procedure steps and their corresponding statuses. View details about any step by selecting the option for that step in the Select column.

## Provisioning BRM

This section provides an overview of how to set up a new Oracle Communications BRM system and components using the Communications Suite Installation Procedure. Applications Management Pack for Oracle Communications provides two options for provisioning BRM:

- The **BRM Basic** option installs a limited set of components on a single target host. Use these systems for development or simple deployments of BRM. See "Provisioning a Basic BRM System" for a list of included components.
- The **BRM Advanced** option enables selecting specific components for installation on one or more hosts. Use this option when installing production systems or testing systems with distributed component architecture.

Using the procedure requires an understanding of BRM architecture and installation. See *Oracle Communications Billing and Revenue Management Installation Guide* for more information about installation details, including installation parameters.

To set up a new BRM instance:

1. Download the required BRM InstallShield MultiPlatform (ISMP) packages from the Oracle Software Delivery Cloud to a location accessible from the Management Server. See "Downloading the BRM Installers" for more information.
2. Create the BRM source components in the Enterprise Manager Cloud Control Software Library. See "Creating the BRM Source Components" for more information.
3. Create the Oracle Enterprise Database used by BRM. See "Specifying the BRM Database" for more information.
4. Provision either a single instance BRM system or individual components on one or more host targets. See "Provisioning a Basic BRM System" and "Provisioning BRM Components" for more information.

### Downloading the BRM Installers

Download the BRM ISMP installer packages from the Oracle Software Delivery Cloud at:

`http://edelivery.oracle.com`

You must download all of the BRM ISMP installer packages when using the BRM Basic option.

Place the downloaded ISMP packages into a file share location accessible from your Enterprise Manager Cloud Control Management Server. The Communications Suite Installation Procedure requires either a local or remote path to the location where the packages are installed.

In some cases, a single ISMP package provisions multiple BRM components. For example, the Portal Base package includes the Connection Manager (CM), Data Manager (DM) and BRM Applications. Table 4–2 contains a list of the ISMP packages and the included installable components in each package.

***Table 4–2 BRM ISMP Packages Descriptions and Base Components***

| BRM ISMP Package | Installable Components | Source Component Name Format | Base Component |
|---|---|---|---|
| AccountSynchTool | Account Synchronization CM<br>Account Synchronization DM | AccountSynchTool_ release_OS | oracle_brm_cm |
| BRM Base | Batch Controller<br>CM Proxy<br>CMMP<br>Connection Manager<br>Email Data Manager<br>Formatter<br>Invoice Data Manager<br>Oracle Data Manager<br>BRM Applications (Device Management, Load notification event, Load price list, Pin A/R taxes, Pin balance transfer, Pin billed, Pin bill handler, Pin bulk adjust, Pin export price, Pin invoice, Pin monitor, Pin ood handler, Pin rate change, Pin remit, Pin rerate, Pin subscription, Pin trial bill, Pin unlock service Invoicing, Misc, Pin_cfg_ bpdump, SOX_Unlock, Subscription, Testnap, UEL, GL_Export, Diagnostics, Infranet Manager CLI, Infranet Manager, Node Manager, Export_price, Credit_ Control Billing, Account Dump Utility, Development_Files) | PortalBase_release_ OS | NA |
| BRM_Services_ Framework_Mgr_ AAA | BRM Services Framework Manager AAA | BRMServicesFramew orkMgrAAA_release_ OS | oracle_brm_cm |
| BRM_Services_ Framework_Mgr | BRM Services Framework Manager | BRM_Services_ Framework_Mgr_ release_OS | oracle_brm_cm |
| CIBERRoaming | CIBER Roaming | CIBERRoaming_ release_OS | oracle_brm_pipeline |
| CollectionsMgr | Collections Manager | CollectionsMgr_ release_OS | oracle_brm_cm |
| ContentMgr | Content Manager | ContentMgr_release_ OS | oracle_brm_cm |
| EAI_ FrameworkMgr | EAI Connection Manager (CM) module<br>EAI Data Manager<br>Payload Generator External Module | EAIFrameworkMgr_ release_OS | oracle_brm_cm |
| EmailMgr | Email Manager | EmailMgr_release_ OS | oracle_brm_cm |
| GPRS_AAA_Mgr | GPRS AAA Manager | GPRSAAAMgr_ release_OS | oracle_brm_cm |

***Table 4–2 (Cont.) BRM ISMP Packages Descriptions and Base Components***

| BRM ISMP Package | Installable Components | Source Component Name Format | Base Component |
|---|---|---|---|
| GPRS_Mgr_30 | GPRS Manager 3.0 | GPRSMgr_release_OS | oracle_brm_cm |
| GSM_AAA_Mgr | GSM AAA Manager | GSMAAAMgr_release_OS | oracle_brm_cm |
| GSM_Mgr | GSM Manager | GSM_Mgr_release_OS | oracle_brm_cm |
| IPAddressMgr | IP Address Manager | IPAddressMgr_release_OS | oracle_brm_cm |
| Interconnect | Interconnect Manager | Interconnect_release_OS | oracle_brm_pipeline |
| InventoryMgr | Inventory Manager | InventoryMgr_release_OS | oracle_brm_cm |
| LDAPMgr | LDAP Manager<br>LDAP Manager has a single component, LDAPMgr. The pin_channel_export component gets deployed as part of it. | LDAPMgr_release_OS | NA |
| MultiDBMgr | MultiDB Manager | MultiDBMgr_release_OS | oracle_brm_cm |
| NumberMgr | Number Manager | NumberMgr_release_OS | oracle_brm_cm |
| PaymentechMgr | Paymentech Manager | PaymentechMgr_release_OS | NA |
| Pipeline | BRE<br>Real-Time Pipeline | Pipeline_release_OS | NA |
| Pipeline_ConfMgr | Pipeline Configuration Manager | PipelineConfMgr_release_OS | oracle_brm_pipeline |
| RadiusMgr | Radius Manager | RadiusMgr_release_OS | oracle_brm_cm |
| RatedEventLoader | Rated Event Loader, Event Extraction Manager | REL_release_OS | NA |
| ResourceResMgr | Resource Reservation Manager | ResourceResMgr_release_OS | oracle_brm_cm |
| RevAssuranceMgr | Revenue Assurance Manager | RevAssuranceMgr_release_OS | oracle_brm_cm |
| SIMMgr | SIM Manager | SIMMgr_release_OS | oracle_brm_cm |
| SuspenseMgr | Suspense Manager | SuspenseMgr_release_OS | oracle_brm_cm |
| TAPRoamingmanager | TAP Roaming Manager | TAPRoamingMgr_release_OS | oracle_brm_pipeline |
| ThirdParty | ThirdParty Applications | ThirdParty_release_OS | NA |
| Timos | Timos Data Manager | Timos_release_OS | NA |
| VertexMgr | Vertex Manager | VertexMgr_release_OS | NA |

*Table 4–2 (Cont.) BRM ISMP Packages Descriptions and Base Components*

| BRM ISMP Package | Installable Components | Source Component Name Format | Base Component |
|---|---|---|---|
| VertexQuantumMgr | Vertex Quantum Manager | VertexQuantumMgr_ release_OS | NA |
| VoucherMgr | Voucher Manager | VoucherMgr_release_ OS | oracle_brm_cm |
| WirelessSuite | GSM AAA Manager<br>GSM Manager<br>GPRS AAA Manager<br>GPRS Manager<br>Number Manager<br>RRF Manager<br>Services Framework Manager<br>Services Framework AAA Manager<br>SIM Manager<br>You cannot choose which features to install. They are all installed. | WirelessSuite_ release_OS | oracle_brm_cm |

## Creating the BRM Source Components

You must configure the ISMP packages as source components in the Enterprise Manager Cloud Control Software Library before running the provisioning procedure. If your environment uses custom applications, you must also create source components for the applications. Use the upload source components utility to upload the ISMP packages into the Software Library.

To add the BRM ISMP packages to the Software Library:

1. Confirm the **BRMComponents** folder exists in the Software Library. See "Creating the Oracle Communications Folders for BRM Installers" for more information.
2. Open a shell session to the host where your Enterprise Manager Cloud Control Management Server is installed.
3. Change directories to the following location:

   *EM_home*`/gc_inst/user_projects/domains/GCDomain/default_xml/platform/swlibUtil`

4. Open the **upload_src.xml** file for editing.
5. Edit the environment parameters in Table 4–3 for your environment.

*Table 4–3 upload_src.xml Environment Parameters*

| Parameter | Description |
|---|---|
| HOSTSTR | The Enterprise Manager Cloud Control fully qualified domain name. |
| SID | The database SID for the Enterprise Manager Cloud Control repository. |
| DB_USER | The database administrative user. For example, sysman. |
| DB_PW | The database administrator's password. |
| PATH | The relative path of the BRMComponents directory in the Software Library. |
| FILEPATH | The file path to the location where the ISMP installers are stored. This path must be accessible from the Management Server. |

6. Confirm that the listing of BRM components is consistent with the ISMP packages downloaded in your environment. The packages and names must match the operating system platform you are provisioning on. For example, the listing for the BRM Account Synch Tool installer uses the following format in the **upload_src.xml** file:

   - On Linux:

     ```
     <DISPLAY_NAME>BRM_AccountSynchTool_7.5.0_Linux</DISPLAY_NAME>
     <DESCRIPTION>AccountSynchTool_7.5.0_Linux</DESCRIPTION>
     <FILE_NAME>7.5.0_Accountsynchtool_linux_32_opt.bin</FILE_NAME>
     ```

   - On Solaris:

     ```
     <DISPLAY_NAME>BRM_AccountSynchTool_7.5.0_Solaris</DISPLAY_NAME>
     <DESCRIPTION>AccountSynchTool_7.5.0_Solaris</DESCRIPTION>
     <FILE_NAME>7.5.0_SMSSettlement_Reports_solaris_32_opt.bin</FILE_NAME>
     ```

7. Upload the source components configuration using the following command in the same directory:

   ```
   perl upload_src_comp.pl -loglevel 2 OMS_home
   ```

   where *OMS_home* is the path of your Management Server's home directory. The BRM components ISMP installers are uploaded to the Software Library.

Check the **upload_src_comp.log** file for errors if the procedure is unsuccessful. Increase the log level to a maximum of 3 when running the perl command if more detail is needed in the utility's log.

### Specifying the BRM Database

BRM requires an Oracle Enterprise Database. When provisioning either a BRM system or components you must choose whether to create a database instance or use and existing instance.

You must specify an existing database when using the BRM Basic option. See "Provisioning a Basic BRM System" for more information on provisioning a BRM system on a single host using an existing database.

Some BRM components, such as the Data Manager, Batch Rating Engine, and Real-time Pipeline, require connection to a BRM database to complete provisioning and to start the service. When provisioning one or more BRM components using the BRM Advanced option, you can specify whether to create a database or use an existing database. See "Provisioning BRM Components" for more information on specifying database information with component provisioning.

### Provisioning a Basic BRM System

Use the BRM Basic option in the Communications Suite Installation Procedure to provision a basic system onto a single host. The procedure installs the following BRM components:

- Portal_Base
- AccountSyncTool
- RatedEventLoader
- WebServicesMgr
- BRM_JCA_Adapter

- DM_AQ
- PaymenttechMgr
- EAI_FrameworkMgr
- CollectionsMgr
- ContentMgr
- WirelessSuite
- AccountMigrationMgr

To provision a BRM system on a single host:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Enterprise** menu, select **Provisioning and Patching**, and then **Procedure Library**.
3. In the **Deployment Procedure Manager**, select **Communications Suite Installation Procedure**.
4. Click **Launch**.
5. Under **Choose Targets**, click **Add**.
6. Select **BRM Basic**.
7. Click **OK**.

   A BRM Basic entry is added to the Choose Targets table, which displays the BRM component as a row.
8. (Optional) You can save your provisioning configuration as a custom system. This is useful when you plan to provision multiple instances of the same application on multiple targets or for backing up configurations for reuse at a later time.

   To save a provisioning procedure configuration as a custom system:

   a. Click **Save**.

      The Custom System Name dialog box appears.

   b. In the **Name** field, enter a name for the configuration.

   c. Click **OK**.
9. Select the **Target Name** text box from the **BRM** row.
10. Select a managed host target from the drop down list.

    The resource information for the target host appears. The Host Configurations area also displays the parameters required for BRM Basic provisioning.
11. Enter the path to the location where the BRM ISMP installers are located in the **BRM Installer Folder** field. Click **Browse** to use the Remote File Browser tool.
12. In **Host Configurations**, provide the parameters needed by the BRM installer. Typically, you enter these values during the installer interview process. Enterprise Manager Cloud Control does not immediately validate the values you provide. See *Oracle Communications Billing and Revenue Management Installation Guide* for more information on installation parameters.

    The BRM Basic option requires an existing database on which to install and configure the BRM instance. The procedure creates the specified database user based on the parameter values entered.

13. (Optional) Expand **Advanced** and edit the default port numbers for the BRM components.
14. For multischema environments, provide details for the additional BRM schemas:
    a. Select **Enable MultiDB**.
    b. From the **No Of Schemas** list, select the number of schemas to provision.
    c. Click **Go**.

       The Add Schemas dialog box appears with fields for the number of schemas that you selected from the **No Of Schemas** list.
    d. In the **Secondary Schema Details** area, provide the value for the required parameters for each additional schema.
    e. Click **Save**.
15. Click **Next**.

    The Credentials page appears.
16. Provide the preferred credentials for the target host. See "Setting Up Host Preferred Credentials" for more information.
17. Click **Next**.
18. Under **Schedule**, specify when the procedure should run.
19. Click **Next**.
20. Under **Review**, verify your installation configuration by checking the summary, and then click **Finish**.

### Provisioning BRM Components

You provision individual BRM components using the Communications Suite Installation Procedure BRM Advanced option. For example, configure production system components requiring a distributed architecture across multiple target hosts using this functionality.

You must deploy the **ThirdParty** and **BRM Base** packages to a target in your installation before deploying optional components. Optional components require CM and DM configuration data when using the BRM Advanced provisioning procedure. Be sure to provide the proper CM and DM parameter values, including correct host names and port numbers, for the environment your optional managers are joining. The procedure cannot validate these parameters as they are specific to your environment.

See *Oracle Communications Billing and Revenue Management Installation Guide* for more information about installing a distributed architecture on multiple hosts.

To provision BRM components using the BRM Advanced option:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Enterprise** menu, select **Provisioning and Patching**, and then **Procedure Library**.
3. In the **Deployment Procedure Manager**, select **Communications Suite Installation Procedure**.
4. Click **Launch**.
5. Under **Choose Targets**, click **Add**.
6. Select **BRM Advanced**.

7. Click **OK**.

   A BRM Advanced row is added to the **Choose Targets** table, which displays the component as a row.

8. (Optional) You can save your provisioning configuration as a custom system. This is useful when you plan to provision multiple instances of the same application on multiple targets or for backing up configurations for reuse at a later time.

   To save a provisioning procedure configuration as a custom system:

   a. Click **Save**.

      The Custom System Name dialog box appears.

   b. In the **Name** field, enter a name for the configuration.

   c. Click **OK**.

9. Select the row for the added component and click **Configure**.

   The **Search and Select: Entities** window containing a list of BRM ISMP installer packages.

10. Select the BRM packages containing the components to provision. You can select more than one component to provision for the procedure by holding the control key.

11. Click **Select**.

    An entry for the selected installer is added to the list of systems on the Choose Targets page.

12. Select the newly added installer row in the list.

    The **BRM Components** list appears. This list contains the BRM components included in the installers selected.

13. Select the BRM components to provision.

14. Click **Add**.

    A row for the BRM components is added to the list of systems on the Choose Targets page.

15. Click in the **Target Name** field of the newly added components and select a target from the drop down list.

    The component's required **Host Configuration** parameters appear.

16. In **Host Configurations** - *target_name*, provide the parameters needed by the BRM installer for the selected component. Typically, you enter these values during the installer interview process. Enterprise Manager Cloud Control does not immediately validate the values you provide.

    The BRM Advanced option enables specifying whether to use an existing BRM database or to initialize a new database instance for use with provisioning. Set the database usage and partitioning behavior using the parameters in Table 4–4.

    The procedure uses the values specified for the **pin_setup.values** file used during BRM configuration. For information about **pin_setup.values**, see the chapter about installing BRM in *Oracle Communications Billing and Revenue Management Installation Guide*.

    When adding components to an existing BRM system, you must provide parameters for the database already in use and ensure that the procedure is not set

to drop existing tables. By default, the options to initialize the database and drop all BRM tables is set to **YES**.

***Table 4–4 Component Provisioning Database Parameters***

| Parameter | Description | Default Value |
|---|---|---|
| SetupInitDb | Specifies whether to initialize the BRM databases. | YES |
| SetupCreatePartition | Specify whether to add partitions to your event tables.<br>Enter Yes to have the installer add 12 monthly partitions, a historic partition, and a last partition to your event tables.<br>Enter No if you want the installer to add only a historic partition and a last partition to the tables. You can use this partitioning layout for a simple test or demonstration system. For a production system, however, you must add purgeable partitions after installation is complete and before the system generates events.<br>This sets the $CREATE_PARTITIONS parameter in the pin_setup.values file to Yes.<br>This prompt is displayed only if you enter Yes to Partition event tables. | YES |
| EnablePartition | Specify whether you want to enable partitioning.<br>To partition any tables, you need Oracle Partitioning. If you select Yes but do not have Oracle Partitioning installed, the BRM setup program fails when it tries to create partitions.<br>This sets the $ENABLE_PARTITION parameter to Yes in the pin_setup.values file.<br>Important<br>If you select No and then change your mind after you've installed BRM, you will have to upgrade your BRM database from a nonpartitioned to a partitioned version before you can partition your tables.<br>If you plan to use Rated Event Loader to load prerated events, you must partition your event tables.<br>If you select Yes, you must configure pin_setup to set up any non-event partitions. Your event tables will be partitioned automatically. | YES |
| CLASSES_TO_BE_PARTITIONED | Assign a list of classes that you want to partition.<br>You cannot partition classes after you run the **pin_setup** utility | NA |
| SetupDropAllTables | Enter whether you want to drop the database tables.<br>If you select **YES**, the installer drops all existing tables on your system. This results in irrecoverable loss of data. Do not use this unless you have backed up all of your existing data.<br>If you select **NO**, the installer uses your existing BRM tables.<br>In test systems, select **YES** to reinitialize the database. | YES |
| CreateDatabaseTables | Enter whether you want the installer to create default BRM tablespaces for you.<br>Enter No to create custom tablespaces manually. You must create your tablespaces before you run the pin_setup script. | YES |

17. (Optional) Expand **Advanced** to specify the component's configuration parameters used in the BRM **pin.conf** file.
18. Click **Next**.

    The Credentials page appears.

19. Provide the preferred credentials for the target host. See "Setting Up Host Preferred Credentials" for more information.
20. Click **Next**.
21. Under **Schedule**, specify when the procedure should run.
22. Click **Next**.
23. Under **Review**, verify your installation configuration by checking the summary, and then click **Finish**.

    **Tip:** You can view the status of the provisioning process in the **Procedure Activity** tab. Click the procedure name in the **Run** column to view the procedure's status. To update the status, click **Refresh**. The **Status Detail** displays all of the provisioning procedure steps and their corresponding statuses. View any step's status by clicking on the link in the **Status** column.

24. Rediscover the BRM target as described in "Rediscovering BRM Targets Using Guided Discovery".

# Starting and Stopping Application Processes

You can start and stop supported Oracle Communications application processes managed as targets using the Enterprise Manager Cloud Control administration console. See the following sections for information on controlling application processes:

- Starting and Stopping BRM Processes
- Starting and Stopping Domains Hosting Oracle Communications Applications

## Starting and Stopping BRM Processes

You can start, stop, and restart BRM application processes on BRM base targets using the Enterprise Manager Cloud Control administration console. You can control single processes or all processes running on a managed host.

