Oracle® Application Management Pack for Oracle Communications

System Administrator's Guide

Release 13.1.1.1

E68286-01

April 2016

ORACLE®

Oracle Application Management Pack for Oracle Communications System Administrator's Guide, Release 13.1.1.1

E68286-01

Contents

3 Configuring Oracle Communications Targets

4 Managing Communications Applications with Enterprise Manager Cloud Control

5 Monitoring Billing and Revenue Management

6 Monitoring Elastic Charging Engine

7 Monitoring Network Charging and Control

8 Monitoring Offline Mediation Controller

9 Monitoring Pricing Design Center

10 Monitoring Operations Support Systems

11 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.

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.

Accessing 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.

Document Revision History

The following table lists the revision history for this guide:

Version	Date	Description
E68286-01	April 2016	Initial release.

1

Understanding Application Management Pack for Oracle Communications

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

Software Versions Covered in This Guide

The functionality described in this guide applies to Application Management Pack for Oracle Communications version 12.1.0.4 and version 13.1.1.1. Both releases include the same features, but 12.1.0.4 is compatible with Oracle Enterprise Manager 12c and 13.1.1.1 is compatible with Enterprise Manager 13c.

Overview of Application Management Pack for Oracle Communications

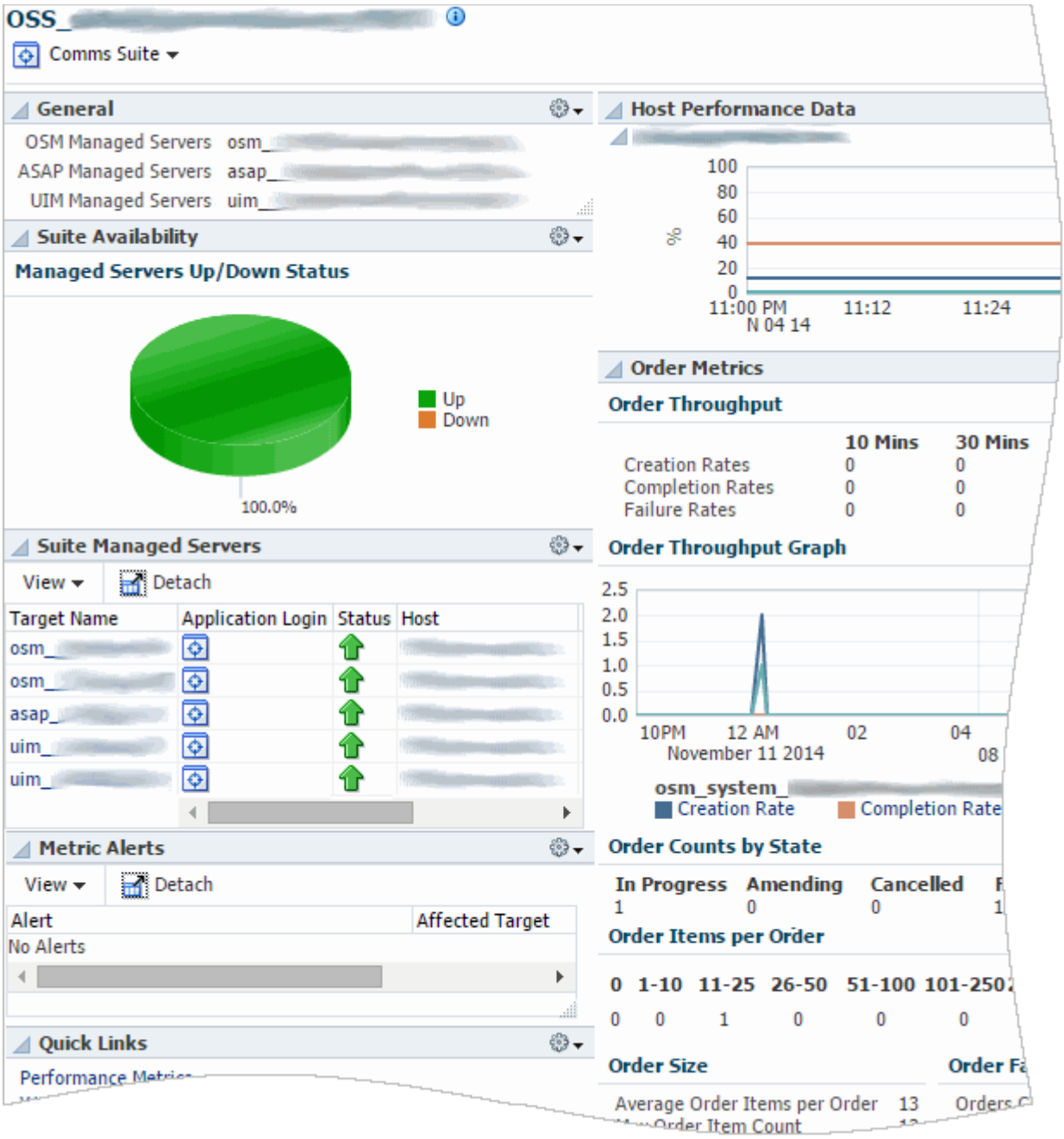
Application Management Pack for Oracle Communications is a plug-in for Oracle Enterprise Manager Cloud Control that provides management capabilities for supported Oracle Communications applications.