When starting or stopping all processes, only the BRM base components included in the **pin_ctl.conf** file will be started or stopped. You cannot start or stop all processes for BRM pipeline components.

See the discussion of customizing the **pin_ctl** utility environment variables in *Oracle Communications Billing and Revenue Management System Administrator's Guide* for more information about specifying components in the **pin_ctl.conf** file.

To start and stop BRM processes:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Click **Targets**, and then **Communications Applications**.

   A table of managed BRM systems appears.
3. To stop or start either a one or more BRM processes on a managed target:
   a. Click the top-level **BRM**_*target_name* link.

      The home page for the BRM target appears.
   b. Click either **STOP ALL** or **START ALL**.

c. (Optional) Monitor the status of the processes under **Status**.

4. To restart one or more BRM processes on a managed target:
   a. Expand the top-level **BRM**_*target_name* where the process is running.
   b. Click the process link to control.

      The overview page for the selected process appears.
   c. Click **ReStart**.
   d. (Optional) Monitor the status of the process under **Status**.

### Starting and Stopping Domains Hosting Oracle Communications Applications

You can use Enterprise Manager Cloud Control to start and shutdown managed Oracle WebLogic Server domains hosting Oracle Communications applications. For example, you can start a WebLogic Server domain hosting OSM or PDC.

To start and stop WebLogic Server domains:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Targets** menu, select **Middleware**.

   The managed **Middleware** targets list appears.
3. Click the name of the domain to be controlled.

   The selected middleware target's home page appears.
4. Under the target's name, from the system type menu, select **Control**.
5. Click **Start Up** or **Shutdown** for the desired operation.

   The Credentials page appears.
6. Specify the required credential parameters.
7. Click OK.
8. Go to the middleware target's home page and confirm that the domain has either started up or shutdown.

## Patching Applications

You can patch BRM installations using the **BRM Patching Procedure**. The procedure uses Enterprise Manager Cloud Control integration with Oracle Support for searching and downloading patches. The procedure then performs patch installation on managed BRM targets.

The BRM Patching Procedure does not support installing password protected patches. Only generally available patches from My Oracle Support are supported.

Install password protected patches and patches unavailable from within Enterprise Manager Cloud Control using the offline patching process. For more information about performing offline patch installation, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

You can patch a single BRM target at a time using the **BRM Patching Procedure**. To patch multiple targets, run the procedure for each target individually.

Patching BRM involves the following tasks:

1. Patching BRM

2. Monitoring BRM Patching Status
3. BRM Post-Patch Tasks
4. Viewing Applied BRM CM and Pipeline Patches

## Patching BRM

To patch managed BRM targets:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Ensure that the Management Agent for the target you intend to patch is up and running.

   For information about verifying Management Agent status, see the discussion of controlling and configuring Management Agents in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
3. Click **Enterprise**, then **Provisioning and Patching**, and then **Procedure Library**.
4. In the **Deployment Procedure Manager**, select **BRM Patching Procedure**.
5. Click **Launch**.
6. Under **Choose Targets and Patches**, click **Add**.

   The **Search and Select: Targets** window appears.
7. Specify the target information:
   - In the **Target Type** field, enter the target type.
   - In the **Target Name** field, enter the name of the target.
   - In the **Host** field, enter the host name.
8. Click **Search**.
9. Select the BRM target to patch.
10. Click **Select**.

    The Choose Targets and Patches page appears. The BRM component to be patched is now listed.
11. In the target's row, click **Add Patch**.

    The **Choose BRM Patches** window appears.
12. In the Search Platforms pull down menu, specify search criteria for the patch by doing one of the following:
    - To search for a specific patch, specify the patch ID in the **Search Patches** field and specify the platform in the **Search Platforms** list.
    - To search for all patches for a BRM release, specify a release value in the **Search Releases** field.
13. Click **Search Patches**.

    A list of patches meeting the search criteria appears.
14. If needed, click the readme link for detailed patch information from Oracle Support.
15. Select the correct patches to apply and click **Add Patches**.

    The Choose Targets and Patches page appears.

16. Under **Target Configuration**, provide the information required about your BRM target. Typically, this information includes the location of your BRM installation and database credentials.
17. Click **Next**.

    The Credentials page appears.
18. Provide the preferred credentials for the target host. See "Setting Up Host Preferred Credentials" for more information.
19. Click **Next**.
20. Under **Schedule**, specify when the procedure should run.
21. Click **Next**.
22. Under **Review**, verify your installation configuration by checking the summary, and then click **Finish**.
23. (Optional) Monitor the status of the patching process as described in "Monitoring BRM Patching Status".
24. Perform post-patch tasks as described in "BRM Post-Patch Tasks".

## Monitoring BRM Patching Status

To monitor the status of the patching procedure:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Enterprise** menu, select **Patching and Provisioning**, and then **Procedure Activity**.
3. In the **Run** column, click the name of the BRM patching procedure for which you want to monitor status.

   The Procedure Steps table for the selected BRM patching procedure appears.
4. In the **Name** column, expand the BRM Patching Phase and host name entries.

   All of the steps for the BRM patching procedure appear.
5. In the **Status** column, review the status of the steps.
6. In the **Select** column, select any step for which you want to view more details.
7. Click **Refresh**.

   The status of all steps is updated.
8. If any steps fail, review the logs, resolve the issue, and try again.

   For example, if the **Automate Post Patch Steps PortalBase** step fails and the Connection Manager target is down:

   a. In the *BRM_home*/**var/cm.pinlog** file, search for the following line:

      ```
      fm_collections_config_scenario_cache cache not specified in pin.conf
      ```

   b. If the line appears, open the Connection Manager configuration file (*BRM_home*/**sys/cm/pin.conf**).

   c. Add the following line anywhere in the file:

      ```
      - cm_cache fm_collections_config_scenario_cache number_of_entries, cache_size, hash_size
      ```

where *number_of_entries*, *cache_size*, and *hash_size* are appropriate numbers for your system. For example:

```
- cm_cache fm_collections_config_scenario_cache 256, 40960, 54
```

**d.** Save and close the file.

**e.** Retry the patching procedure.

## BRM Post-Patch Tasks

After patching BRM, perform the following tasks:

1. Verify the patch log files for any errors. By default, the patch log files are located in the following directory:

   ```
   BRM_home/staging/patching/
   ```

   Where *BRM_home* is the directory where BRM is installed.

2. Verify that the **testnap** utility works. See *Oracle Communications Billing and Revenue Management Developer's Guide* for information about using **testnap**.

3. The patching process backs up your Pipeline and Real-Time Pipeline registry files, such as **wireless.reg** and **wirelessRealtime.reg**, and creates new ones. For each registry file, merge any configuration changes that you made in the original files to the new registry files.

   For example:

   **a.** In the new Real-Time Pipeline registry file, search for the following section:

   ```
   RealtimePipeline
   {
      ModuleName = NET_EM
      Module
      {
         ThreadPool
         {
            Port =
   ```

   **b.** Edit the **Port** entry so that the value is the same as in the backup registry file. For example:

   ```
   ThreadPool
   {
      Port = 14579
   ```

   See the discussion of using registry files to configure Pipeline Manager in *Oracle Communications Billing and Revenue Management System Administrator's Guide* for more information about registry files.

4. Rediscover the BRM target as described in "Rediscovering BRM Targets Using Guided Discovery".

## Viewing Applied BRM CM and Pipeline Patches

To view the list of patches that have been applied to a BRM CM or pipeline target:

1. Log in to the Enterprise Manager Cloud Control administration console.

2. Navigate to the home page for the BRM or Pipeline target to which you applied the patch, as described in "Viewing Home Pages".

The **Patch Set Level** field in the **Summary** displays the component's patch level.

# Monitoring Oracle Communications Application Targets

You can monitor supported Oracle Communications application and component targets in Enterprise Manager Cloud Control. Monitoring targets enables you to maintain your Oracle Communications environment and manage incidents and alerts.

Application Management Pack for Oracle Communications provides extended metrics for Oracle Communications applications that augment standard monitoring data.

Once you have discovered and promoted your Oracle Communications targets, you can monitor a variety of metrics. You use configurable thresholds when configuring warning and critical event states notifications useful for alerting you to potential system problems.

The following monitoring procedures are supported:

- Viewing Home Pages
- Viewing Target Metrics
- Viewing Log Files
- Configuring Metric Monitoring Thresholds and Alerts
- Configuring Collection Schedules
- Adding Corrective Actions
- Monitoring Groups of Targets

See "About Conditions that Trigger Notifications" for information on the formatting of the included information in the application monitoring chapters.

## Viewing Home Pages

You can view home pages for applications, components, and suite level targets managed in Enterprise Manager Cloud Control. These summary pages provide an overview of the target, including information such as availability, metric alerts and other performance data.

Home pages are available for the following target types:

- ASAP targets
- BRM targets
- ECE targets
- Communications suite targets (Comms Suite target type)
- OSM node and system targets
- UIM targets
- NCC targets
- Oracle Communications Integration targets (Oracle AIA)

To view a home page:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Targets** menu, select **All Targets**.
3. In the Target Type tree, select the type of target you want to view.

4. In the list of targets, click the name of the target you want to view.

   The target's home page appears.

## Viewing Target Metrics

To view data from individual metrics for Oracle Communications application targets:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the home page for the target for which you want to view metrics, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Monitoring**, and then **All Metrics**.
4. In the left-hand tree control, expand the metric category and select the metric you want to view.

## Viewing Log Files

To view Oracle Communications application log files:

1. Log in to the Enterprise Manager Cloud Control administration.
2. Navigate to the home page for the target for which you want to view log files, as described in "Viewing Home Pages".
3. In the **Quick Links** region, click **View Log Files**.

## Configuring Metric Monitoring Thresholds and Alerts

Application Management Pack for Oracle Communications comes with default thresholds for critical metrics in supported applications. Enterprise Manager Cloud Control also includes default thresholds for host metrics including CPU and physical memory usage. You can define additional metrics needed for your environment.

To better suit the monitoring needs of your organization, you can edit the thresholds provided and define new thresholds. When defining thresholds, choose acceptable values to avoid unnecessary alerts.

You can establish thresholds that quickly provide important information by defining baselines reflecting how your system runs for a normal period.

To edit existing or configure new metrics and related thresholds for Oracle Communications targets:

1. Log in to the Enterprise Manager Cloud Control administration.
2. Navigate to the home page for the target for which you want to configure metrics and thresholds, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Monitoring**, and then **Metric and Collection Settings**.
4. Configure the monitoring thresholds as required for your environment by clicking the **Edit** pencil icon for a metric.
5. Edit the **Warning Threshold** and **Critical Threshold** fields.

   Click **Add** to create a monitored object for the selected metric.
6. Click **Continue.**
7. Click **OK** to save your changes.

For detailed information on configuring Enterprise Manager Cloud Control notification settings, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

## Configuring Collection Schedules

To configure collection schedules for collection items and metrics:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the home page for the target for which you want to configure collection schedules, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Monitoring**, and then **Metric and Collection Settings**.
4. Configure the **Collection Schedule** time interval by clicking on the currently set interval link for a listed metric.
5. Set the new **Frequency Type** and **Repeat Every** values, and then click **Continue**.
6. Click **OK** to save your changes.

## Adding Corrective Actions

Corrective actions let you specify automated responses to alerts. Corrective actions ensure that routine responses to alerts are automatically executed, ensuring problems are dealt with before they impact business operations. By default, Application Management Pack for Oracle Communications does not include any corrective actions set for alerts generated by Oracle Communications applications.

See the section on creating corrective actions in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for more information on configuring corrective actions.

To add corrective actions for warnings and critical alerts:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the home page for the target for which you want to configure collection schedules, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Monitoring**, and then **Metric and Collection Settings**.
4. Click the edit pencil icon for the metric you want to configure a corrective action for.
5. Under **Corrective Actions**, click **Add**.
6. Select a task from the pull down menu in the **Add Corrective Action** step.
7. Click **Continue**.
8. Define the corrective action and provide the necessary information.
9. Click **Continue**.

## Monitoring Groups of Targets

You can use Enterprise Manager Cloud Control generic system targets and dynamic groups for monitoring groups of targets in the administration console. For example:

- Create a generic system that logically groups a selection of managed targets best suited for your environment, such as:

  - Targets that comprise a collection of integrated products, as in an Oracle Rapid Service Design and Order Deliver or Rapid Offer Design and Order Delivery solution
  - Targets in a highly-available BRM environment with services across hosts used for different deployment models
- Create a dynamic group containing the same target type for monitoring groups of targets that perform the same function.

By default, Application Management Pack for Oracle Communications includes the following systems targets:

- BRM Target
- Comms Suite

See the discussion of dynamic groups in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for more information about using dynamic groups.

See the overview of relationships in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for more information about creating generic systems.

### Creating New Generic Systems

You can create new generic systems with the following methods:

- By selecting the **Enable Logical Grouping** option and creating a new system or adding targets to an existing system when discovering and promoting targets as described in "Discovering and Rediscovering Targets Using Guided Discovery" and "Promoting Discovered Targets".
- By creating the system and then adding targets to it. To create a new generic system and add targets to it:
  1. Log in to the Enterprise Manager Cloud Control administration console.
  2. From the **Setup** menu, select **Add Target**, and then **Generic System**.
  3. Create a new generic system as described in the overview of relationships in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

### Monitoring Systems

You can monitor the overall health of your system and access more details about incidents, jobs, and unavailable or incompliant targets. You can also access the topology view to see the system topology and relationships between targets in the system.

To monitor the default BRM and Comms Suite systems, or generic systems you have created:

1. Log in to the Enterprise Manager Cloud Control administration.
2. From the **Targets** menu, select **Systems**.
3. In the **Search** list, select **BRM Target**, **Comms Suite**, or **Generic System**.
4. Click the right arrow icon.
5. Select a system from the list.

   The home page for that system appears.

The home page for generic system targets organizes metrics into the regions described in Table 4–5.

*Table 4–5 Regions on the Generic System Home Page*

| Region | Description |
|---|---|
| General | Lists the user who created the system and whether privilege propagation is enabled in Enterprise Manager Cloud Control. |
| Overview of Incidents and Problems | Summarizes incidents and problems over the last 24 hours and the last 7 days. |
| Jobs Activity | Summarizes jobs started in the last 7 days. |
| Status | Summarizes the availability of the system overall and of the targets in the system. Lists the targets that have been down the most in the last 24 hours. |
| Compliance Summary | Summarizes any compliance evaluations, violations, and scores for the targets in the system. |
| Dependent Targets | Lists any targets dependent on the targets in the system. |

You can see a full list of metrics collected for a system target and you can monitor the data that an individual metric collects for the target. See "Viewing Target Metrics" for information about accessing the list of metrics.

## About Conditions that Trigger Notifications

Management Agents continuously collect metrics on the health and performance of your Oracle Communications applications and host targets and return the information to the Management Server. Enterprise Manager Cloud Control generates alerts and notifications when metric values exceed preset conditions notifying you of potential issues with your environment.

Application Management Pack for Communications includes default conditions with thresholds for metrics such as application process up/down status, CPU and memory usage by a process, and transaction latency. You can customize the conditions containing the metric thresholds using the Enterprise Manager Cloud Control administration console.

See "Configuring Metric Monitoring Thresholds and Alerts" for information on setting thresholds.

Table 4–6 describes each attribute in a condition.

*Table 4–6 Condition Attributes*

| Attribute | Description |
|---|---|
| Condition Name | The name of the condition. |
| Evaluation and Collection Frequency | The rate at which the metric is collected and evaluated to determine whether it has crossed its threshold. The evaluation frequency is the same as the collection frequency. |
| Upload Frequency | The rate at which the Management Agent moves data to the Management Repository. For example, upload every $n^{th}$ collection. The upload frequency for a metric comes from the Enterprise Manager default collection file for that target type. This column is present in the Metric Collection Summary table only when the Upload Frequency is different from the Collection Frequency. |

*Table 4–6 (Cont.) Condition Attributes*

| Attribute | Description |
|---|---|
| Operator | The comparison method Enterprise Manager Cloud Control uses to evaluate the metric value against the threshold values.<br>■ LE: Less than or equals<br>■ EQ: Equals<br>■ LT: Less than<br>■ GT: Greater than<br>■ NE: Not equal<br>■ CONTAINS:<br>■ OCCURENCES<br>■ MESSAGE<br>■ CLEAR_MESSAGE |
| Default Warning Threshold | Value that indicates whether a warning alert should be initiated. If the threshold is reached for the number of consecutive occurrences, a warning alert is triggered. |
| Default Critical Threshold | Value that indicates whether a critical alert should be initiated. If the threshold is reached for the number of consecutive occurrences, a warning alert is triggered |
| Consecutive Number of Occurrences Preceding Notification | Consecutive number of times a metric's value reaches either the warning threshold or critical threshold before a notification is sent. |
| Alert Text | Message indicating why the alert was generated. See the chapter on managing alerts in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for information on formatting alert text. |

See the overview of key default collection metadata elements and attributes in *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Reference* for more information about using and customizing collection item conditions in target definition files.

Table 4–7 provides an example of a metric attributes summary table. Collected metrics for each Oracle Communications application with default conditions are summarized in similar tables in the monitoring chapters. The table shows the attributes that trigger warning or critical notifications, and when configurable, the threshold values.

*Table 4–7 Sample Conditions Summary Table*

| Condition Name | Evaluation and Collection Frequency | Upload Frequency | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|---|---|
| CANCEL_ MAX_ LATENCY | 5 minutes | 5 minutes | GT | 10000000 ns | 12500000 ns | 1 | Bytes sent by the server are %value% |

See the following chapters for information about monitored metrics in specific Oracle Communications applications:

- Monitoring Billing and Revenue Management
- Monitoring Elastic Charging Engine
- Monitoring Network Charging and Control
- Monitoring Operations Support Systems
- About the Monitoring Home Page for Integrations

# Monitoring Host and Foundational Software Targets

Oracle Communications applications rely on host health and performance. Enterprise Manager Cloud Control provides the following functions used in monitoring hosts and foundational software:

- Monitoring Basic Target Collection Items and Metrics
- Monitoring Oracle Fusion Middleware Targets
- Monitoring Oracle Enterprise Database Targets

See "Monitoring Oracle Communications Application Targets" for information about monitoring supported Oracle Communications application targets.

See the chapter about using Incident Management in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for information about setting up notification channels and resolving incidents.

## Monitoring Basic Target Collection Items and Metrics

Enterprise Manager Cloud Control monitors basic collection item (non-metric) and metrics for all managed host targets. The Management Agent installed on a managed host provides system information including software and hardware configuration, status, health, performance, and storage.

See the chapter on enterprise monitoring in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for more information on monitoring, managing incidents, and notifications.

## Monitoring Oracle Fusion Middleware Targets

Enterprise Manager Cloud Control provides comprehensive monitoring of Fusion Middleware, Oracle Service-Oriented Architecture (SOA), and Coherence cluster targets. You use the monitoring capabilities to monitor the domains and clusters on which some Oracle Communications applications run.

See the chapters about managing Fusion Middleware, SOA, and Coherence in *Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide* for more information about discovering and monitoring these targets.

You must discover and promote SOA targets before discovering Oracle AIA targets. Discovering the SOA targets lets you resolve system faults in bulk for the AIA targets that you are monitoring. See "Viewing and Recovering from Faults" for more information.