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.

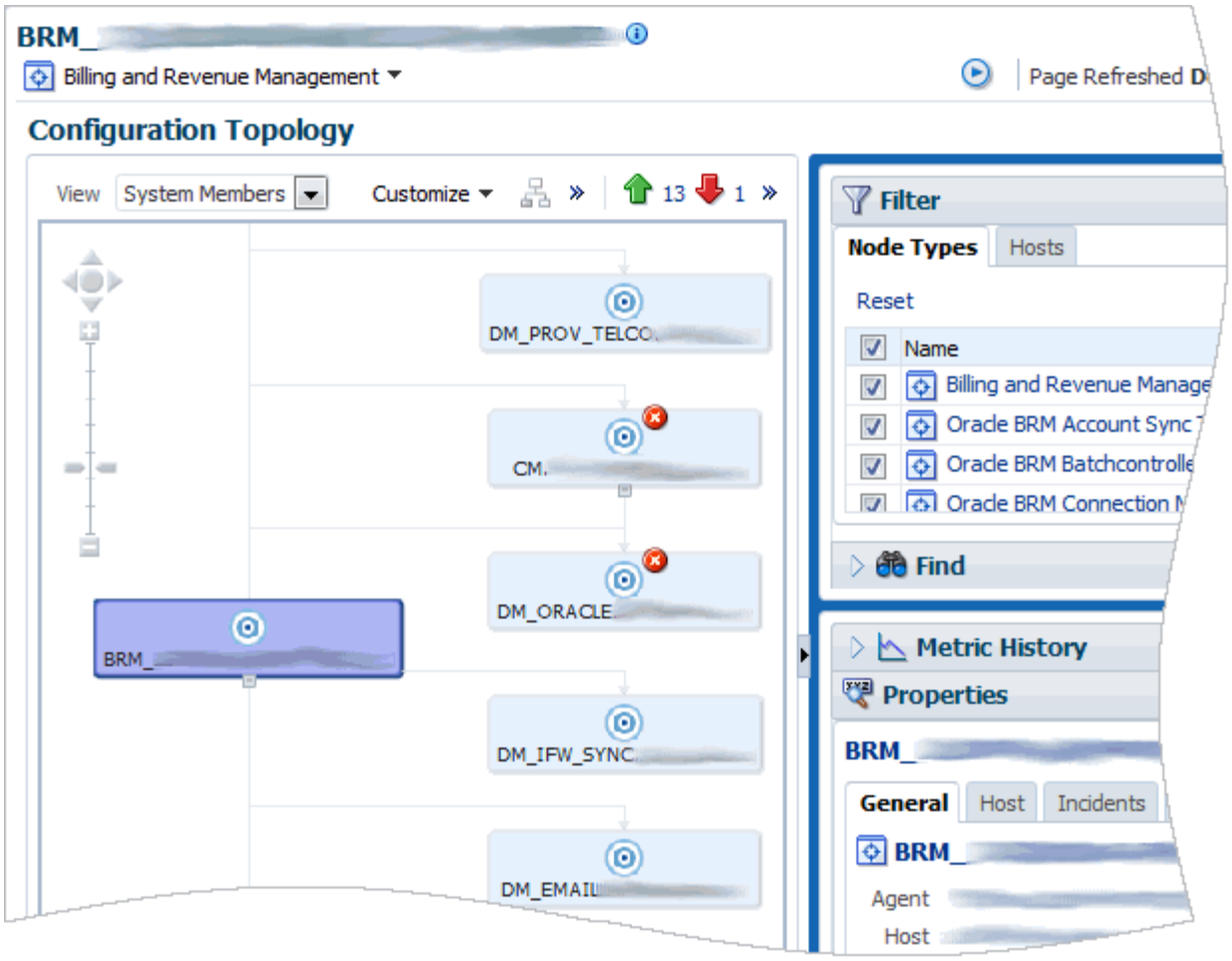
Application Management Pack for Oracle Communications also provides individual home pages for supported applications and application components.

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



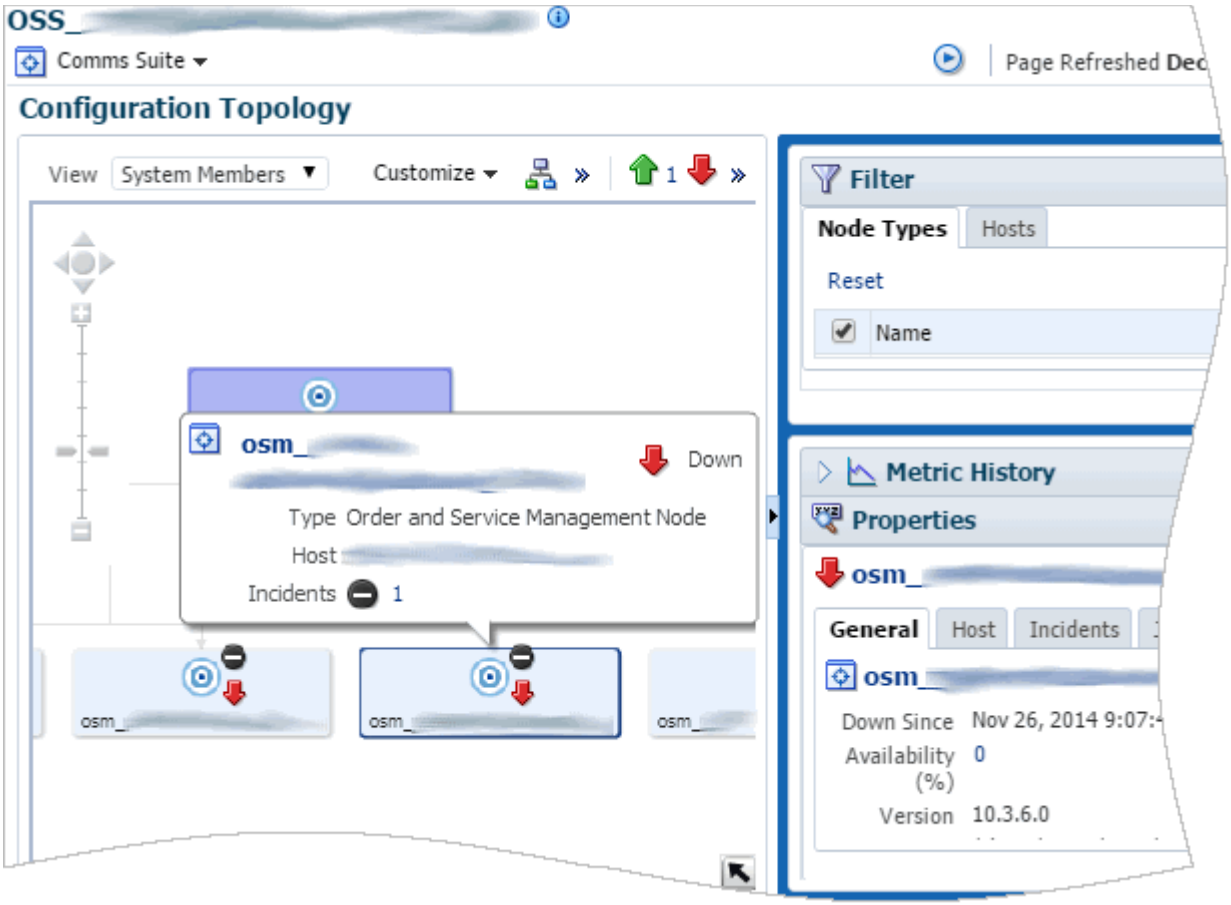
Application Management Pack for Oracle Communications displays managed Oracle Communications targets allowing you to view application, component, and host status. For example, view the topology of Oracle Communications Billing and Revenue Management (BRM) components such as the Connection Manager (CM)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