## Monitoring Oracle Enterprise Database Targets

Enterprise Manager Cloud Control monitors and manages Oracle Enterprise and Exadata Databases used by Oracle Communications applications. For more information on monitoring databases, see the Enterprise Manager Cloud Control

Documentation database management and Exadata Database Machine documents available at:

http://docs.oracle.com/cd/E24628_01/nav/management.htm

# Configuring BRM

You can view, edit, and compare configurations for managed BRM targets including host systems and individual components. See the following sections for information on performing configuration tasks:

- Viewing BRM Configurations
- Editing BRM Configurations
- Comparing BRM Configurations

Enterprise Manager Cloud Control retains configuration changes and history as part of Configuration Management. See the chapter on managing configuration information in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for more information at:

http://docs.oracle.com/cd/E24628_01/em.121/e27046/config_mgmt.htm#EMLCM11614

## Viewing BRM Configurations

You view BRM system and component configurations using the Enterprise Manager Cloud Control administration console.

To access the configuration viewer:

1. Log in to the Enterprise Manager Cloud Control administration.
2. Navigate to the home page for the BRM target for which you want to view configurations, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Configuration**, and then **Last Collected**.

   The configuration viewer for the selected system appears.

Table 4–8 describes the configuration viewer tabs.

***Table 4–8 Configuration Viewer Tabs***

| Tab | Description |
|---|---|
| *System_Name* | Contains host information and configuration parameters of the BRM target including host and component version, user name, directories and port numbers. |
| System Structure | Shown for only managed system targets, contains an expandable and selectable listing of the system's installed and managed BRM managed targets. |
| Immediate Relationship | Displays the immediate relationships of the managed target to other selectable managed BRM targets. |
| Member Of | Lists selectable managed BRM target component's membership in managed system targets. |
| Uses | Lists selectable targets used by the managed BRM target. |
| Used By | Lists selectable targets using the managed BRM target. |

## Editing BRM Configurations

You can edit BRM configuration files with Enterprise Manager Cloud Control. See the chapter about using configuration files to connect and configure components in *Oracle Communications Billing and Revenue Management System Administrator's Guide* for information on configuration files and parameters.

Use the **Edit Configurations for BRM Targets** procedure for changing the configuration of a managed BRM component target. You can edit multiple BRM component configurations at a time.

To run the procedure:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the home page for the BRM target for which you want to edit configurations, as described in "Viewing Home Pages".
3. In the **Components Installed** region, click the link to the component you want to configure.

   The home page for the BRM component appears.
4. In the **Quick Links** region, click **Edit Configurations**.

   The **Edit Configurations for BRM Targets** procedure is launched.
5. Under **Choose BRM Targets**, click **Add**.

   The **Search and Select: Targets** window containing a list of managed BRM component targets appears.
6. Select the managed BRM targets to edit.
7. Click **Select**.

   The selected components are added to the **Choose BRM Targets** table, which displays the component as a row.
8. Select the row for the added component.

   The component's **Configuration** parameter in the **Configurations - Name Value Mode** appears. You edit in a text editor by setting the **Config Mode** value in the target row to **File**.
9. In **Component Configurations** - *mode*, provide the updated configuration parameters.

   **Note:** if you are editing the configuration of a Connection Manager Proxy, DM-EMAIL, or DM-FUSA target to which a patch has been applied, the value in the *target_type*.**qm_port** field will contain a dash (-). For example:

   ```
   dm_email.qm_port -1234
   ```

   Do not remove this dash when updating the port number.
10. Click **Next**.

    The Credentials page appears.
11. Provide the preferred credentials for the target host. See "Setting Up Host Preferred Credentials" for more information.

12. Click **Next**.
13. Under **Schedule**, specify when the procedure should run.
14. Click **Next**.
15. Under **Review**, verify your new configuration by checking the summary, and then click **Finish**.
16. Rediscover the BRM target as described in "Rediscovering BRM Targets Using Guided Discovery".

    **Tip:** You can view the status of the configuration process in the **Procedure Activity** tab. Click the procedure name in the **Run** column to view the procedure's status. To update the status, click **Refresh**. The **Status Detail** displays all of the configuration procedure steps and corresponding status. View any step's status by clicking on the link in the **Status** column.

## Comparing BRM Configurations

You can compare two or more managed BRM target configurations, as well has historical configurations for a single target, using the Enterprise Manager Cloud Control administration console. You can compare configurations of a single component type running on multiple systems for compliance or troubleshooting reasons.

The Enterprise Manager Cloud Control administration console provides multiple ways of running a configuration comparison. The following procedure uses the Communications Applications target page. For additional methods for searching for and comparing target configurations. see the chapter about enterprise configuration management in *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Guide*.

To compare two or more managed BRM target configurations:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the home page for the BRM target for which you want to compare configurations, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Configuration**, and then **Compare**.

   The **Compare Configurations** wizard launches with the first configuration already set in the first step, **Compare Configurations: First Configuration**.
4. Click **Next**.
5. In the **Compare Configurations: Comparison Configurations** screen, click **Add Configurations**.

   The **Search and Select Configurations** window appears.
6. Select either the **Latest Configuration** or **Saved Configuration** search option.
7. Ensure that the **Target Type** matches the type of the first configuration selected in step 5.
8. Provide a name in the **Target Name** field, if known.
9. Click **Search**.

   A list of managed targets meeting the search criteria appears.

10. Select the targets you want to compare.
11. Click **OK** to return to the **Compare Configurations: Comparison Configurations** screen.
12. Click **Next**.
13. Specify a comparison template and template settings in step 3 if you are comparing configurations against a template.

    See the chapter about enterprise configuration management in *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Guide* for information on creating and using configuration templates.
14. Click **Next**.
15. In the **Compare Configurations: Schedule and Notify** screen, specify when the procedure should run and any notification email addresses.
16. Click **Next**.
17. In the **Compare Configurations: Review and Submit** screen, review your new configuration by checking the summary.
18. Click **Submit**.

> **Tip:** You can view the status of the configuration process in the **Procedure Activity** tab. Click the procedure name in the **Run** column to view the procedure's status. To update the status, click **Refresh**. The **Status Detail** displays all of the configuration procedure steps and corresponding status. View any step's status by clicking on the link in the **Status** column.

## Viewing Topology

Application Management Pack for Oracle Communications provides topology views of Oracle Communications applications and components managed as systems in Enterprise Manager Cloud Control. The views supplement existing Enterprise Manager Cloud Control configuration and routing topology views for Oracle Fusion Middleware and Oracle Enterprise Database, providing graphical and relational diagrams of managed targets. The views are displayed in the Configuration Topology Viewer in Oracle Enterprise Manager Cloud Control.

The Configuration Topology Viewer shows you the relationships between different elements in the target's topology. Different elements appear for different target types. For example:

- The topology for an OSM node target shows relationships between elements for the node, the WebLogic Server domain (including servers, hosts, homes, and clusters), and the database elements, while the topology for an OSM system also shows relationships between the members of the system.
- The topology for an Oracle Communications Integration target shows relationships between elements for Oracle AIA, SOA, WebLogic Server, the Oracle AIA and SOA databases, and integrated applications such as OSM and BRM.
- The topology for a Comms Suite target shows relationships between elements for the OSM nodes, OSM systems, ASAP, UIM, and the suite.

**Note:** Database elements appear in a target's topology only if a Management Agent is installed on the database host.

For BRM targets deployed on Oracle RAC databases, you must manually associate the database with the target from the BRM target's home page. See "Associating Oracle RAC Database Targets with BRM Targets" for more information.

You can filter the elements that appear in the topology using the sidebar and the **View** list. The **View** list includes the following views:

- **Uses**: Shows the targets that the selected target depends on. If a target is having problems, this view can help you determine whether its problems have been caused by another target it depends on.
- **Used By**: Shows the targets that depend on the selected target. This view can help you determine how shutting down the selected target might affect other targets.
- **System Members**: Shows the members of the system (available only for targets that are systems, such as generic systems or OSM system targets).

The Configuration Topology Viewer also lets you view more information about the elements in the topology, including properties, metrics, and incidents.

## Using the Configuration Topology Viewer

You can use the Configuration Topology Viewer to view topology for systems, such as Comms Suite targets or generic systems that you have created, and individual applications, such as OSM node targets.

To view topology for systems or applications:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Do one of the following:
   - Access the Configuration Topology Viewer from the list of targets:
     a. From the **Targets** menu, select **All Targets**.
     b. From the Target Type tree, select the type of target for which you want to view the topology.
     c. From the list of targets, right click the target for which you want to view the topology.
     d. From the menu, select **Configuration**, and then **Topology**.
   - Access the Configuration Topology Viewer from the target home page:
     a. From the **Targets** menu, select **All Targets**.
     b. From the Target Type tree, select the type of target for which you want to view the topology.
     c. From the list of targets, right click the name of the target for which you want to view the topology.

        The target's home page appears.
     d. Under the target's name, from the target type menu, select **Configuration**, and then **Topology**.

The Configuration Topology Viewer appears for the selected target, displaying the target's relationships to other targets and components.

3. (Optional) To view summary information about a component in the target's topology, including the target type, host, and number of incidents:
   a. Hover your cursor over a component.

      A pop-up caption containing the target name appears.

   b. Hover your cursor over the arrows beside the target name.

      The pop-up caption expands with summary information about the target.

   c. (Optional) In the summary information pop-up caption, click any link to go to the related page. For example, click the target name to go to the target's home page, or click an incident icon to go to the Incident Manager.
4. (Optional) To view more detailed information about a component in the target's topology:
   a. Click the component.
   b. From the sidebar:
      – To view a summary of metrics for the component, expand **Metric History**.
      – To view information about the target, the host, incidents, jobs, and configuration compliance or changes, expand **Properties** and click any of the tabs.
   c. (Optional) Click any link to go to the related page. For example, click the target name to go to the target's home page or click an incident name to go to the Incident Manager.

See the overview of Configuration Topology Viewer in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for more information about using and interpreting topology.

See the chapters about managing Enterprise Database and Fusion Middleware in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for information about viewing topologies for these applications.

## Managing Compliance

Oracle Enterprise Manager Cloud Control provides a framework and features for evaluating how well your targets comply with default standards that Oracle provides or custom standards that you create. See *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for more information about the compliance framework.

Application Management Pack for Oracle Communications provides ready to use compliance standards for OSM node targets. See "Managing OSM Compliance" for more information.

# 5

# Monitoring Billing and Revenue Management

This chapter describes how to monitor the Oracle Communications Billing and Revenue Management (BRM) and BRM components using the home pages provided by Oracle Application Management Pack for Oracle Communications.

It also describes the BRM monitoring collection items and metrics provided by Oracle Application Management Pack for Oracle Communications.

## About Monitoring BRM

Application Management Pack for Oracle Communications enables monitoring BRM targets using Oracle Enterprise Manager Cloud Control. A Management Agent monitors targets for collection items and metrics and sends the data to the Management Server for presentation.

You can monitor BRM system targets and BRM component targets. Application Management Pack for Oracle Communications collects collection items and metrics for BRM systems and components, including real-time and batch rating pipeline components.

> **Note:** The BRM Number Manager and System Manager components do not support monitoring with Enterprise Manager Cloud Control.

You must install and deploy the Application Management Pack for Oracle Communications plug-in on both your Management Server and host agents before monitoring BRM targets.

See the following chapters for information about setting up Oracle Communications application monitoring with Enterprise Manager Cloud Control:

- Installing Application Management Pack for Oracle Communications
- Configuring Oracle Communications Targets
- Managing Communications Applications with Enterprise Manager Cloud Control

### About the Monitoring Home Page for BRM Systems

The home page for a BRM system target displays metrics data that you can use to monitor the health of your BRM system and identify problems. See "Viewing Home Pages" for information about accessing BRM home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Figure 5–1 shows the regions on the home page for a BRM system target.

***Figure 5–1 BRM System Target Home Page***

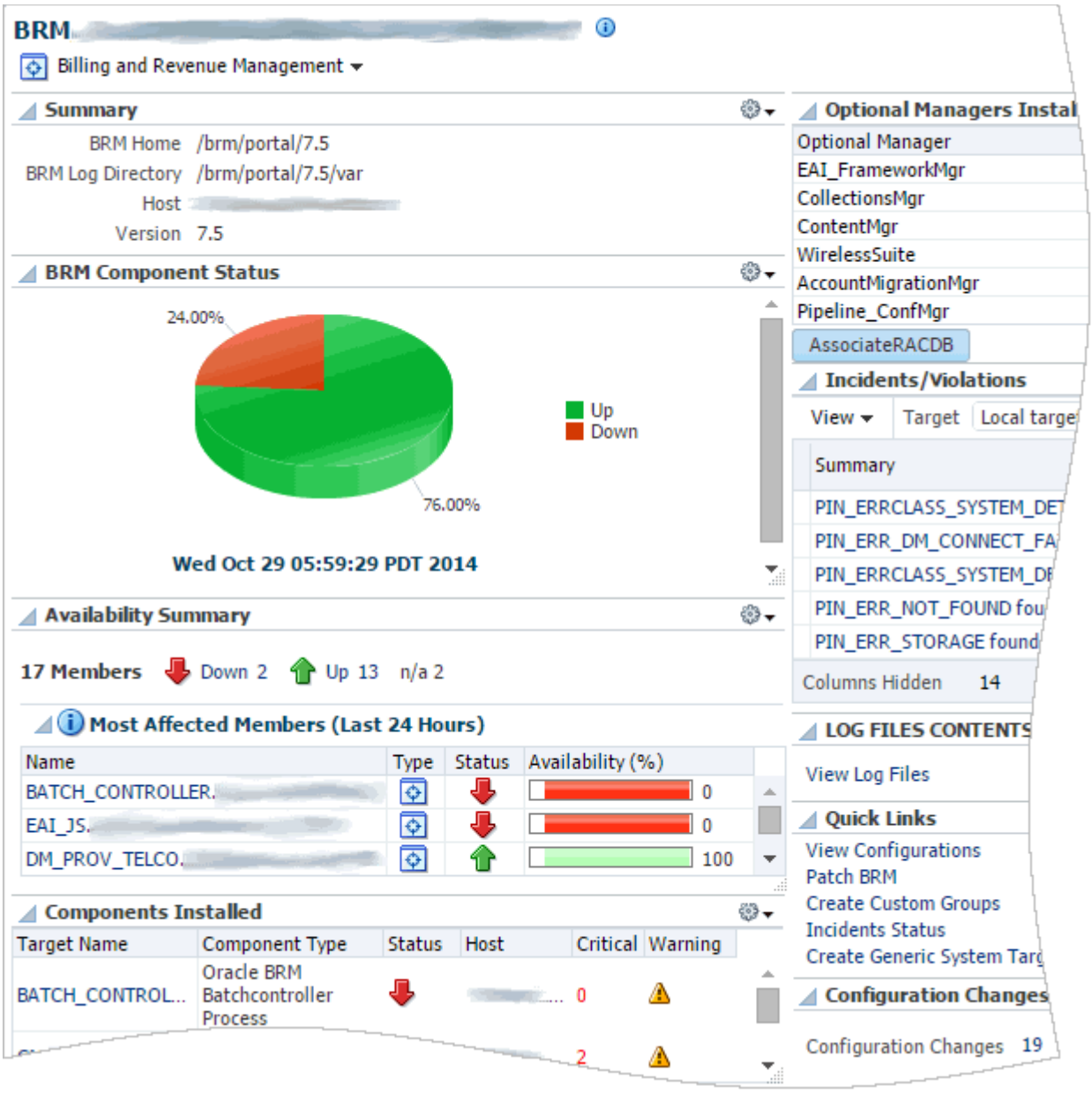



Table 5–1 describes the regions on the home page for BRM system targets.

***Table 5–1 Regions on the BRM Home Page***

| Region | Description |
|---|---|
| Summary | Displays the paths to the BRM home and log directories, the name of the host on which BRM is deployed, and the BRM version number. |
| BRM Component Status | Displays the percent of components that are up and down.<br>Use this region to determine if unavailable components are causing problems. |

*Table 5–1 (Cont.) Regions on the BRM Home Page*

| Region | Description |
|---|---|
| Availability Summary | Displays the number of components that are up and down and gives details about the components affected most in the last 24 hours.<br>Use this region to identify which components are causing problems and to access the home pages for those components. |
| Components Installed | Displays summary information about the components that are installed for the BRM system. Includes status, host name, and incident counts.<br>Use this region to get a high-level view of all the components in your BRM system, and identify those with high incident counts. |
| Optional Managers Installed | Displays the optional BRM managers installed for the target. |
| Incidents/Violations | Displays the number of critical, warning, and escalated incidents and violations, as well as a summary of each incident and links to view the incidents in Incident Manager.<br>Use this region to identify and resolve incidents. |
| Log Files Contents | Provides a link to the BRM log files. |
| Quick Links | Provides links to Enterprise Manager Cloud Control tasks related to the target, such as viewing configurations or patching BRM. |
| Configuration Changes | Displays the number of configuration changes and provides a link to the list of configuration changes for the target.<br>Use this region to identify configuration changes that could be causing problems. |

The BRM home page also includes an **AssociateRACDB** button. This button lets you associate an Oracle Real Application Clusters (Oracle RAC) database with the BRM target for viewing on the topology page. If the BRM target does not use an Oracle RAC database or you have already associated the Oracle RAC database with the target, nothing happens when you click the button. See "Associating Oracle RAC Database Targets with BRM Targets" for information about the tasks required to associate an Oracle RAC database with a BRM target.

## About the Monitoring Home Page for BRM Components

The home page for a BRM component target displays metrics data that you can use to monitor the health of the target and identify problems. See "Viewing Home Pages" for information about accessing BRM component home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Figure 5–2 shows the regions on the home page for a BRM component.

***Figure 5–2 BRM Component Target Home Page***

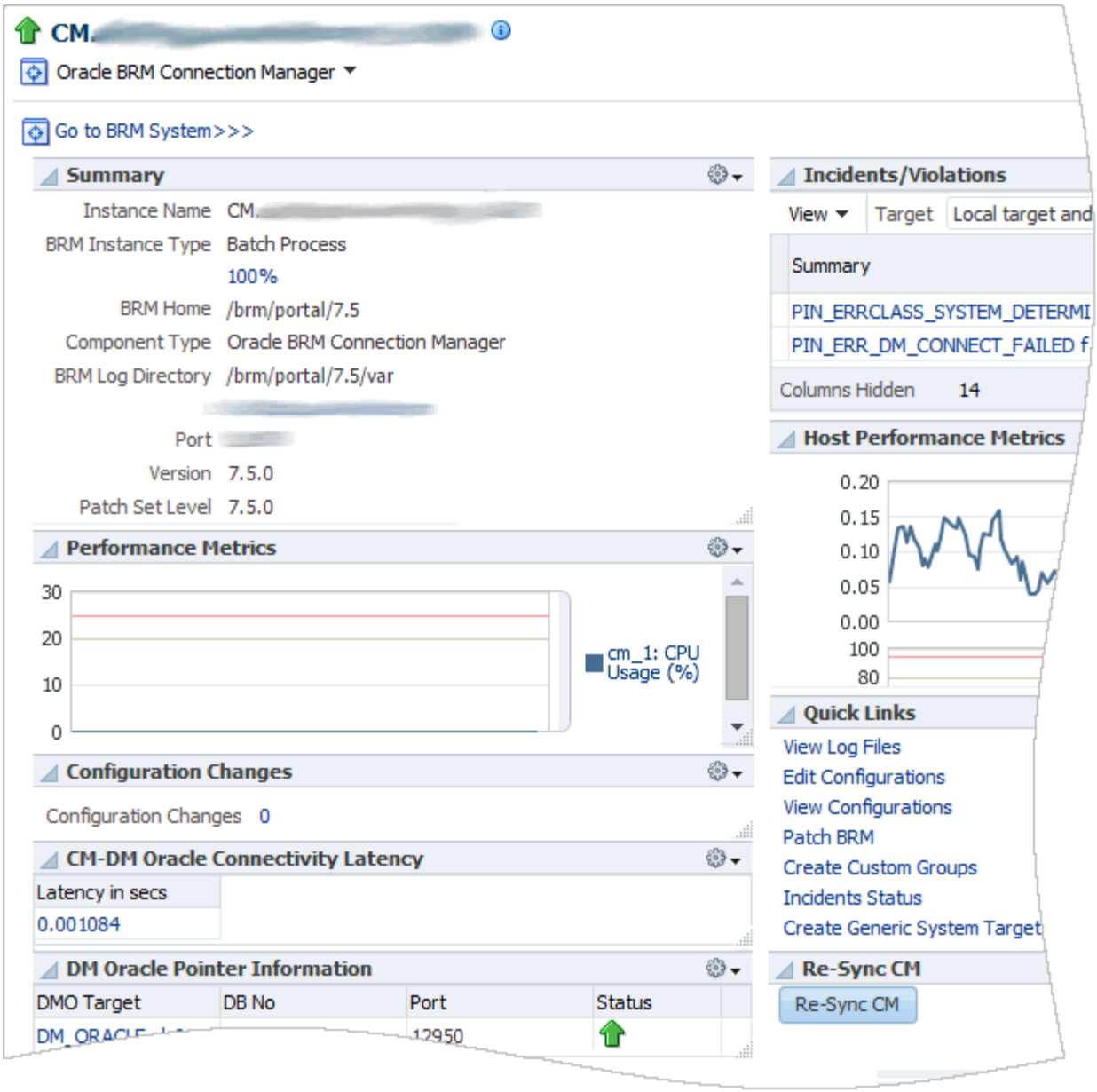



Table 5–2 describes the regions on all BRM component home pages.

***Table 5–2 Common Regions on BRM Component Home Pages***

| Region | Description |
|---|---|
| Summary | Displays summary information about the component, including the instance name and type, the component type, the path to the BRM home and log directories, the host and port, and the component version and patch numbers. |
| Performance Metrics | Displays graphs of CPU usage and physical memory usage by process.<br>Use this region to determine whether a particular process is causing problems by identifying fluctuations in process performance. |

*Table 5–2 (Cont.) Common Regions on BRM Component Home Pages*

| Region | Description |
|---|---|
| Configuration Changes | Displays the number of configuration changes since discovery or provisioning with Application Management Pack for Oracle Communications and provides a link to the list of configuration changes for the component.<br>Use this region to identify configuration changes that could be causing problems. |
| Incidents/Violations | Displays the number of critical, warning, and escalated incidents and violations, as well as a summary of each incident and links to view the incidents in Incident Manager.<br>Use this region to identify and resolve incidents. |
| Host Performance Metrics | Displays graphs of average number of processes run in the last 5 minutes, CPU usage, and physical memory usage by host.<br>Use this region to determine whether a particular host is causing problems by identifying fluctuations in host performance. |
| Quick Links | Provides links to Enterprise Manager Cloud Control tasks related to the target. |

Depending on the type of component target, the home page might contain additional regions. For example, Table 5–3 lists the additional regions included in the Connection Manager (CM) component home page shown in Figure 5–2.

*Table 5–3 Regions on BRM Connection Manager Component Home Pages*

| Region | Description |
|---|---|
| Re-Sync CM | Provides a button for refreshing the connection parameters between the CM and the Data Manager (DM) for the target. |
| CM-DM Oracle Connectivity Latency | Displays the latency between the CM and the DMs.<br>Use this region to identify latency problems. |
| DM Oracle Pointer Information | Displays the DMs connected to the CM target, including their status, database number, and port. Also provides links to the DM home pages. |

You can see a full list of metrics collected for a BRM component target and you can monitor the data that an individual metric collects for the target. See "Viewing Target Metrics" for information about accessing the list of metrics.

# BRM Collection Items and Metrics

This section describes the collection items and metrics collected for managed BRM targets. The component targets include the CM, DMs, and other components such as the Batch Controller, Universal Event Loader and Enterprise Application Integration (EAI) Manager.

See "About Conditions that Trigger Notifications" for an explanation of the entries in the tables included in this section.

Application Management Pack for Oracle Communications provides default thresholds for critical collection items and metrics. You can customize the thresholds and add thresholds and alerts for collection items and metrics that have no default

thresholds. See "Configuring Metric Monitoring Thresholds and Alerts" for more information about configuring thresholds.

## CollectionItem: Response

All BRM component targets have a Response Status collection item that provides target connection status. The Response Status is displayed as a green Up arrow or a red Down arrow beside the target name on the target's home page, in the list on the All Targets page, and in the regions on the BRM system target's home page.

The Management Agent checks the Response Status at a default interval of every minute.

Table 5–4 describes the condition that triggers an alert.

***Table 5–4 Component Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | LT | NA | 1 | 0 | The BRM *target* is down |

## CollectionItem: Processes

This collection item collects the following statistics for the BRM component process targets at a default interval of every minute:

- CPU Usage (%)
- Physical Memory Percentage

View the processes information in the Performance Metrics region of the BRM component target home page.

Table 5–5 shows the Processes conditions.

***Table 5–5 Process Conditions***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| percentage_cpu_usage | GT | 20 | 25 | 0 | The cpu usage exceeded the critical limit for %target% |
| physical_memory_percentage | GT | 20 | 25 | 0 | The memory usage exceeded the critical limit for %target% |

## Metric: LogFileMonitoring

This metric scans BRM manager component logs every 30 minutes and notifies the administrator when text indicating an error is found.

See the discussion of troubleshooting BRM in *Oracle Communications Billing and Revenue Management System Administrator's Guide* for information about error codes.

Table 5–6 shows the BRM LogFileMonitoring condition.

***Table 5–6 LogFileMonitoring Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| LogFileMonitoring | GT | 0 | Not Defined | 0 | *log_file_match_pattern* found in *log_file_name* |

You can add new error codes for this metric to search for in the log files. To add new error codes:

1. On the BRM host operating system, navigate to the BRM scripts folder in the directory where the Management Agent is installed. For example:

   ```
   Agent_home/plugins/oracle.cgbu.ocom.agent.plugin_12.1.0.2.0/scripts/brm
   ```

   where *Agent_home* is the directory where the Management Agent is installed.

2. Open the **brm_pattern.values** file in a text editor.

3. Search for the following line:

   ```
   PCM_PATTERNS = (
   ```

4. Add the new error code to the list.

   See the discussion of troubleshooting BRM in *Oracle Communications Billing and Revenue Management System Administrator's Guide* for information about error codes.

5. Search for the following line:

   ```
   PCM_ERROR_HELP = (
   ```

6. Add a description of the new error code to remind you what the error represents.

7. Save and close the file.

## Metric: *component*_config

The Management Agent uses this metric to collect a component's configuration parameters at a default interval of every 10 minutes.

There are no conditions for this metric.

See "Viewing BRM Configurations" for information about viewing configurations in the administration console.

### Metric: Latency on TEST_LOOPBACK

This metric checks the time in seconds that the CM takes to submit a test opcode and receive a response from the DM. The time is checked at a default interval of every minute.

View the latency information in the CM-DM Oracle Connectivity Latency region of the BRM CM target home page.

There are no conditions for this metric.

## BRM Pipeline Collection Items and Metrics

This section describes collection items and metrics collected for BRM real-time and batch rating pipeline components.

See "About Conditions that Trigger Notifications" for an explanation of the entries in the tables included in this section.

Application Management Pack for Oracle Communications provides default thresholds for critical collection items and metrics. You can customize the thresholds and add thresholds and alerts for collection items and metrics that have no default thresholds. See "Configuring Metric Monitoring Thresholds and Alerts" for more information about configuring thresholds.

### CollectionItem: Response

All BRM pipeline targets have a Response Status collection item that provides target connection status. The Response Status is displayed as a green Up arrow or a red Down arrow beside the target name on the target's home page and in the list on the All Targets page.

The Management Agent checks the Response Status at a default interval of every minute. Table 5–7 describes the condition that triggers an alert.

***Table 5–7 Pipeline Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | LT | NA | 1 | 0 | The BRM %target% is down |

### CollectionItem: Processes

This collection item collects the CPU usage and physical memory percentage for the pipeline processes on the target at a default interval of every minute.

There are no conditions for this collection item.

### CollectionItem: ElapsedTime

This collection item retrieves the time that has elapsed since the process began. The time is presented in the number of days, hours, minutes, and seconds that have elapsed.

The Management Agent retrieves the elapsed time at a default interval of every minute.

There are no conditions for this collection item.

## Metric: ModuleProcTime

This metric represents the pipeline module processing time. The Management Agent updates ModuleProcTime every 30 minutes.

Table 5–8 shows the condition that triggers a message.

***Table 5–8 ModuleProcTime Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| count | GT | 0 | Not Defined | 0 | The Module Processing times for *target* is *log_file_message* |

## Metric: Input Controller MaxMin

This metric collects the maximum and minimum processing time in nanoseconds for the BRM Pipeline target to convert input data to event data record (EDR). This metric is collected every 5 minutes.

There are no conditions for this metric.

## Metric: Input Controller Table

This metric collects the following pipeline Input Control data at a default interval of every 5 minutes:

- Processing Time (ns)
- Timestamp

There are no conditions for this metric.

## CollectionItem: Output Stats Avg

This collection item collects the following output statistics on the pipeline target at a default interval of every 5 minutes:

- Accumulated Txn Processing Time (sec)
- Total EDR Count (after transaction ended)
- Total EDR Count (real-time)
- Total Txn Count

There are no conditions for this collection item.

## CollectionItem: Output Stats Table

This collection item collects the following output statistics on the pipeline target at a default interval of every 5 minutes:

- Throughput (edrs/sec)
- Timestamp

There are no conditions for this collection item.

## Metric: *pipeline*_config

The Management Agent uses this metric to collect a pipeline's configuration parameters at a default interval of once per day.

There are no conditions for this metric.

See "Viewing BRM Configurations" for information about viewing configurations in the administration console.

# 6

# Monitoring Elastic Charging Engine

This chapter describes how to monitor Oracle Communications Elastic Charging Engine (ECE) targets using the home pages provided by Oracle Application Management Pack for Oracle Communications.

It also describes the ECE monitoring metrics provided by Oracle Application Management Pack for Oracle Communications.

## About Monitoring ECE

Application Management Pack for Oracle Communications enables monitoring ECE targets using Oracle Enterprise Manager Cloud Control. You can monitor ECE node targets and ECE cluster targets.

You must install and configure the Application Management Pack for Oracle Communications plug-in before monitoring ECE. See the following chapters for information about setting up Oracle Communications application monitoring with Enterprise Manager Cloud Control:

- Installing Application Management Pack for Oracle Communications
- Configuring Oracle Communications Targets
- Managing Communications Applications with Enterprise Manager Cloud Control

### About the Monitoring Home Page for ECE Targets

The home page for an ECE target displays metrics data that you can use to monitor the health of your ECE node and identify problems. See "Viewing Home Pages" for information about accessing target home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Figure 6–1 shows the regions on the home page for an ECE node target.

***Figure 6–1 ECE Node Target Home Page***

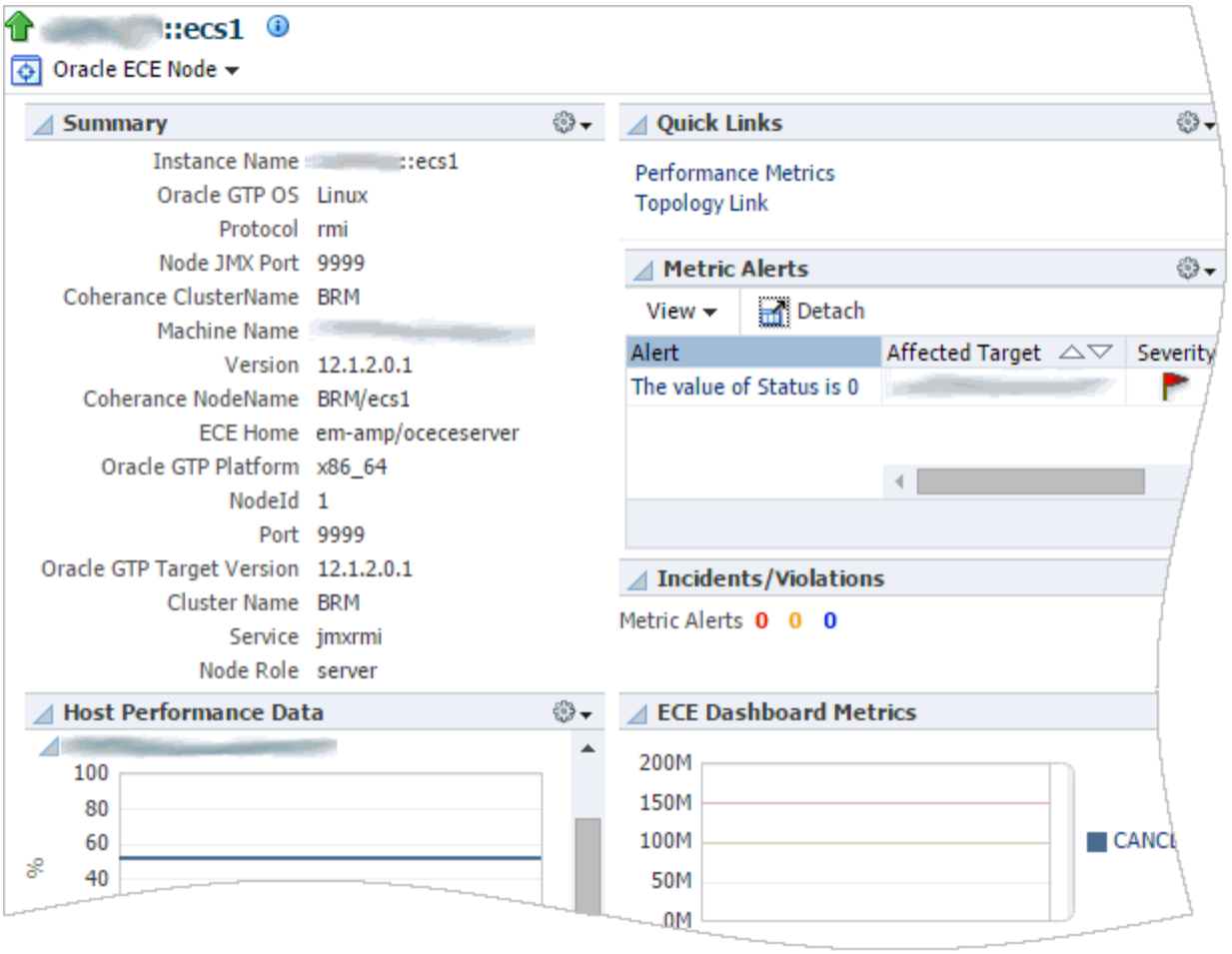



Table 6–1 describes the regions on the home page for ECE targets.

***Table 6–1 Regions on the ECE Node Target Home Page***

| Region | Description |
|---|---|
| Summary | Displays information about the ECE instance, including operating systems, ports, cluster names, version numbers, and more. |
| Host Performance Data | Displays performance information including CPU and memory usage.<br>Use this region to identify performance problems for individual hosts. |
| Quick Links | Provides links to the topology viewer and to performance metrics for the ECE target. |
| Metric Alerts | Displays any metric alerts for the targets in the suite.<br>Use this region to identify and resolve alerts. |
| Incidents/Violations | Displays the number of critical, warning, and escalated incidents and violations.<br>Use this region to identify problems based on high numbers of incidents. |

*Table 6–1 (Cont.) Regions on the ECE Node Target Home Page*

| Region | Description |
|---|---|
| ECE Dashboard Metrics | Displays latency time for ECE operations.<br>Use this region to identify operations that are taking too long or creating backlogs. |

The home pages for ECE cluster targets also include the ECE Oracle Coherence Installation region, which shows the status of all the Coherence targets in the cluster. The home pages for ECE cluster targets do not include the Incidents/Violations, Metric Alerts, or ECE Dashboard Metrics regions.

# ECE Node Metrics

This section describes metrics collected for ECE client nodes.

See "About Conditions that Trigger Notifications" for an explanation of fields and tables included below.

Application Management Pack for Oracle Communications provides default thresholds for critical collection items and metrics. You can customize the thresholds and add thresholds and alerts for collection items and metrics that have no default thresholds. See "Configuring Metric Monitoring Thresholds and Alerts" for more information about configuring thresholds.

## Metric: Response

All ECE targets have a Response Status collection item that provides target connection status. The Response Status is either up or down.

The Management Agent checks the Response Status at a default interval of every minute. Enterprise Manager Cloud Control administration console displays a message indicating whether the ECE node is either up or down. Table 6–2 describes the condition that triggers an alert.

*Table 6–2 ECE Node Response Condition*

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | EQ | NA | 0 | 0 | The ECE Node is down |

## Metric: Performance

This metric monitors event processing performance in ECE. Application Management Pack for Oracle Communications generates alerts when processing parameters exceed the warning and critical thresholds listed in Table 6–3.

***Table 6–3 ECE Node Performance Condition***

| Condition Column Name | Description | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|---|
| CANCEL_ MAX_ LATENCY | The mean latency of an ECE cancel operation. | GT | 100000000ns | 150000000ns | 0 | CANCEL_ MAX_ LATENCY is %value% and has crossed warning (%warning_ threshold%) or critical (%crticial_ threshold%) threshold. |
| INITIATE_ MAX_ LATENCY | The maximum latency of an ECE initiation operation. | GT | 50000000ns | 100000000ns | 0 | INITIATE_ MAX_ LATENCY is %value% and has crossed warning (%warning_ threshold%) or critical (%crticial_ threshold%) threshold. |
| TERMINATE _MAX_ LATENCY | The maximum latency of ECE termination operations. | GT | 100000000ns | 150000000ns | 0 | TERMINAT E_MAX_ LATENCY is %value% and has crossed warning (%warning_ threshold%) or critical (%crticial_ threshold%) threshold. |
| UPDATE_ MAX_ LATENCY | The maximum latency of an ECE update operation. | GT | 100000000ns | 0150000000ns | 0 | UPDATE_ MAX_ LATENCY is %value% and has crossed warning (%warning_ threshold%) or critical (%crticial_ threshold%) threshold. |

# ECE Cluster Metrics

This section describes metrics collected for ECE clusters.

See "About Conditions that Trigger Notifications" for an explanation of fields and tables included below.

Application Management Pack for Oracle Communications provides default thresholds for critical collection items and metrics. You can customize the thresholds and add thresholds and alerts for collection items and metrics that have no default thresholds. See "Configuring Metric Monitoring Thresholds and Alerts" for more information about configuring thresholds.

## Metric: Response

All ECE clusters have a Response Status collection item that provides target connection status. The Response Status is either up or down.

The Management Agent checks the Response Status at a default interval of every minute. Enterprise Manager Cloud Control administration console displays a message indicating whether the ECE node is either up or down. Table 6–4 describes the condition triggering an alert.

***Table 6–4 ECE Cluster Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | EQ | NA | 0 | 0 | The ECE Cluster is down |

## Additional Coherence Cluster Metrics

See the chapter on monitoring a Coherence cluster in *Oracle Enterprise Manager Cloud Control Getting Started with Oracle Fusion Middleware Management* for more information about monitoring the Coherence cluster on which ECE runs.

# 7

# Monitoring Network Charging and Control

This chapter describes how to monitor Oracle Communications Network Charging and Control (NCC) targets using the home pages provided by Oracle Application Management Pack for Oracle Communications.

It also describes the NCC monitoring collection items and metrics provided by Oracle Application Management Pack for Oracle Communications.