Figure 1–2 BRM Topology



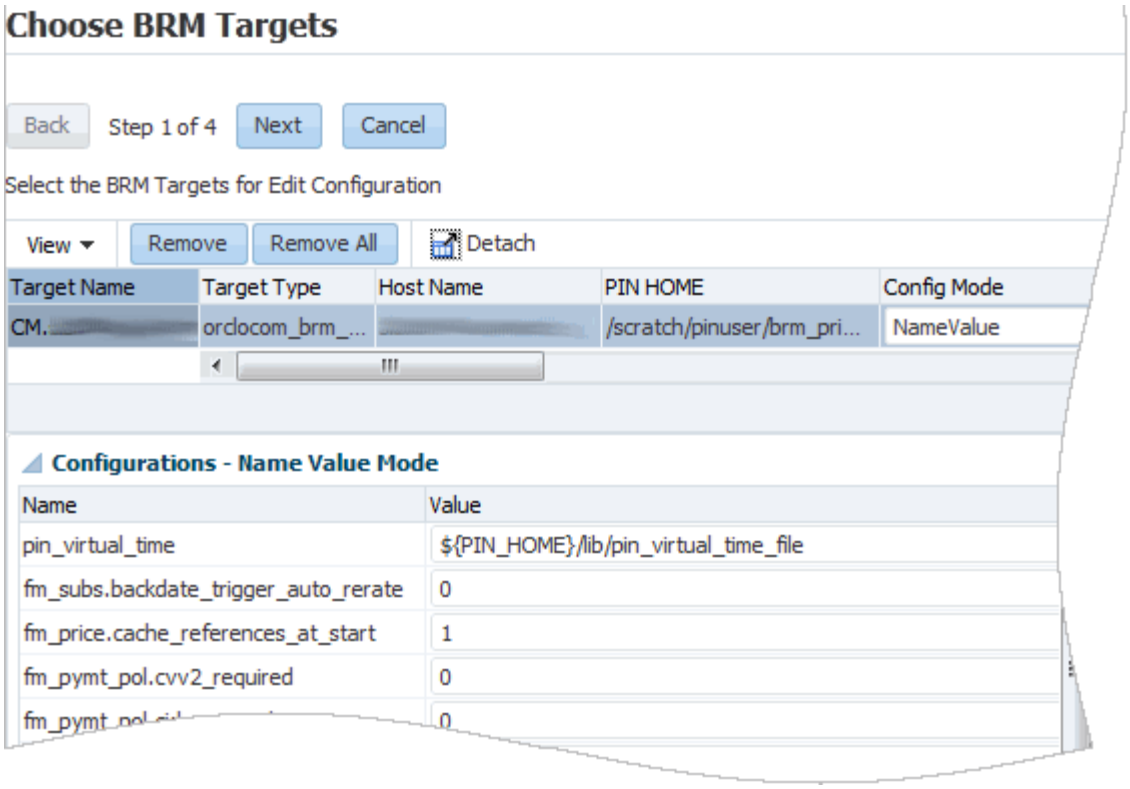
The configuration topology provides a visual representation of managed target relationships. Clicking on an element in the topology provides additional details in the Properties panel. Hovering over an element in the topology provides additional details as shown in Figure 1–3.