## About Monitoring NCC

Application Management Pack for Oracle Communications enables monitoring NCC targets using Oracle Enterprise Manager Cloud Control. You can monitor NCC system targets and NCC component targets.

An NCC system contains the following types of targets:

- NCC: Represents the whole NCC system.
- NCC SLC: Represents the NCC Service Logic Controller component.
- NCC SMP: Represents the NCC Service Management System component.
- NCC VWC: Represents the NCC Voucher and Wallet Server component.

You must install and deploy the Application Management Pack for Oracle Communications plug-in on both your Management Server and host agents before monitoring NCC targets.

See the following chapters for information about setting up Oracle Communications application monitoring with Enterprise Manager Cloud Control:

- Installing Application Management Pack for Oracle Communications
- Configuring Oracle Communications Targets
- Managing Communications Applications with Enterprise Manager Cloud Control

See "About Conditions that Trigger Notifications" for an explanation of entries and tables included below.

### About the Monitoring Home Page for NCC Targets

The home page for an NCC target displays metrics data that you can use to monitor the health of your NCC system and identify problems. See "Viewing Home Pages" for information about accessing communications NCC target home pages. You can also view the target's configuration topology as described in "Viewing Topology".

Figure 7–1 shows the regions on the home page for an NCC system target.

***Figure 7–1 NCC System Target Home Page***

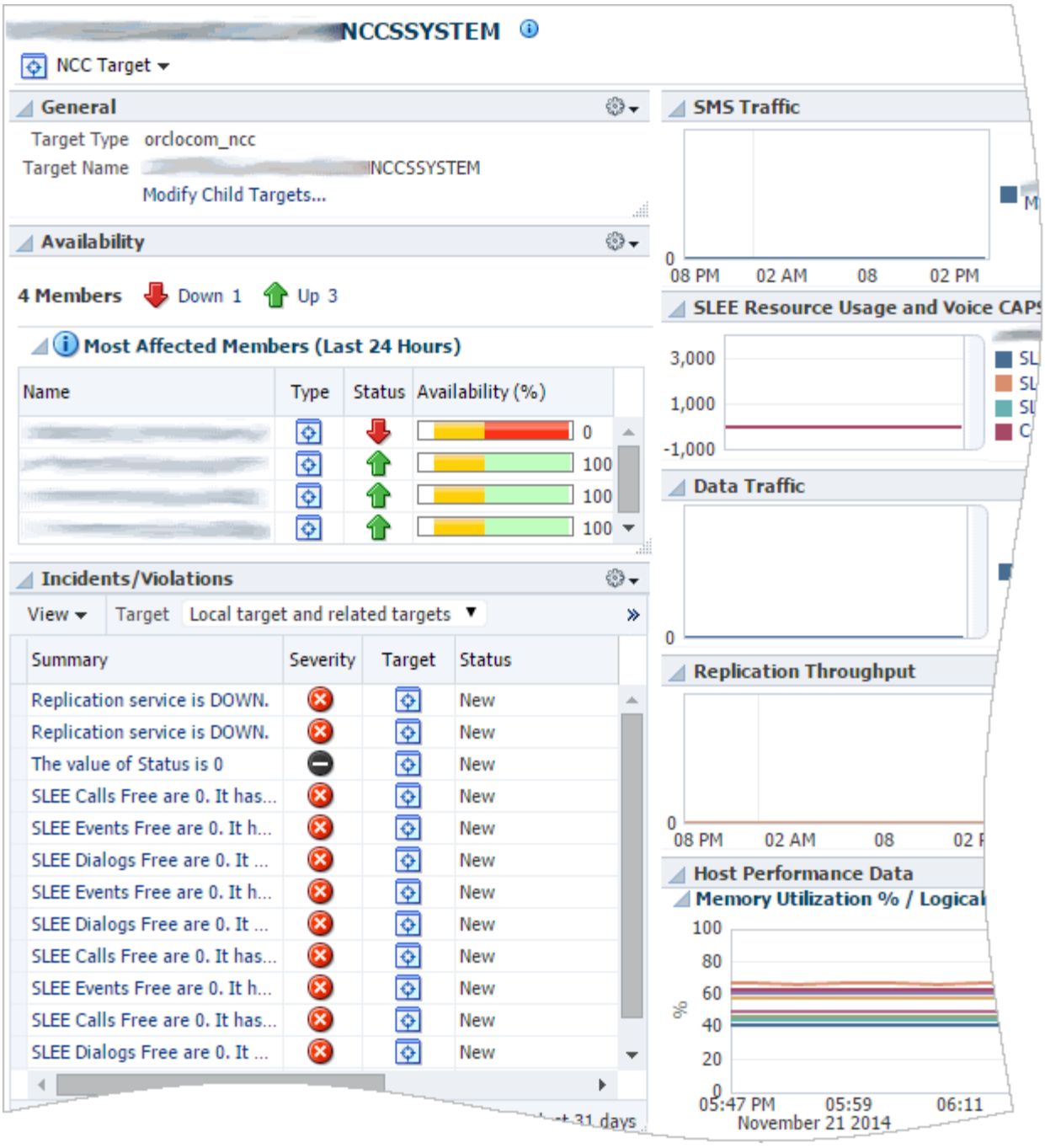



Table 7–1 describes the regions on the home page for NCC system targets.

***Table 7–1 Regions on the NCC Target Home Page***

| Region | Description |
|---|---|
| General | Displays the target type and name, and a link for adding or removing child targets from the system. |

*Table 7–1 (Cont.) Regions on the NCC Target Home Page*

| Region | Description |
|---|---|
| Availability | Displays the number of components that are up and down and gives details about the components affected most in the last 24 hours.<br>Use this region to identify which components are causing problems and to access the home pages for those components. |
| Incidents/Violations | Displays details about incidents and violations for all the components in the system.<br>Use this region to identify and resolve incidents. |
| SMS Traffic | Displays a graph representing the rate at which SMS messages are passing through the system. |
| SLEE Resource Usage and Voice CAPS | Displays graphs representing the usage of Service Logic Execution Environment (SLEE) events, dialogs, and calls, as well as Camel Application Part (CAP) operations for each component in the system. |
| Data Traffic | Displays graphs representing the number of active data sessions, engaged services, and throttled requests currently in the system. |
| Replication Throughput | Displays a graph representing the rate at which replication events are passing through the system. |
| Host Performance Data | Displays performance information for the host on which ECE is deployed, including CPU and memory use.<br>Use this region to determine whether a particular host is causing problems by identifying fluctuations in host performance. |

Table 7–2 describe the regions on the home pages for NCC component targets.

*Table 7–2 Regions on the NCC Component Home Pages*

| Region | Description |
|---|---|
| Summary | Displays the status of the NCC component target. |
| Incidents and Problems | Displays details about incidents and violations for the component.<br>Use this region to identify and resolve incidents. |

You can see a full list of metrics collected for an NCC or NCC component target and you can monitor the data that an individual metric collects for the target. See "Viewing Target Metrics" for information about accessing the list of metrics.

# NCC Service Management System Collection Items

This section describes collection items collected for NCC Service Management System nodes.

See "About Conditions that Trigger Notifications" for an explanation of entries and tables included below.

## CollectionItem: Response

Service Management System targets have a Response Status collection item that provides target connection status. The Response Status is either up or down.

The Management Agent checks the Response Status at a default interval of every minute. Enterprise Manager Cloud Control administration console displays a message indicating whether the Service Management System node is either up or down. Table 7–3 describes the condition that triggers an alert.

***Table 7–3 Service Manager System Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | EQ | NA | 0 | 0 | NA |

## CollectionItem: PORTS_IN_CLOSE_WAIT

This collection item generates an alert when the Management Agent detects two occurrences of a port in CLOSE_WAIT state. Table 7–4 describes the condition that triggers an alert.

***Table 7–4 PORTS_IN_CLOSE_WAIT Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| state | EQ | NA | CLOSE_WAIT | 2 | Port stuck in CLOSE_ WAIT |

## CollectionItem: Replication Throughput

This collection item monitors the replication throughput at a default interval of every 5 minutes. Table 7–5 describes the condition that triggers an alert.

***Table 7–5 Replication Throughput Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| state | EQ | NA | 0 for a duration of 5 minutes | 0 | Replication service is DOWN. |

# NCC Voucher and Wallet Server Collection Items

This section describes collection items collected for Voucher and Wallet Server nodes.

See "About Conditions that Trigger Notifications" for an explanation of entries and tables included below.

### CollectionItem: Response

Voucher and Wallet Server targets have a Response Status collection item that provides target connection status. The Response Status is either up or down.

The Management Agent checks the Response Status at a default interval of every minute. Enterprise Manager Cloud Control administration console displays a message indicating whether the NCC node is either up or down. Table 7–6 describes the condition that triggers an alert.

***Table 7–6 Voucher and Wallet Server Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | EQ | NA | 0 | 0 | NA |

### CollectionItem: PORTS_IN_CLOSE_WAIT

This collection item generates an alert when the Management Agent detects two occurrences of a port in CLOSE_WAIT state. Table 7–7 describes the condition that triggers an alert.

***Table 7–7 PORTS_IN_CLOSE_WAIT Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| state | EQ | NA | CLOSE_WAIT | 2 | Port stuck in CLOSE_ WAIT |

### CollectionItem: SLEE_AND_CAPS

This collection item collects the following Service Logic Execution Environment (SLEE) statistics for Enterprise Manager Cloud Control monitoring at a default interval of every 1 minute:

- SLEE Dialogues Free
- SLEE Events Free
- SLEE Calls Free
- CAPS in Last Minute

There are no conditions for this collection item.

## NCC Service Logic Controller Collection Items and Metrics

This section describes collection items and metrics collected for Service Logic Controller nodes.

See "About Conditions that Trigger Notifications" for an explanation of entries and tables included below.

## CollectionItem: Response

Service Logic Controller targets have a Response Status collection item that provides target connection status. The Response Status is either up or down.

The Management Agent checks the Response Status at a default interval of every minute. Enterprise Manager Cloud Control administration console displays a message indicating whether the Service Logic Controller node is either up or down. Table 7–8 describes the condition that triggers an alert.

***Table 7–8 Service Logic Controller Node Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | EQ | NA | 0 | 0 | NA |

## CollectionItem: PORTS_IN_CLOSE_WAIT

This collection item generates an alert when the Management Agent detects two occurrences of a port in CLOSE_WAIT state. Table 7–9 describes the condition that triggers an alert.

***Table 7–9 PORTS_IN_CLOSE_WAIT Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| state | EQ | NA | CLOSE_WAIT | 2 | Port stuck in CLOSE_ WAIT |

## CollectionItem: SLEE_AND_CAPS

This collection item collects the following Service Logic Execution Environment (SLEE) statistics for Enterprise Manager Cloud Control monitoring at a default interval of every 1 minute:

- SLEE Dialogues Free
- SLEE Events Free
- SLEE Calls Free
- CAPS in Last Minute

There are no conditions for this collection item.

## CollectionItem: SLEE_MAPS

This collection item collects the following Service Logic Execution Environment (SLEE) statistics for Enterprise Manager Cloud Control monitoring at a default interval of every 5 minutes:

- Short Message Attempts per Second

There are no conditions for this collection item.

### CollectionItem: DiameterSessions

This collection item collects the following Diameter statistics for Enterprise Manager Cloud Control monitoring at a default interval of every 5 minutes:

- Active Sessions

There are no conditions for this collection item.

### CollectionItem: DiameterThrottled

This collection item collects the following Diameter statistics for Enterprise Manager Cloud Control monitoring at a default interval of every 5 minutes:

- Throttled Requests

There are no conditions for this collection item.

### CollectionItem: DiameterEngagedServices

This collection item collects the following Diameter statistics for Enterprise Manager Cloud Control monitoring at a default interval of every 5 minutes:

- Engaged Services

There are no conditions for this collection item.

## Additional NCC Metrics

Management Agents on NCC hosts also support the following Enterprise Manager Cloud Control host and database monitoring metrics useful for maintaining your system:

See "About Conditions that Trigger Notifications" for an explanation of entries and tables included below.

- Hardware Failure
- Disk Space Used
- Process Memory Usage
- Database Fragmentation
- Tablespace Usage
- Invalid Objects in Schema
- SYSAUX Tablespace Used
- Share Pool Usage

Table 7–10 contains the conditions that generate alerts for these metrics.

***Table 7–10 Host Alert Conditions***

| Metric | Operator | Default Warning Threshold | Default Critical Threshold |
|---|---|---|---|
| Hardware Failure | EQ | NA | Any |
| Disk Space Used | GT | NA | 90% |
| Process Memory Usage | GT | NA | 2GB |

*Table 7–10 (Cont.) Host Alert Conditions*

| Metric | Operator | Default Warning Threshold | Default Critical Threshold |
|---|---|---|---|
| Database Fragmentation | GT | NA | 3 (High Water Mark) |
| Tablespace Usage | GT | NA | 90% |
| Invalid Objects in Schema | EQ | NA | Any |
| SYSAUX Tablespace Used | GT | NA | 90% |
| Share Pool Usage | GT | NA | 95% |

# 8

# Monitoring Operations Support Systems

This chapter describes how to monitor the Oracle Communications operations support systems (OSS) using the home pages provided by Oracle Application Management Pack for Oracle Communications.

This chapter also describes the monitoring metrics provided by Application Management Pack for Oracle Communications for OSS systems.

## About Monitoring Operations Support Systems

Operations support systems include Oracle Communications Order and Service Management (OSM), Oracle Communications Unified Inventory Management (UIM), and Oracle Communications ASAP.

Application Management Pack for Oracle Communications enables monitoring OSS targets using Oracle Enterprise Manager Cloud Control. A Management Agent monitors targets for collection items and metrics and sends the data to the Management Server for presentation.

You must install and deploy the Application Management Pack for Oracle Communications plug-in on both your Management Server and host agents before monitoring OSS targets.

You can monitor the following operations support system target types:

- Communications suite: The home pages for communications suite targets display information about all of the applications that make up the suite. See "About the Monitoring Home Page for Communications Suite Targets".
- OSM System: The home pages for OSM System targets display information about all of the OSM nodes that make up the system. See "About the Monitoring Home Page for OSM System Targets".
- The following OSS application target types:
  - OSM Node: The home pages for OSM node targets display information about the individual OSM nodes.
  - UIM: The home pages for UIM targets display information about the individual UIM nodes.
  - ASAP: The home pages for ASAP targets display information about the individual ASAP nodes.

  See "About the Monitoring Home Page for OSS Application Targets".

See the following chapters for information about setting up Oracle Communications application monitoring with Enterprise Manager Cloud Control:

- Installing Application Management Pack for Oracle Communications
- Configuring Oracle Communications Targets
- Managing Communications Applications with Enterprise Manager Cloud Control

## About the Monitoring Home Page for Communications Suite Targets

The home page for a communications suite target displays metrics data that you can use to monitor the health of your suite and identify problems. See "Viewing Home Pages" for information about accessing communications suite home pages. You can also view the suite's configuration topology as described in "Viewing Topology".

Figure 8–1 shows the regions on the home page for a communications suite target.

***Figure 8–1 Communications Suite Target Home Page***

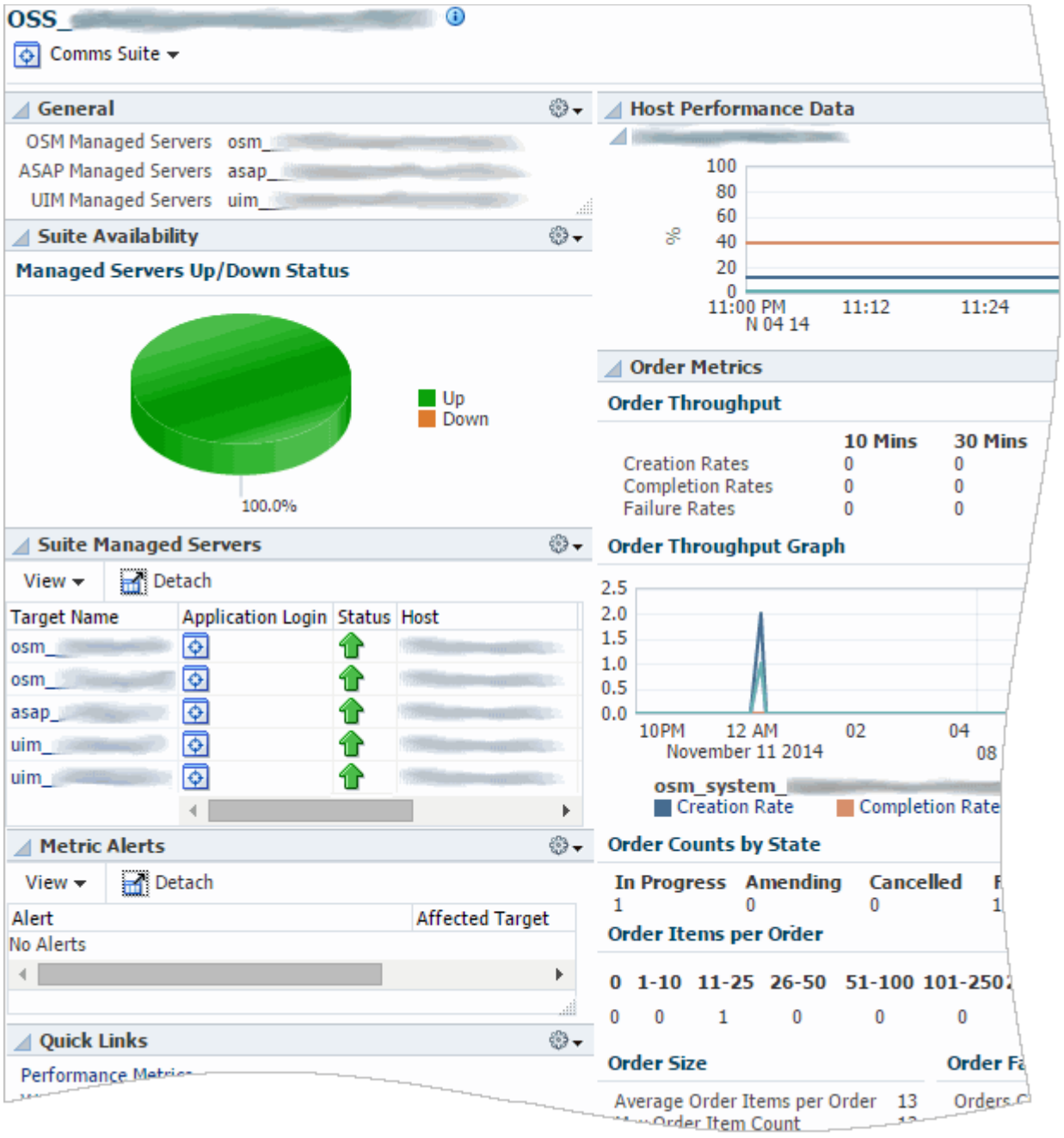



Table 8–1 describes the regions on the home page for communications suite targets.

***Table 8–1 Regions on the Communications Suite Home Page***

| Region | Description |
|---|---|
| General | Lists the managed servers for OSM, ASAP, and UIM. |
| Suite Availability | Displays the percentage of managed servers that are available. |

*Table 8–1 (Cont.) Regions on the Communications Suite Home Page*

| Region | Description |
|---|---|
| Suite Managed Servers | Displays information about each managed server representing a node in the suite. Information includes the target name, the server status, the host, port, and server name, the number of alerts for the node, and links to the node home page and external application page. |
| Metric Alerts | Displays any metrics alerts for the targets in the suite. |
| Quick Links | Provides links to related Enterprise Manager Cloud Control pages. |
| Host Performance Data | Displays performance information including CPU and memory usage. |
| Order Metrics | Displays information about order throughput, states, size, and the number of order failures. This region is identical to the Order Metrics region on the OSM system home page. See "About the Order Metrics Region". |

You can see a full list of metrics collected for a suite target and you can monitor the data that an individual metric collects for the target. See "Viewing Target Metrics" for information about accessing the list of metrics.

## Configuring Monitoring Credentials for Displaying Host Performance Data

If the graph for a host in the Host Performance region of the Comms Suite target home page displays an error message, you may need to configure the monitoring credentials for that host.

To configure the monitoring credentials:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. Click **Targets**, and then **All Targets**.
3. In the Target Type tree, select the OSM node, ASAP, or UIM target type.
4. In the list of targets, right-click the OSM, ASAP, or UIM target deployed on the host for which the error message is displayed.
5. From the context menu, select **Target Setup**, and then **Monitoring Configuration**.
6. In the **Hostname** field, do one of the following:
   - If the field contains an IP address, such as **192.0.2.1**, but the name of the Comms Suite target contains a host name, such as **osshost1.example.com**, replace the IP address with the name of the host on which the OSM, ASAP, or UIM target is deployed, such as **osshost2.example.com**.
   - If the field contains a host name, such as **osshost2.example.com**, but the name of the Comms Suite target contains an IP address, such as **192.0.2.1**, replace the host name with the IP address of the host on which the OSM, ASAP, or UIM target is deployed, such as **192.0.2.2**.
7. Click **OK**.
8. Navigate to the Comms Suite target home page and confirm that the host performance information appears.

# About the Monitoring Home Page for OSM System Targets

The home page for an OSM system displays metrics data that you can use to monitor the health of your entire OSM system and identify the source of problems. See "Viewing Home Pages" for information about accessing OSM system home pages. You can also view the system's configuration topology as described in "Viewing Topology".

Use the **Dashboard** tab to get an overall view of the system. See "About the Dashboard Tab" for a description of the regions on the **Dashboard** tab and examples of how to use these regions to identify the source problems.

Use the **Metrics by Server**, **Metrics by Order Type**, and **Metrics by Cartridge** tabs to see the metrics as they pertain to individual servers, order types, and cartridges. Categorizing the metrics helps you identify whether problems are restricted to a particular server, order type, or cartridge. See "About the Metrics by Server, Order Type, and Cartridge Tabs" for descriptions of the regions on these tabs.

Application Management Pack for Oracle Communications includes the OSM Order Metrics Manager feature, which provides the metrics displayed on the home page for OSM systems. If you see an error on the OSM home page in Enterprise Manager Cloud Control stating that the metrics are not available, you will need to manually install the metrics rules files that Order Metrics Manager uses. See the discussion of manually loading metric rules files in *Oracle Communications Order and Service Management Installation Guide* for more information.

You can see a full list of metrics collected for an OSM system target and you can monitor the data that an individual metric collects for the target. See "Viewing Target Metrics" for information about accessing the list of metrics.

## About the Dashboard Tab

The **Dashboard** tab displays summary information for the entire OSM system. It is divided into the regions described in this section.

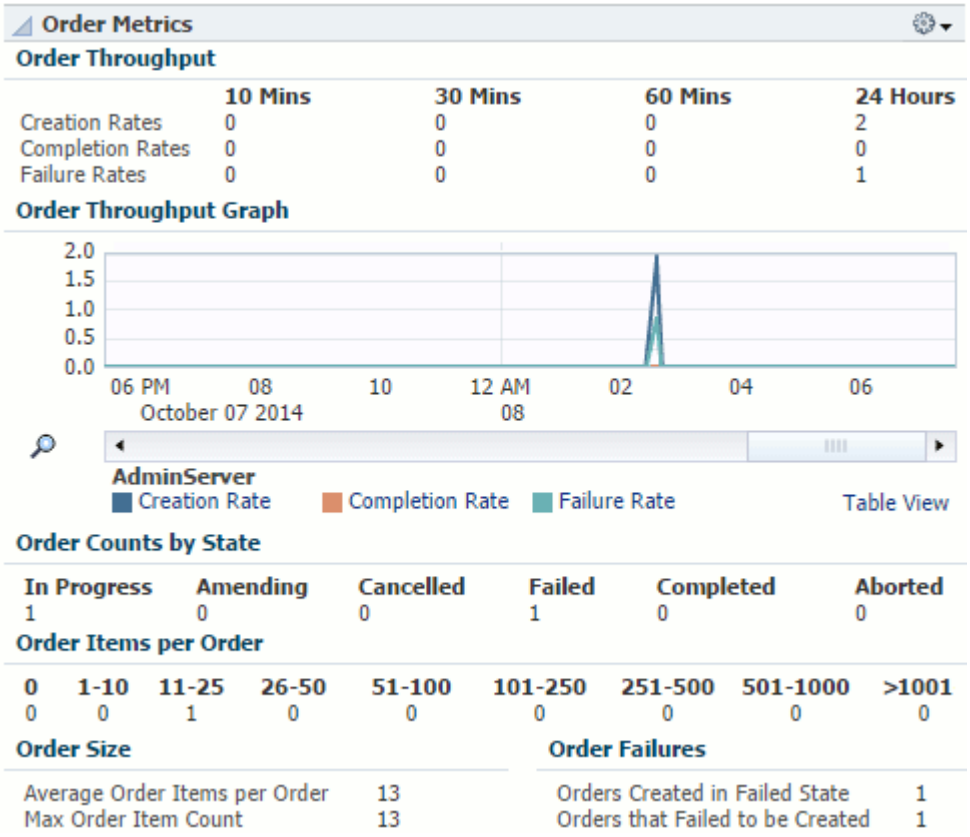
### About the Order Metrics Region

The Order Metrics region helps you assess how well your system is processing orders.

This region, shown in Figure 8–2, displays the following information:

- The rates at which orders are created, completed, and failed. Compare these rates to identify order backlogs. A higher number of created or failed orders compared to a low number of completed orders can indicate a problem.
- The number of orders in different states. Use these numbers to monitor order state transitions. A high number of orders in the Failed, Amending, or Aborted states can indicate a problem.
- The size of orders based on order items. Use these numbers to identify performance problems. If a high number of large orders negatively impacts performance, you may need to tune your system differently.
- The number of orders failing on creation. Use these numbers to identify order creation and recognition issues.

*Figure 8–2 Order Metrics Region of the Dashboard Tab*



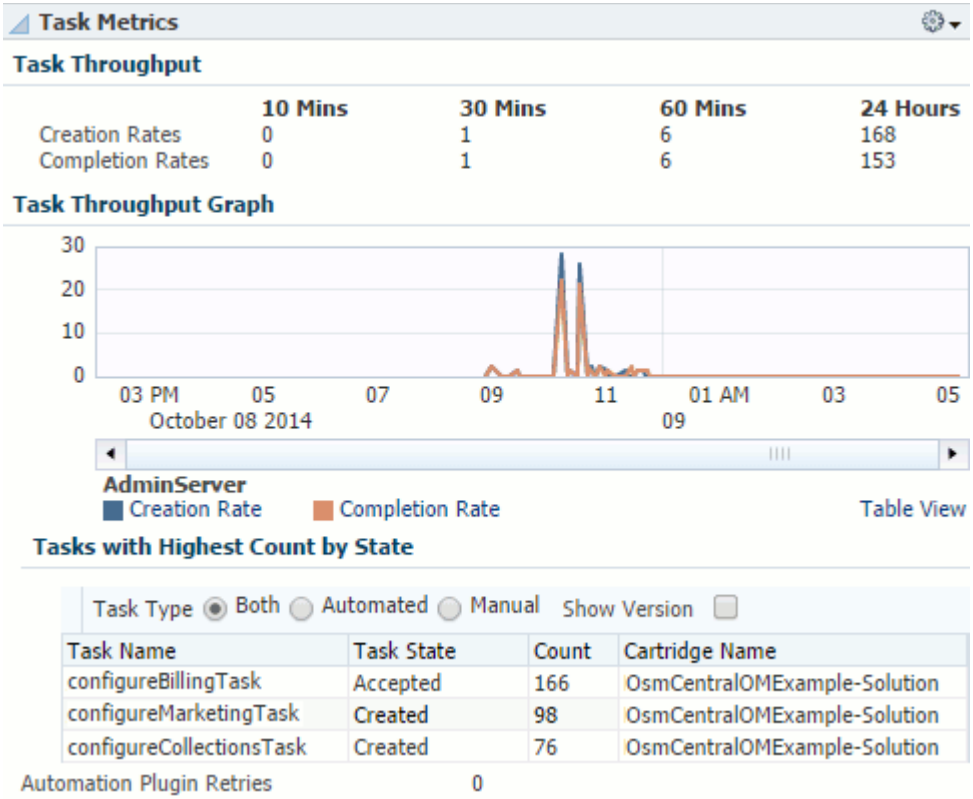

## About the Task Metrics Region

The Task Metrics region helps you assess how well your system is completing tasks and identify particular tasks that may be causing problems.

This region, shown in Figure 8–3, displays the following information:

- The rates at which tasks are created and completed. Compare these rates to identify task backlogs. A higher number of created tasks than completed tasks can indicate a problem.
- The name and number of tasks in a given state. Use these numbers to identify whether a particular task is causing problems.

*Figure 8–3 Task Metrics Region of the Dashboard Tab*




You can use this region in conjunction with the Order Metrics region. For example, if you see a high number of failed orders in the Order Metrics region, and the Task Metrics region shows a high number of a particular task in the Failed state, that task is likely causing the order failure. You can investigate and resolve the task in the OSM Task Web client. See *Oracle Communications Order and Service Management Task Web Client User's Guide* for information about using the Task Web client.

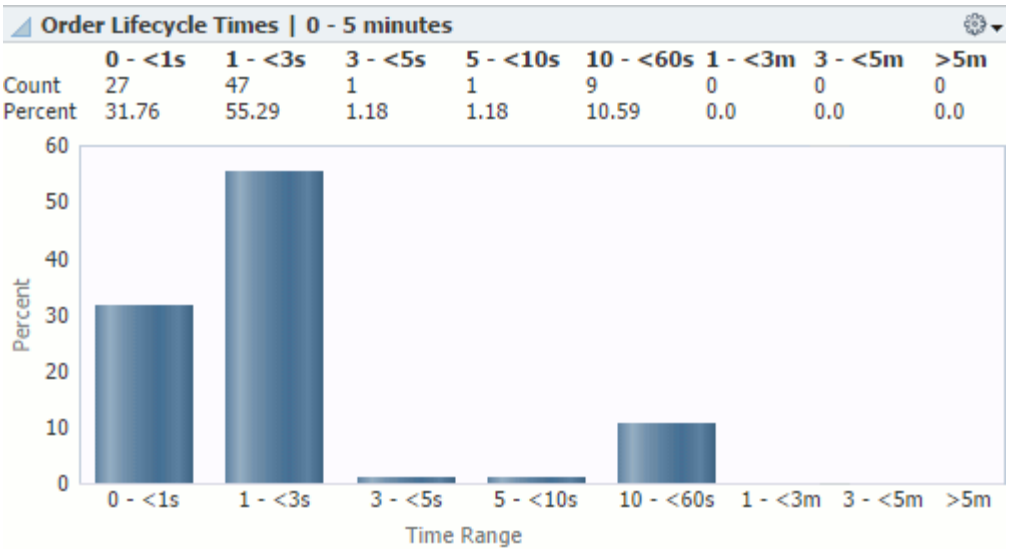
## About the Order Lifecycle Times Region

The Order Lifecycle Times region helps you identify performance issues and assess how long your system is taking to process orders.

This region, shown in Figure 8–4, displays the number of orders completed within a range of time periods and the percent of the total orders that each time period represents. A significant change in order lifecycle times can indicate a problem.

By default, this region shows orders completed in 0 to 5 minutes. You can add regions to display orders completed in 5 minutes to 7 days, or in 7 days to 90 days. Add regions using the **Personalize Page** button as described in the discussion of personalizing a Cloud Control page in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

***Figure 8–4 Order Lifecycle Times Region of the Dashboard Tab***




You can use this region in conjunction with the Order Metrics region. For example, if the Order Metrics region shows that most of your orders have very few order items, but the Order Lifecycle Times region shows that majority of your orders are taking a long time to complete, your system may have a performance issue. See *Oracle Communications Order and Service Management System Administrator's Guide* for information about improving OSM performance.

### About the Quick Links Region

The Quick Links region provides the following links:

- **OSM Information Center**: Opens the My Oracle Support page for the OSM information center. You can see news and announcements, knowledge articles, and information about how to use, troubleshoot, maintain, patch, install, configure, and certify OSM.
- **Oracle Communications Documentation**: Opens the Oracle Technology Network page for Oracle Communications documentation. You can see the documentation for all Oracle Communications products.
- **Performance Metrics**: Opens the performance dashboard for the OSM system target. You can see information about the OSM system's server performance.
- **WebLogic Domain Dashboard**: Opens the home page for the WebLogic Server domain on which the OSM system is deployed. You can see information about the servers on the domain.
- **WebLogic Server Performance Summary**: Opens the performance summary page for the first managed server in the cluster on which the OSM system is deployed. You can see graphs of the performance information.
- **WebLogic Server Topology**: Opens the Configuration Topology Viewer for the first managed server in the cluster on which the OSM system is deployed. You can see relationships between the various middleware and application nodes.
- **Database Dashboard**: Opens the home page for the OSM database. You can see information about the database. This link appears if you registered the database target when discovering and promoting the OSM target.

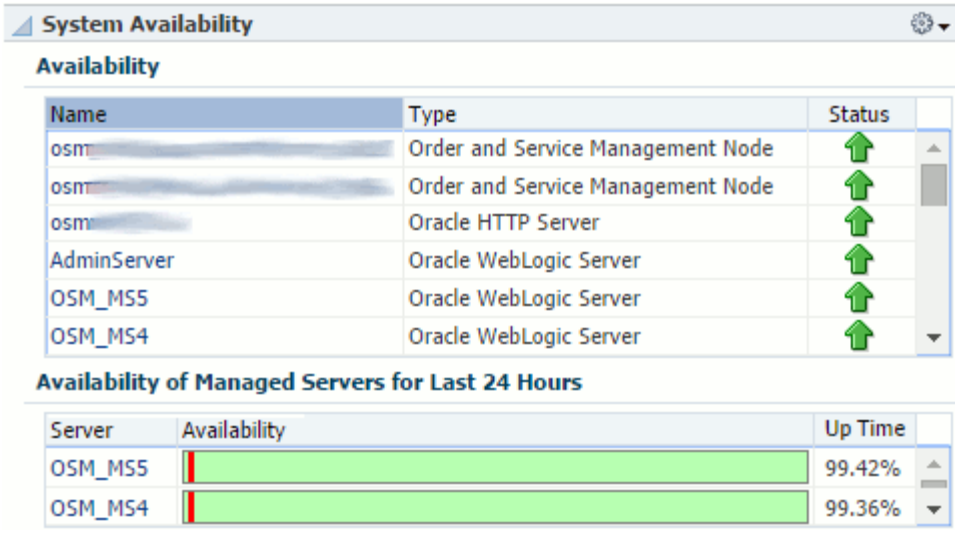
## About the System Availability Region

The System Availability region helps you identify problems with individual servers and assess the overall health of your system.

This region, shown in Figure 8–5, displays the following information:

- The current status of the servers in the system, including OSM nodes, HTTP servers, the administration server, managed servers, database instances, hosts, and Management Agents.
- The availability of the managed servers for the last 24 hours.

***Figure 8–5 System Availability Region of the Dashboard Tab***




You can use this region in conjunction with the other regions of the **Dashboard** tab. For example, if the Order Metrics region shows that order throughput decreased at a certain point in time, you can check if any of the managed servers were down at that same time. If several servers were down or unreachable, the servers that were up could have been overloaded, causing the decreased order throughput.

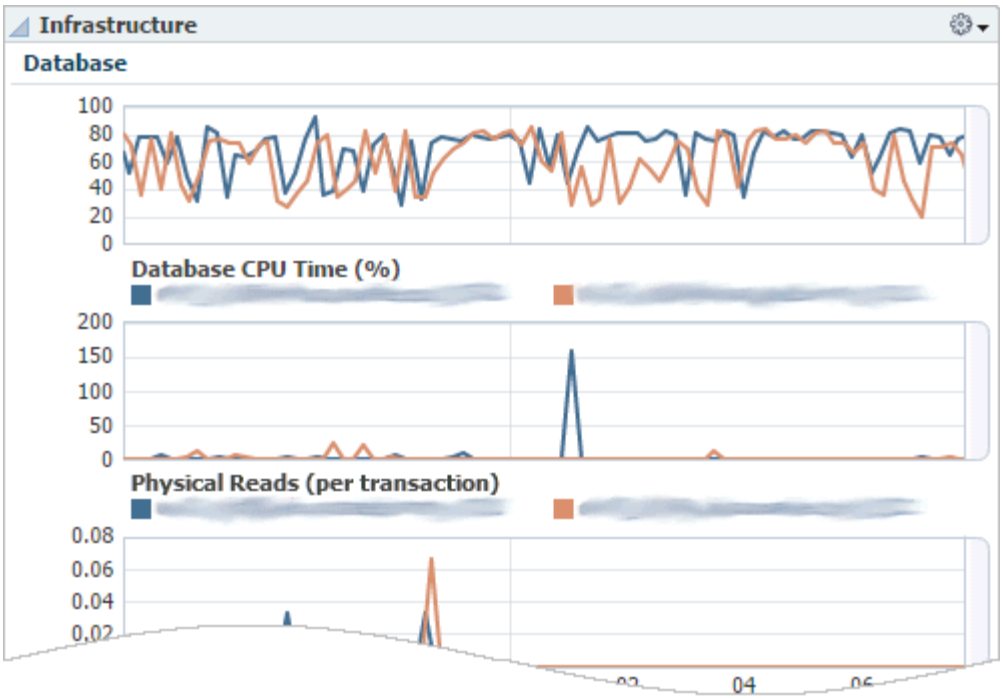
## About the Infrastructure Region

The Infrastructure region helps you assess the health and performance of your system's infrastructure components.

This region, as shown in part in Figure 8–6, displays the following information:

- The JVM heap usage and number of garbage collector invocations over time.
- The host CPU and memory usage over time.
- The database CPU usage, the number of times the database is queried for each transaction, and number of rollbacks over time. These graphs will also show any associated Oracle Real Application Clusters databases that you have discovered.

*Figure 8–6 Infrastructure Region of the Dashboard Tab*




You can use this region to identify whether the JVM, host, or database is causing performance issues. For example, high numbers of physical database reads can indicate problems with your execution plan, such as the database performing full table scans, and high numbers of rollbacks can indicate high numbers of transaction failures.

## About the Metrics by Server, Order Type, and Cartridge Tabs

The **Metrics by Server**, **Metrics by Order Type**, and **Metrics by Cartridge** tabs display information pertaining to managed servers, order types, and cartridges respectively. All three tabs include the following regions that show the information for each managed server, order type, or cartridge:

- **Order Throughput**: Shows the number of created, completed, and failed orders and a graph of the order creation rates.
- **Task Throughput**: Shows the number of created, completed, and failed tasks and a graph of the task creation rates.
- **Order Metrics**: Shows the number of orders in various states, the average and maximum number of order items per order, the number of orders created in the failed state, and the number of orders that failed on creation.
- **Order Lifecycle Times**: Shows the number and percentage of orders with lifecycle times ranging from 0 seconds to 90 days.

The **Metrics by Server** tab includes the following additional regions:

- **JVM**: Identical to the JVM area of the Infrastructure region on the **Dashboard** tab. See "About the Infrastructure Region".
- **Availability**: Identical to the Availability of Managed Servers for Last 24 Hours area of the System Availability region on the **Dashboard** tab. See "About the System Availability Region".