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 Features

Application Management Pack for Oracle Communications provides features that let you install, configure, and monitor Oracle Communications applications and infrastructure components from a centralized location.

- Application installation (called provisioning) includes:
  - Installing BRM in multischema environments with up to 9 schemas
  - Installing applications individually or as members of suites and solutions
  - Upgrading and patching BRM and rolling back applied patches
  - Upgrading BRM Pricing Design Center (PDC)
- Application monitoring includes:
  - Monitoring applications installed using Application Management Pack for Oracle Communications
  - Monitoring existing Oracle Communications applications installed independently of Application Management Pack for Oracle Communications
  - Monitoring groups of applications from a single landing page
  - Monitoring applications grouped by lifecycle status, such as development, testing, and production systems
  - Monitoring infrastructure components such as Oracle databases, Oracle WebLogic Server application servers, and Oracle Application Integration Architecture (Oracle AIA)

  - Viewing graphical representations of system topology for Oracle Communications applications
  - Monitoring in-depth order throughput and lifecycle metrics for OSM systems, servers, order types, and cartridges
  - Monitoring and comparing the compliance of OSM, UIM, and Oracle AIA installations with Oracle's recommended settings
  - Extending ready-to-use monitoring metrics by using metric extensions and monitoring templates
  - Sending notifications through multiple channels when configurable operating thresholds are reached by using metric-specific alerts and incident management for overall trends
  - Viewing log files
  - Recovering from faults
  - Identifying data inconsistency between applications integrated by Oracle AIA
- Application configuration includes:
  - Editing configuration properties for business support systems (BSS) applications
  - Comparing configurations of multiple applications, historical configurations for a single application, and overall system configuration by using configuration templates and drift management
  - Enforcing configuration policies across multiple installations of BRM, ensuring consistent versioning and configuration

Supported Applications, Suites, and Solutions

This section lists the applications, suites, and solutions for which Application Management Pack for Oracle Communications provides management capabilities.

Supported Applications

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

- BRM Application Management Pack, which licenses management for the following applications:
  - BRM
  - BRM Elastic Charging Engine (ECE)
  - BRM Pipeline Configuration Center (PCC)
  - Oracle Communications Network Charging and Control (NCC)
  - Oracle Communications Offline Mediation Controller
  - Oracle Communications Pricing Design Center (PDC)
  - Oracle AIA Oracle Communications Order to Cash Integration Pack for BRM
- OSM Application Management Pack, which licenses management for the following applications:
  - OSM

  - Oracle AIA Oracle Communications Order to Cash Integration Pack for OSM
  - Oracle AIA Oracle Communications Order to Cash Integration Pack for Oracle Configure, Price, and Quote (Oracle CPQ) Cloud
  - Oracle AIA Oracle Communications Order to Cash Integration Pack for Siebel customer relationship management (Siebel CRM)
- Application Management Pack for Oracle Communications, which licenses management for the following applications:
  - ASAP
  - UIM

Supported Suites

Application Management Pack for Oracle Communications lets you install and configure applications together in the following suite topologies:

- Oracle Communications Order to Cash: Includes ASAP, BRM, OSM, PCC, PDC, and UIM
- Oracle Communications OSS Fulfillment: Includes ASAP, OSM, and UIM

High-availability installation of these suites is also supported.

Supported Solutions

Application Management Pack for Oracle Communications helps monitor Oracle Communications Rapid Offer Design and Order Delivery (RODOD) solutions.

RODOD is a TM Forum certified solution that lets you design and provide offers rapidly and manage orders throughout their lifecycle. RODOD solutions include many of the applications that you can monitor and manage using Application Management Pack for Oracle Communications.

Application Management Pack for Oracle Communications supports RODOD solutions by enabling the following:

- Installing, monitoring, and configuring OSM and BRM
- Monitoring and configuring Oracle AIA
- Monitoring status and errors for Oracle Communications applications and supporting infrastructure components from a single landing page
- Resolving Oracle AIA errors
- Identifying inconsistency in data shared across integrated applications

Application Management Process Flow

Implementing and using Application Management Pack for Oracle Communications involves the following tasks:

1. Install Enterprise Manager Cloud Control and the Application Management Pack for Oracle Communications plug-in. See "Installing Application Management Pack for Oracle Communications".
2. Add the hosts on which your applications are deployed as managed targets in Enterprise Manager Cloud Control, deploy the Management Agent to the hosts, and set up preferred credentials for the hosts. See "Adding Host Targets Manually

and Installing the Management Agent" and "About Host Preferred Credentials".

3. Deploy Application Management Pack for Oracle Communications to the Enterprise Manager Cloud Control Management Server and the Management Agent on each host. See "Deploying the Application Management Pack for Oracle Communications Plug-In".
4. Set up the users and roles required to restrict access to your environment. See the discussion of access control points in *Application Management Pack for Oracle Communications Security Guide*.
5. Discover your existing applications using guided or automatic discovery, organizing them into functional groups during discovery. Discovered applications are called **targets**. See "Adding Oracle Communications Targets".
6. Extend the ready-to-use monitoring capabilities by using metric extensions and monitoring templates. See "Extending Monitoring Metrics".
7. Set up compliance management to monitor how well your targets comply with Oracle's recommendations. See "Managing Compliance".
8. For RODOD solutions, set up data discrepancy reports to help keep the data shared by RODOD applications consistent. See "Identifying Discrepancies in Shared Data".
9. Configure alerts and notifications for targets. See "Configuring Alerts".
10. Create dynamic groups to group targets. See "About Dynamic Groups".
11. Monitor targets by using the Oracle Communications Applications landing page, dynamic group home pages, target home pages, the compliance dashboard, and data discrepancy reports. See "Monitoring Oracle Communications Application Targets".

    For example, for RODOD targets, you can monitor:

    - System performance and availability
    - System topology
    - Log files
    - Configuration compliance reports and comparisons
    - Incidents and violations
    - Order and task throughput
    - Consistency of shared data

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 and OSM 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 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.

OSM Deployment Limitations

Although it is possible to deploy OSM to the administration server in a WebLogic Server domain that includes only an administration server, Oracle does not recommend using Application Management Pack for Oracle Communications to monitor instances of OSM deployed in this configuration. This configuration is intended for development and test environments only and Application Management Pack for Oracle Communications is intended to monitor production environments where OSM is deployed to a managed server in a cluster.

To use Application Management Pack for Oracle Communications to monitor an instance of OSM deployed to the administration server, you must configure a listen address for the administration server. If you do not configure a listen address, Enterprise Manager Cloud Control displays the OSM target's status as down, regardless of the target's actual status.

For information about configuring a server's listen address, see the WebLogic Server Help.

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 where Enterprise Manager Cloud Control is installed.
AMP_home	The directory where the Application Management Pack for Oracle Communications plug-in is installed. This is specific to your version of the plug-in. For example, for 12c: *EM_home*/**plugins/oracle.cgbu.ocom.oms.plugin_12.1.0.4.0**
BRM_home	The directory where BRM is installed.
Oracle_home	The directory where Oracle products are installed.
Database_home	The directory where 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 versions 13c and 12c.