The **Metrics by Order Type** tab includes the following additional region:

- **Order Items per Order**: For each order type, shows the number of order items in ranges from 0 to greater than 5000.

You can use these tabs to assess the throughput and health of individual servers, order types, and cartridges, and identify whether a particular server, order type, or cartridge is causing problems.

## About the Monitoring Home Page for OSS Application Targets

You can monitor the health and performance of OSS application targets on the target home page. OSS application targets include UIM, ASAP, and OSM nodes.

The home page for an OSS application target provides metric data that you can use to monitor availability, alerts, and performance. See "Viewing Home Pages" for information about accessing home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Figure 8–7 shows the regions on the home page for an OSS node target.

***Figure 8–7 OSS Application Target Home Page***

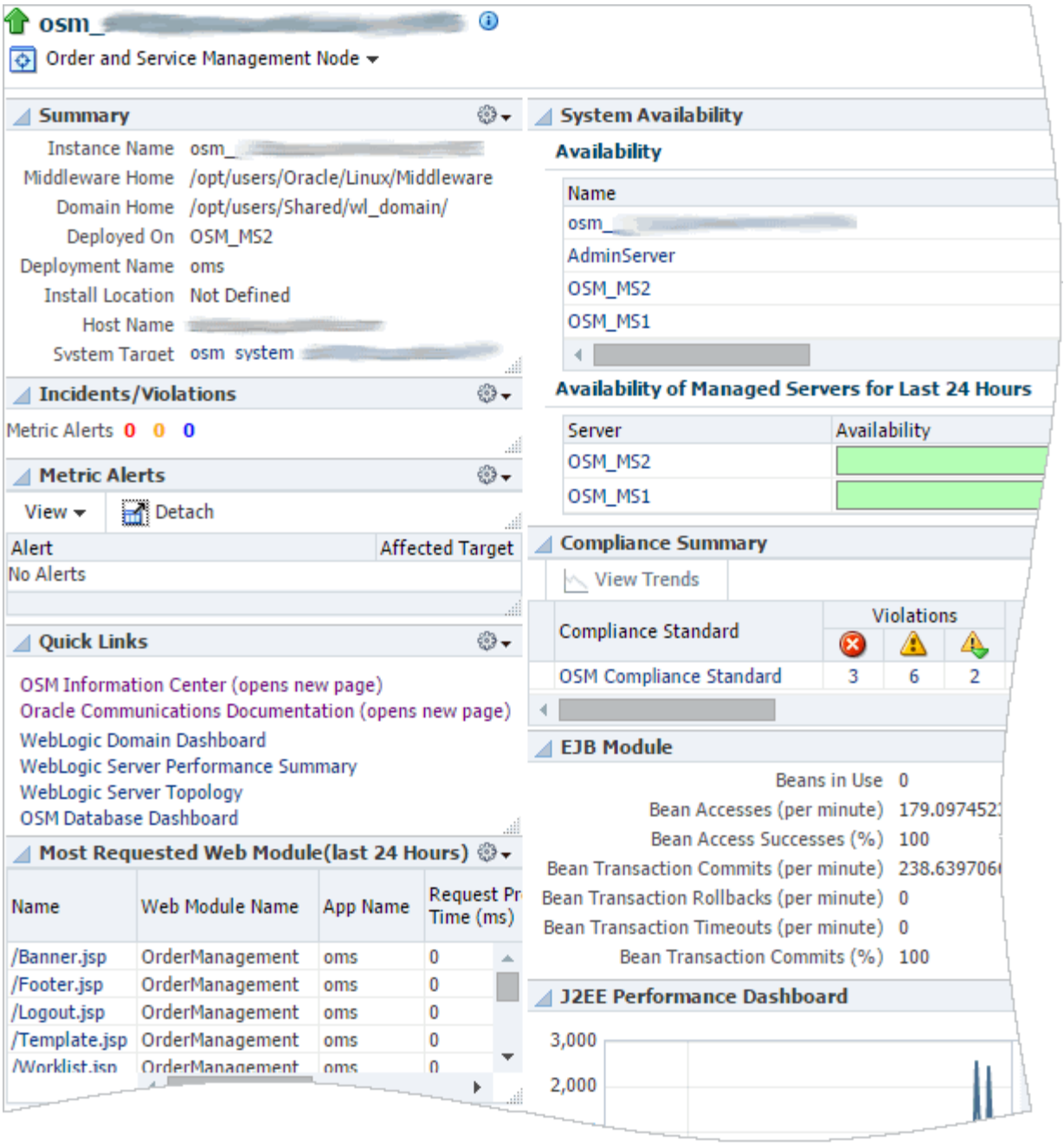



Table 8–2 describes the regions on the home page for OSS application targets.

***Table 8–2 Common Regions on OSS Application Home Pages***

| Region | Description |
|---|---|
| Summary | Displays summary information about the target, including paths to Middleware and domain homes, the installation location, and the server, host, and system target to which the application is deployed. |
| Incidents/Violations | Displays the number of critical, warning, and escalated metrics alerts. |

*Table 8–2 (Cont.) Common Regions on OSS Application Home Pages*

| Region | Description |
|---|---|
| Metric Alerts | Displays details about metrics alerts affecting the target. |
| Quick Links | Provides links to related Enterprise Manager Cloud Control pages, such as performance data, WebLogic Server and domain pages, and database pages. See "About the Quick Links Region" for descriptions of each link on OSM node and system pages. |
| Most Requested Web Modules | Displays information about the most requested web modules over the last 24 hours, including the number and processing time of requests and the number of times the module was reloaded, since startup and by the minute. |
| System Availability | Displays information about the availability of servers related to the target, currently and over the last 24 hours. |
| Compliance Summary | Displays displays a summary of compliance evaluations, violations, and scores for the OSM node. Only appears for OSM nodes.<br>See "Managing OSM Compliance" for more information about managing OSM compliance and using the Enterprise Manager Cloud Control compliance tools. |
| EJB Module | Displays summary information about Enterprise JavaBeans, including their use and access, and their transaction commits, rollbacks, and timeouts. |
| J2EE Performance Dashboard | Displays graphs showing J2EE performance by the number and processing time of requests, the number of active sessions, heap usage, and active threads. |

You can see a full list of metrics collected for an OSS application target and you can monitor the data that an individual metric collects for the target. See "Viewing Target Metrics" for information about accessing the list of metrics.

## Managing OSM Compliance

Application Management Pack for Oracle Communications provides the OSS Compliance Framework, which you can use to evaluate whether your OSM configuration conforms to Oracle's recommendations.

The OSS Compliance Framework lets you ensure that the node targets in your OSM production systems are configured consistently across multiple systems and environments. You can use the provided framework to create a similar framework if, for example, the configuration of your production system differs from that of your development system.

Monitoring compliance helps you prevent problems or identify their source. When problems occur, you can determine if your configuration is the cause by verifying whether your configuration conforms to Oracle's recommendations, identifying recent changes to configurations, and comparing the configuration of different environments.

Application Management Pack for Oracle Communications extends the compliance frameworks and features of Oracle Enterprise Manager Cloud Control. For detailed information about managing compliance in Enterprise Manager Cloud Control, including information about creating and applying custom compliance standards, suppressing violations, and to see examples, see the chapter about managing compliance in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

For information about OSM compliance rules, see *Oracle Communications Order and Service Management System Administrator's Guide*.

## About the OSS Compliance Framework

The OSS Compliance Framework consists of the following compliance standards:

- **OSM Compliance Standard**: Defines compliance rules applicable to OSM node targets.
- **OSM Compliance Standard - WebLogic Patches**: Defines compliance rules applicable to WebLogic Server domain targets. The rules evaluate whether the appropriate patches for OSM have been applied to the WebLogic Server domains.

The compliance rules that make up these standards are based on Oracle product documentation, product uses, best practices, and guidelines. Because this framework and its associated standards and rules are system-defined, you cannot edit or delete them.

The OSS Compliance Framework is intended for OSM production systems. If your configuration differs for development or test systems, you can copy the system-defined framework and use it as the basis for your own framework. See the discussion of creating like a compliance framework in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for more information about creating a copy of a system-defined framework.

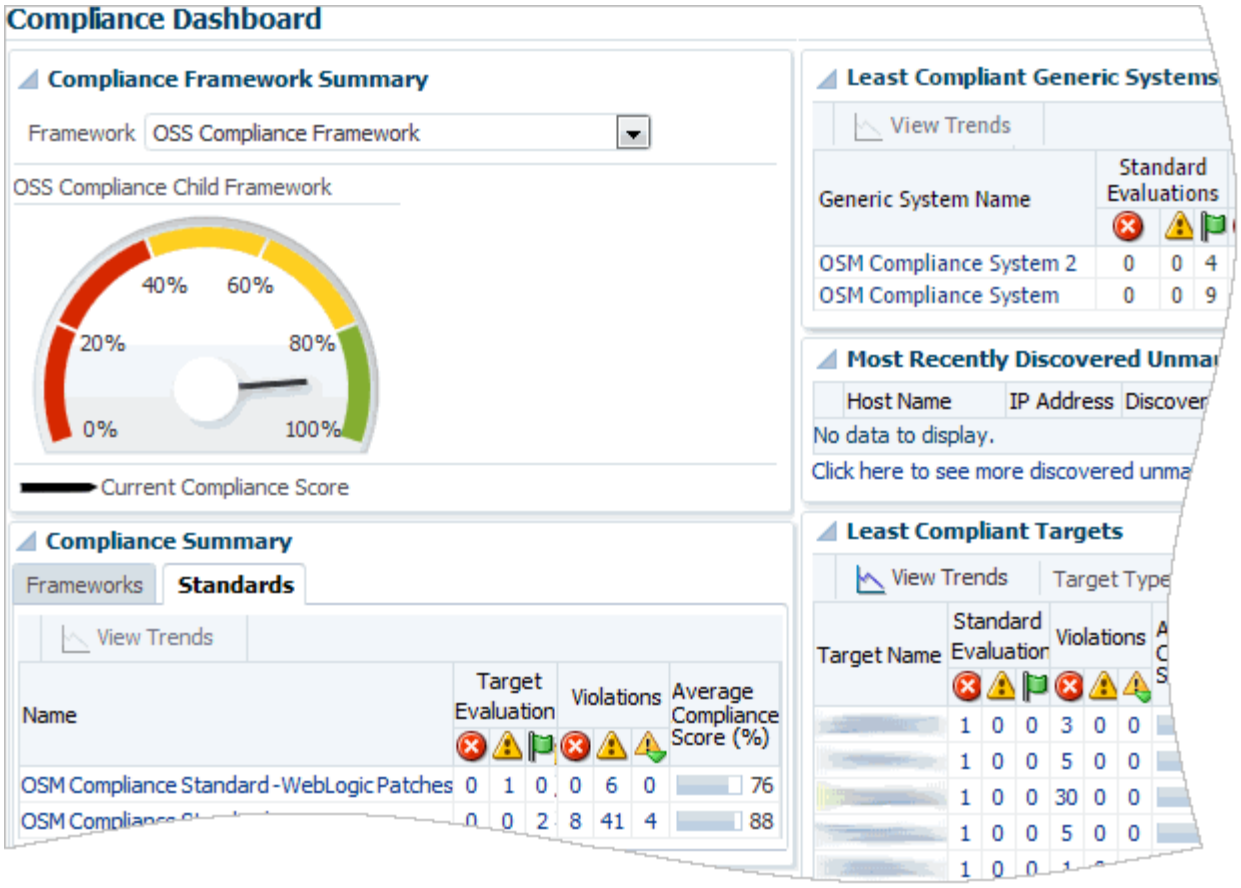
## About Monitoring OSM Compliance

Enterprise Manager Cloud Control evaluates targets against compliance rules and provides a compliance score, describes any violations, and recommends corrective actions.

This section provides an overview of the Enterprise Manager Cloud Control pages used to monitor compliance. Accessing and using these pages is described in "Monitoring OSM Compliance".

For an overall view of the compliance for all the targets associated with the standards within the OSS Compliance Framework, you use the Compliance Dashboard, shown in Figure 8–8.

***Figure 8–8 Compliance Dashboard***




You can use the Compliance Dashboard to:

- Determine the overall compliance of all targets by reviewing the compliance score for an entire framework.
- Identify which standard contains the most violations by reviewing the compliance summary for both standards.
- Compare the compliance scores, evaluations, and violations of different OSM systems.
- Identify the targets that need the most attention by reviewing the list of least compliant targets.

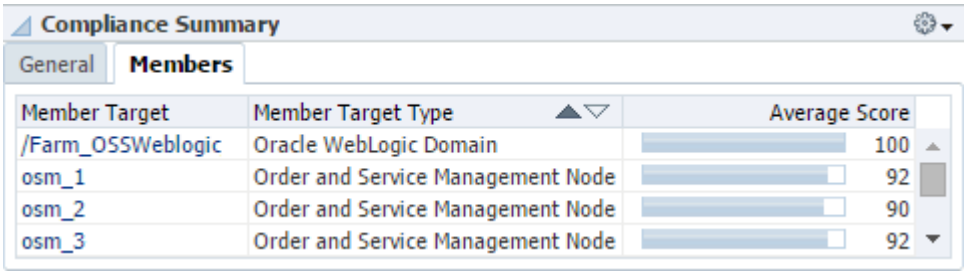
For details about the results of the compliance evaluations, you use the Compliance Results pages. You can use these pages to:

- Review results for an entire framework, for an individual standard, and an individual target.
- See a full list of compliance rules included in a framework or standard, with icons indicating any violations.
- Get details about violations and see tips for how to resolve them.
- Monitor compliance trends over time.

For a view of the compliance of an entire OSM system, you create a generic system target that includes the OSM nodes and WebLogic Server domain that are in that system. You can then monitor the compliance of the OSM system from the generic

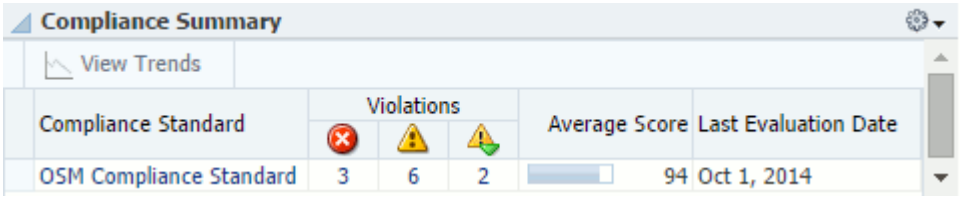
system's home page. The Compliance Summary region, shown in Figure 8–9, provides an overall compliance score for the entire generic system, and an individual score for each member of the system.

***Figure 8–9 Compliance Summary Region for a Generic System***




For a finer view of the compliance of an individual OSM node, you can use the OSM node target's home page. The Compliance Summary region, shown in Figure 8–10, provides a summary of compliance evaluations, violations, and scores for the selected OSM node.

***Figure 8–10 Compliance Summary Region for an OSM Node***




From the OSM node target's home page, you can also access more details about the violations and standards, or access the compliance evaluation results for that target.

See *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for detailed information about accessing compliance features and using the compliance dashboard and results pages effectively.

## Monitoring OSM Compliance

Monitoring OSM compliance includes the following tasks:

- (Optional) Viewing the OSM Compliance Standards and Rules
- (Optional) Creating Generic Systems for Monitoring OSM System Compliance
- Associating the Compliance Standards with Targets
- Monitoring OSM Compliance Summary and Results

### Viewing the OSM Compliance Standards and Rules

You can view the OSM compliance standards and the rules that they include at any time, whether or not you have associated them with targets.

To view the OSM compliance standards and the rules that they include:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. From the **Enterprise** menu, select **Compliance,** and then **Library**.

3. Do any of the following:
   - To view the list of rules within the OSM compliance standards, and view details about individual rules:
     a. Click the **Compliance Standards** tab.
     b. In the Search region, in the **Compliance Standard** field, enter **OSM Compliance Standard** and click **Search**.
     c. From the list of compliance standards, select the link for one of the OSM compliance standards.
     d. Select a rule from the list and review information about it, including a description of the rule and its definition.
   - To view details for all rules that apply to OSM nodes:
     a. Click the **Compliance Standard Rules** tab.
     b. In the Search region, from the **Applicable To** list, select **Order and Service Management Node**.
     c. From the **System-Defined** menu, select **Yes**.
     d. Click **Search**.

        All system-defined rules that can apply to OSM node targets appear. Review the details for the rules. The descriptions of all the rules are displayed on one page.
     e. To view more details about a rule, including the rule's definition and rationale, click its name.
   - To view details for all rules that apply to WebLogic Server domains:
     a. Click the **Compliance Standard Rules** tab.
     b. In the Search region, from the **System-Defined** menu, select **Yes**.
     c. From the **Applicable To** list, select **Oracle WebLogic Domain**.
     d. In the **Keywords** field, enter **Patch**.
     e. Click **Search**.

        All system-defined rules with the **Patch** keyword that can apply to WebLogic Server domain targets appear. Review the details for the rules. The descriptions of all the rules are displayed on one page.

        **Note:** The list may include some rules that are not part of the OSM WebLogic patches standard. To determine which rules are part of the OSM WebLogic patches standard, review the list of rules accessible from the **Compliance Standards** tab.

     f. To view more details about a rule, including the rule's definition and rationale, click its name.

### Creating Generic Systems for Monitoring OSM System Compliance

Because the OSM Compliance Standard is evaluated against OSM node targets rather than OSM system targets, you must create generic systems to be able to monitor the compliance of OSM systems as a whole.

You must create the generic systems before associating the compliance standards with the node targets.

To create a generic system for monitoring OSM system compliance, perform the following steps for each OSM system for which you want to monitor compliance:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. From the **Setup** menu, select **Add Target**, and then **Generic System**.

   The Add Target page for creating a generic system appears.
3. In the **Name** field, enter a unique name identifying the generic system as a compliance monitoring system. For example, **OSM Compliance System**.
4. In the Members region, click **Add**.

   The **Select Targets** dialog box appears.
5. From the **Target Type** menu, select the **Order and Service Management Node** and **Oracle WebLogic Domain** options.
6. From the list of targets, select all of the OSM nodes that belong to a single system, and select the domain on which that system is deployed. Hold down the CTRL key while clicking to select multiple targets.
7. Click **Select**.
8. Click **Next**.

   The Define Associations page appears.
9. Click **Next** without defining any associations.

   The Availability Criteria page appears.
10. In the Key Members region, click the double arrow icon to move all of the node targets from the Members list to the Key Members list.
11. Click **Next**.

    The Charts page appears.
12. (Optional) Add, edit, or remove charts. The charts specified here appear on the Charts page for the generic system, which you can access from the target type menu on the generic system's home page. You can use the charts to monitor performance data for the system.
13. (Optional) To review your generic system configuration, click **Next**.

    The Review page appears.
14. Click **Finish**.

    The generic system is created and the Systems page appears, showing the list of generic systems.

### Associating the Compliance Standards with Targets

If you want to monitor compliance at the system level, you must create generic systems as described in "Creating Generic Systems for Monitoring OSM System Compliance" before completing this procedure.

To associate the OSM compliance standards with OSM node and WebLogic Server domain targets:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. From the **Enterprise** menu, select **Compliance,** and then **Library**.
3. Click the **Compliance Standards** tab.
4. In the Search area, in the **Compliance Standard** field, enter **OSM Compliance Standard** and click **Search**.
5. From the list of compliance standards, highlight **OSM Compliance Standard** and click the **Associate Targets** button.
6. Click the **Add** button.
7. Select the OSM node targets for which you want to evaluate compliance and click **Select**.
8. Click **OK**.