Enterprise Manager Cloud Control requires an Oracle Enterprise Database.

This guide assumes you have installed and configured the versions of Enterprise Manager Cloud Control and Enterprise Database that are compatible with your release of Application Management Pack for Oracle Communications.

You can find the latest details about system requirements and compatibility on the **Certifications** tab of My Oracle Support. Search for Application Management Pack for Oracle Communications and Enterprise Manager Base Platform.

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

See the Oracle Enterprise Database documentation for information about installing and configuring Oracle Enterprise Database.

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 Help Center at:

- `https://edelivery.oracle.com`
- `http://docs.oracle.com/en/industries/communications/`

See "Supported Applications, Suites, and Solutions" for a list of supported Oracle Communications applications.

For information about compatible application versions, search for Application Management Pack for Oracle Communications on the **Certifications** tab of My Oracle Support.

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

You install the same plug-in for all of the licensed management packs.

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.

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

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 Oracle Application Management Pack for Oracle Communications plug-in from the Oracle Software Delivery Cloud:

   `https://edelivery.oracle.com`

2. Copy one of the following files to the Enterprise Manager Cloud Control host:
   - For 12c: **12.1.0.4.0_oracle.cgbu.ocom_2000_0.opar**
   - For 13c: **13.1.1.1.0_oracle.cgbu.ocom_2000_0.opar**
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 OPAR file using one of the following commands:

   - For 12c:

     ```
     emcli import_update -file=filepath/12.1.0.4.0_oracle.cgbu.ocom_2000_0.opar
     -omslocal
     ```

   - For 13c:

     ```
     emcli import_update -file=filepath/13.1.1.1.0_oracle.cgbu.ocom_2000_0.opar
     -omslocal
     ```

   where *filepath* is the absolute path to the location where the 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 "About 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, do the following for all host targets where Oracle Communications applications are installed:

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.

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 upgraded plug-in to the Management Server and Management Agents.

You can use the following upgrade paths:

- From version 12.1.0.3 to 12.1.0.4
- From version 12.1.0.3 to 13.1.1.1
- From version 12.1.0.4 to 13.1.1.1

The upgrade process is slightly different for the different target versions. See one of the following sections, depending your target version:

- Upgrading to Version 13.1.1.1
- Upgrading to Version 12.1.0.4

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

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

Upgrading to Version 13.1.1.1

Upgrading to version 13.1.1.1 of the Application Management Pack for Oracle Communications plug-in involves upgrading to Enterprise Manager Cloud Control 13c. As part of the Enterprise Manager Cloud Control upgrade process, the Application Management Pack for Oracle Communications plug-in is also upgraded and deployed. Because of errors in the automated plug-in upgrade process, you must uninstall and reinstall the plug-in.

To upgrade to version 13.1.1.1 of the plug-in:

1. Upgrade your 11g Oracle Database to 12c as described in *Oracle Database Upgrade Guide* for version 12c.
2. Upgrade Enterprise Manager Cloud Control from 12c to 13c as described in *Enterprise Manager Cloud Control Upgrade Guide* for version 13c.
3. Uninstall version 13.1.1.1 of the Application Management Pack for Oracle Communications plug-in as described in "Uninstalling the Application Management Pack for Oracle Communications Plug-In".
4. Reinstall version 13.1.1.1 of the plug-in as described in "Installing the Application Management Pack for Oracle Communications Plug-in".
5. Deploy the plug-in to the management server and agents as described in "Deploying the Application Management Pack for Oracle Communications Plug-In".
6. 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.
7. Install the default configuration template files. See "Installing the Default Configuration Template Files" for details.
8. Rediscover all targets as described in "Adding Oracle Communications Targets".

   For most targets for which you had previously configured automatic discovery, because the information required has not changed, you can run automatic discovery using the pre-existing configuration. See "Running Automatic Discovery On Demand".