   The compliance standard is associated with the OSM node targets.
9. From the list of compliance standards, highlight **OSM Compliance Standard - WebLogic Patches** and click the **Associate Targets** button.
10. Click the **Add** button.
11. Select the WebLogic Server domain target on which the OSM targets are deployed and click **Select**.
12. Click **OK**.

    The compliance standard is associated with the WebLogic Server domain targets.

### Monitoring OSM Compliance Summary and Results

To monitor compliance results:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. To view the compliance summary for all targets associated with compliance standards:
   a. From the **Enterprise** menu, select **Compliance,** and then **Dashboard**.

      The Compliance Dashboard page appears.
   b. From the **Framework** menu, select **OSS Compliance Framework**.

      The overall score for the OSS Compliance Framework appears.
   c. In the Least Compliant Targets region, from the **Target Type** menu, select the **Order and Service Management Node** and **Oracle WebLogic Domain** options, and then click anywhere outside the menu.

      The table shows only OSM nodes and WebLogic Server domains.

      **Note:** Some domains that appear may not be domains on which OSM is deployed.

   d. Review the regions for summary information about the generic systems, targets, and standards.

3. View the results of evaluating targets against the rules of the OSS Compliance Framework:
   a. From the **Enterprise** menu, select **Compliance,** and then **Results**.

      The Compliance Results page appears.

   b. Do one of the following:
      – On the **Compliance Standards** tab, click an OSM compliance standard.
      – Click the **Compliance Framework** tab, and then click **OSS Compliance Framework**.

      The results for the OSS Compliance Framework or OSM compliance standard appear.

   c. Review the **Summary**, **Trend Overview**, and **Violations** tabs for information about targets associated with the standard.

   d. To view information about an individual rule, navigate to the rule in the tree at the left of the Compliance Result Page.

4. If you created generic systems to monitor compliance for OSM systems, view the compliance summary and results for a generic system that includes OSM node targets:
   a. From the **Targets** menu, select **Systems**.

   b. From the list of systems, select a generic system that you created for monitoring OSM system compliance.

      The home page for the generic system appears.

   c. Review the information in the Compliance Summary region.

   d. From the target type menu under the target's name, select **Compliance**, and then **Results**.

      The Compliance Results page for the generic system appears, showing the results of evaluating the targets that are members of the system against the rules in the standards to which the members are associated.

   e. Review the results on the **Compliance Frameworks**, **Compliance Standards**, and **Target Compliance** tabs.

5. View the compliance summary and results for a single OSM node target:
   a. From the **Targets** menu, select **All Targets**.

   b. In the Target Type tree, select **Order and Service Management Node**.

   c. In the list of targets, click the name of the target for which you want to view the compliance summary.

      The target's home page appears.

   d. Review the information in the Compliance Summary region.

   e. From the target type menu, select **Compliance**, and then **Results**.

      The Compliance Results page for the target appears, showing the results of evaluating the target against the rules in the standards to which the target is associated.

   f. Review the results on the **Compliance Frameworks**, **Compliance Standards**, and **Target Compliance** tabs.

See *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for detailed information about accessing compliance features and using the compliance dashboard and results pages effectively.

# Operations Support Systems Collection Items and Metrics

This section describes the general collection items and metrics for OSS targets and for the collection items and metrics specific to UIM targets. The collection items and metrics specific to OSM systems are displayed on the OSM system target's home page, as described in "About the Monitoring Home Page for OSM System Targets".

See "About Conditions that Trigger Notifications" for an explanation of the entries in the tables included in this section.

Application Management Pack for Oracle Communications provides default thresholds for critical collection items and metrics. You can customize the thresholds and add thresholds and alerts for collection items and metrics that have no default thresholds. See "Configuring Metric Monitoring Thresholds and Alerts" for more information about configuring thresholds.

## General Operations Support Systems Collection Items

This section describes collection items and metrics that apply to all OSS targets. View the data provided by these metrics in the OSS target's home page.

### CollectionItem: Response

Operations Support Systems targets have a Response Status collection item that provides target connection status. The Response Status is either up or down.

The Management Agent checks the Response Status at a default interval of every minute. Enterprise Manager Cloud Control administration console displays a message indicating whether the Operations Support Systems node is either up or down. Table 8–3 describes the condition that triggers an alert.

***Table 8–3 Operations Support Systems Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| Status | EQ | NA | 0 | 0 | NA |

### CollectionItem: deployment_overview

This collection item collects deployment data for an Operations Support System for Enterprise Manager Cloud Control monitoring at a default interval of every 5 minutes.

There are no conditions for this collection item.

### CollectionItem: deployment_ejb_module

This collection item collects deployed Enterprise JavaBean data for Enterprise Manager Cloud Control monitoring at a default interval of every 60 minutes.

There are no conditions for this collection item.

See the discussion of EJB module metrics in *Oracle Enterprise Manager Oracle Fusion Middleware Metric Reference Manual* for more information about monitored EJB collection items.

### CollectionItem: JMS Server Metrics

This collection items collects deployed Java Message Service data for Enterprise Manager Cloud Control monitoring at a default interval of every 60 minutes. The following JMS metrics are collected for Operations Support Systems:

- JMSConsumerRuntime
- JMSRuntime
- JMSDestinationRuntime

There are no conditions for this collection item.

See the discussion of JMS server metrics in *Oracle Enterprise Manager Oracle Fusion Middleware Metric Reference Manual* for more information about monitored JMS collection items.

### CollectionItem: JVM Metrics

These collection items collects deployed Java Virtual Machine data for Enterprise Manager Cloud Control monitoring at a default interval of every 15 minutes. The following JVM metrics are collected for Operations Support Systems:

- jvm_memory_pools
- jvm_garbage_collectors
- jvm
- jvm_compilation_time

There are no conditions for this collection item.

See the discussion of JVM metrics in *Oracle Enterprise Manager Oracle Fusion Middleware Metric Reference Manual* for more information on monitored JVM collection items.

### CollectionItem: servlet_jsp

This collection item collects deployed Java Servlet Pages data for Enterprise Manager Cloud Control monitoring at a default interval of every 60 minutes.

There are no conditions for this collection item.

See the discussion of servlet/JSP metrics in *Oracle Enterprise Manager Oracle Fusion Middleware Metric Reference Manual* for more information on monitored servlet/JSP collection items.

## UIM Collection Items

This section describes collection items and metrics that are specific to UIM. View the data provided by these metrics on the communications suite target home page.

### CollectionItem: uim_services_summary

This collection item collects services summary data for Enterprise Manager Cloud Control monitoring at a default interval of every 60 minutes.

There are no conditions for this collection item.

### CollectionItem: uim_cartridges

This collection item collects information about UIM cartridges deployed in a target at a default interval of every 60 minutes.

There are no conditions for this collection item.

# 9

# Monitoring Oracle Communications Integrations

This chapter describes how to monitor Oracle Communications Integration targets in Enterprise Manager Cloud Control using the home page provided by Oracle Application Management Pack for Oracle Communications.

It also describes the Oracle Communications Integration monitoring collection items and metrics provided by Oracle Application Management Pack for Oracle Communications.

## About Monitoring Integrations

Integration targets represent Oracle Application Integration Architecture (Oracle AIA) Oracle Communications Pre-Built Integrations deployed on Oracle Service Oriented Architecture (SOA).

Application Management Pack for Oracle Communications lets you monitor Integration targets using Oracle Enterprise Manager Cloud Control. A Management Agent monitors targets for collection items and metrics and sends the data to the Management Server for presentation.

You must install and deploy the Application Management Pack for Oracle Communications plug-in on both your Management Server and host agents before monitoring Integration targets.

See the following chapters for information about setting up Oracle Communications application monitoring with Enterprise Manager Cloud Control:

- Installing Application Management Pack for Oracle Communications
- Configuring Oracle Communications Targets
- Managing Communications Applications with Enterprise Manager Cloud Control

### About the Monitoring Home Page for Integrations

The home page for Integration targets displays summary information and metrics data that you can use to monitor the health and performance of your integration. See "Viewing Home Pages" for information about accessing home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Figure 9–1 shows the regions on the home page for an Integration target.

***Figure 9–1 Integration Target Home Page***

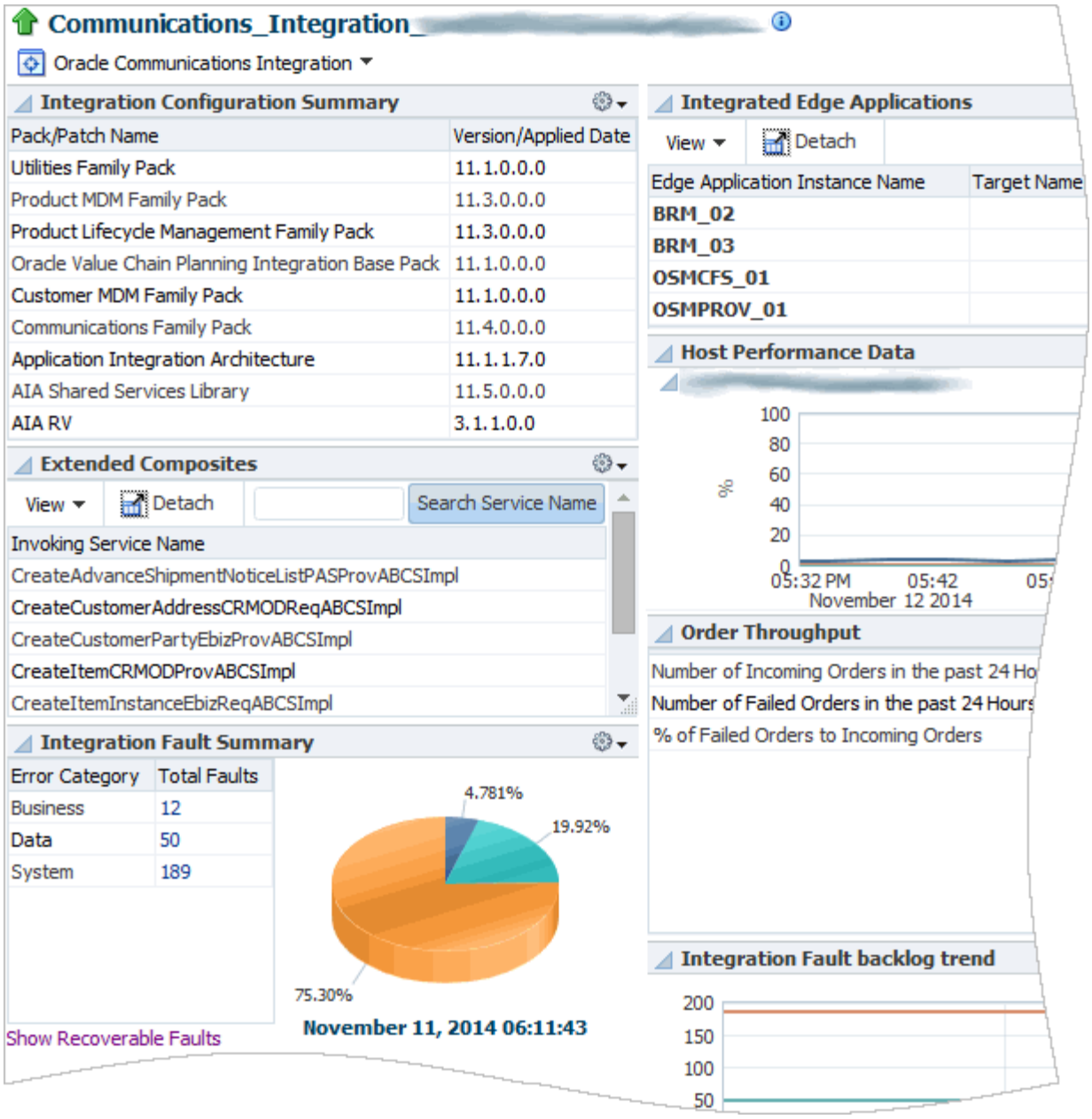



Table 9–1 describes the regions shown in the home page for Integration targets.

***Table 9–1 Regions on the Integration Home Page***

| Region | Description |
|---|---|
| Integration Configuration Summary | Displays version numbers and dates for Oracle AIA and SOA integration packs and patches. |
| Extended Composites | Lists the service composites configured for Oracle AIA in alphabetical order. You can filter the list by searching for a particular service name. |

*Table 9–1 (Cont.) Regions on the Integration Home Page*

| Region | Description |
|---|---|
| Integration Fault Summary | Displays the total number and percentage of business, system, and data faults.<br>Use this region to identify and resolve faults.<br>You can click the links in the Total Faults column to see a list of faults and their details, and use the arrows in the list to see the SOA trace instance for the fault.<br>You can click the **Show Recoverable Faults** link to go to the SOA infrastructure target home page where you can recover from faults in bulk. See "Viewing and Recovering from Faults" for more information. |
| Integrated Edge Applications | Provides the status of the BRM and OSM instances that the Integration target integrates.<br>You can use this region to add a monitoring agent and configure automatic discovery for the integrated applications. See "Configuring Integrated Applications for Status Monitoring" for more information. |
| Host Performance Data | Displays performance information for the host on which SOA and Oracle AIA are deployed, including CPU and memory use.<br>Use this region to determine whether a particular host is causing problems by identifying fluctuations in host performance. |
| Order Throughput | Displays the number of incoming and failed orders for the last 24 hours in a list and a graph.<br>Use this region to identify failed order backlogs or to determine if increased numbers of incoming orders are causing performance problems. |
| Integration Fault Backlog Trend | Displays a graph of the total number of backlogged errors over time. |

You can see a full list of metrics collected for an Integration target and you can monitor the data that an individual metric collects for the target. See "Viewing Target Metrics" for information about accessing the list of metrics.

# Configuring Integrated Applications for Status Monitoring

After you have discovered an Integration target, you can monitor the status of the applications that the target integrates from the target's home page.

You can monitor the status of integrated applications that have been discovered and promoted as targets in Enterprise Manager Cloud Control, and configured on the Integration target's home page.

To configure the integrated applications for status monitoring, repeat the following steps for each application listed in the Integrated Edge Applications region:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. From the **Targets** menu, select **All Targets**.
3. In the Target Type tree, select **Oracle Communications Integration**.
4. From the list of targets, select the Integration target you want to monitor.

5. In the Integrated Edge Applications region, select an application row and click **Configure Edge Application Details**.
6. In the **Hostname** field, enter the host on which the application is deployed.
7. In the **PinUser/Port** field, enter one of the following:
   - For BRM, enter the user name for the BRM host.
   - For OSM, enter the port for the OSM server.
8. Click **Submit**.

   The application's name appears as a link to the application's target home page, and its status is shown. For OSM targets, the status is a green Up arrow or a red Down arrow. Because BRM targets consist of many components, some of which may be up or down, the status is always **n/a**.

If the **Add Agent** or **Discover Edge Application** link appears beside the target name, you have not installed a Management Agent on the integrated application's host or discovered the application. To monitor the integrated application's status from the Integration target's home page, do the following:

- If the **Add Agent** link appears, click the link to go to the Add Targets Manually page. You must perform the following tasks:
  a. Add the host target and agent as described in "Adding Host Targets Manually and Installing the Management Agent".
  b. Discover and promote the edge applications as described in "Adding Oracle Communications Targets".
- If the **Discover Edge Application** link appears, click the link to go to the Setup Discovery page for configuring automatic discovery. You must discover and promote the integrated application as described in "Discovering Targets Automatically".

# Viewing and Recovering from Faults

You can view lists of faults from the Integration target home page, and recover from some system faults from the SOA infrastructure target home page.

## Viewing Faults

To view lists of faults and their details:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. From the **Targets** menu, select **All Targets**.
3. In the Target Type tree, select **Oracle Communications Integration**.
4. From the list of targets, select the Integration target for which you want to view faults.
5. In the Total Faults column in the Integration Fault Summary region, select one of the number of business, data, or system faults links.

   The fault list page with summary information about the faults appears.
6. In the first column of the table, next to an individual fault, click the arrow icon.

The Trace Instance page appears for that fault. This page provides detailed information about all faults associated with the same Execution Context ID (ECID).

### Recovering from System Faults

To recover from system faults:

1. Log in to the Enterprise Manager Cloud Control administration console as a privileged user.
2. From the **Targets** menu, select **All Targets**.
3. In the Target Type tree, select **Oracle Communications Integration**.
4. From the list of targets, select the Integration target for which you want to recover from system faults.
5. In the Integration Fault Summary region, click **Show Recoverable Faults**.

   The home page appears for the SOA infrastructure target to which the Integration target is deployed.
6. Click the **Faults and Rejected Messages** tab.
7. In the Search panel, set the search criteria. Ensure that you select **Recoverable** from the **Fault** list.
8. Click **Search**.
9. In the Faults and Rejected Messages table, select up to 5 faults.
10. From the **Recovery Options** menu, select a recovery action.

    A message is displayed indicating whether the recovery job can be submitted successfully.
11. Click **OK**.

    The fault recovery job is run.
12. To verify that the recovery job was successful, set the same search criteria and click **Search**.

    The faults for which you selected a recovery action do not appear if the recovery job was successful.

See the chapter about discovering and monitoring the SOA suite in *Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide* and the Enterprise Manager Online Help for more information about instance tracing and managing faults.

## Integration Collection Items and Metrics

This section describes the collection items and metrics collected for Integration targets.

See "About Conditions that Trigger Notifications" for an explanation of entries and tables included below.

Application Management Pack for Oracle Communications provides default thresholds for critical collection items and metrics. You can customize the thresholds and add thresholds and alerts for collection items and metrics that have no default thresholds. See "Configuring Metric Monitoring Thresholds and Alerts" for more information about configuring thresholds.

## CollectionItem: Response

This collection item provides the connection status of the Integration target. The status is displayed as a green Up arrow or a red Down arrow beside the target name on the target's home page and in the list on the All Targets.

The Management Agent retrieves the Response Status at a default interval of every minute.

Table 9–2 describes the condition that triggers an alert.

***Table 9–2 Component Response Condition***

| Condition Column Name | Operator | Default Warning Threshold | Default Critical Threshold | Consecutive Number of Occurrences Preceding Notification | Alert Text |
|---|---|---|---|---|---|
| UpDown Status | EQ | NA | Down | 1 | NA |

## CollectionItem: Fault Details

This collection item provides the details about Oracle AIA faults. You can use these details to trace the faults across the Oracle AIA and SOA architecture.

The Management Agent retrieves the fault details at a default interval of every 24 hours.

There are no conditions for this collection item.

## CollectionItem: Fault Summary

This collection item provides the number of business, system, and data faults. You can use these numbers to track the backlog of faults over time.

The Management Agent generates the fault summary at a default interval of every 24 hours.

There are no conditions for this collection item.

## CollectionItem: Faulted Orders per 24 Hours

This collection item provides the number of faulted orders that passed through Oracle AIA in the last 24 hours. You can use this number in conjunction with the number of incoming orders to identify order backlogs.

The Management Agent retrieves the number of the faulted orders at a default interval of every 24 hours.

There are no conditions for this collection item.

## CollectionItem: Incoming Orders per 24 Hours

This collection item provides the number of orders that Oracle AIA received in the last 24 hours. You can use this number in conjunction with the number of faulted orders to identify order backlogs and to determine possible sources of performance fluctuation.

The Management Agent retrieves the number of received orders at a default interval of every 24 hours.

There are no conditions for this collection item.

## Metric: Deployments

This metric provides the list of applications that Oracle AIA integrates.

The Management Agent retrieves the list of applications at a default interval of every 24 hours.

There are no conditions for this collection item.

## Metric: Extensions

This metric provides the list of the extended composites that make up Oracle AIA.

The Management Agent retrieves the list of extended composites at a default interval of every 24 hours.

There are no conditions for this collection item.