   For ECE targets, because you must provide additional information about the targets, you must reconfigure automatic discovery as described in "Configuring

Automatic Discovery". See Table 3–10, " ECE Automatic Discovery Fields" for details about the required information for discovery.

Upgrading to Version 12.1.0.4

Upgrading to version 12.1.0.4 of the Application Management Pack for Oracle Communications plug-in follows the standard upgrade process.

Additionally, because of changes to the structure for Oracle Communications Integration and ECE targets, you must remove and rediscover these targets after deploying the 12.1.0.4 version of the plug-in.

To upgrade to version 12.1.0.4 of the plug-in:

1. Upgrade Enterprise Manager Cloud Control to version 12.1.0.5 as described in *Oracle Enterprise Manager Cloud Control Upgrade Guide* for version 12c.
2. Install the 12.1.0.4 version of the Application Management Pack for Oracle Communications plug-in as described in "Installing the Application Management Pack for Oracle Communications Plug-in".
3. Deploy the plug-in to Oracle Management Service and each Management Agent as described in "Deploying the Application Management Pack for Oracle Communications Plug-In".
4. 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.
5. Install the default configuration template files. See "Installing the Default Configuration Template Files" for details.
6. Confirm that all of your previously-discovered targets appear in the All Targets list.
7. Do the following for each ECE Cluster, ECE Node, and Oracle Communications Integration target:
   a. In the Enterprise Manager Cloud Control administration console, from the **Targets** menu, select **All Targets**.
   b. In the Target Type tree, select ECE Cluster, ECE Node, or Oracle Communications Integration.

      A list of targets of that type appears.
   c. Right-click the name of a target.
   d. From the context menu, select **Target Setup** and then **Remove Target**.

A confirmation dialog box appears.

e. Click **Yes**.

8. Rediscover the removed targets.

   For ECE targets, because you must provide additional information about the targets, you must reconfigure automatic discovery as described in "Configuring Automatic Discovery". See Table 3–10, " ECE Automatic Discovery Fields" for details about the required information for discovery.

   For Oracle Communications Integration targets, because the information required has not changed, you can run automatic discovery using the pre-existing configuration. See "Running Automatic Discovery On Demand".

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 one of the following files to the new *EM_home*/**../gc_inst/user_projects/domains/GCDomain/default_xml/platform** directory:

   - For 12c: *EM_home*/**plugins/oracle.cgbu.ocom.oms.plugin_12.1.0.4.0/metadata/swlib/platform/components/default_xml.zip**
   - For 13c: *EM_home*/**plugins/oracle.cgbu.ocom.oms.plugin_13.1.1.1.0/metadata/swlib/platform/components/default_xml.zip**

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.

Extending Application Domains with the Enterprise Manager Template

Before you can use Enterprise Manager Cloud Control to monitor applications deployed to Oracle Fusion Middleware domains, you must extend the application's domain with the Enterprise Manager template.

You extend domains by selecting the Enterprise Manager template on the Templates screen of the Fusion Middleware Configuration Wizard or by using the WebLogic

Scripting Tool (WLST). You can extend domains at any time. After extending existing domains, restart the servers for the changes to take effect.

You must extend the Fusion Middleware domains before you can monitor the following applications:

- Oracle Communications ASAP
- Oracle Communications Order and Service Management (OSM)
- Oracle Communications Pricing Design Center (PDC)
- Oracle Communications Unified Inventory Management (UIM)

For more information about templates and extending domains, see the following:

- For information about the Enterprise Manager template, see *Oracle Fusion Middleware Domain Template Reference*.
- For information about configuring domains by using the Configuration Wizard, see *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.
- For information about configuring domains by using WLST, see *Oracle Fusion Middleware Understanding the WebLogic Scripting Tool*.

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*.

About Host Preferred Credentials

Application Management Pack for Oracle Communications uses preferred credentials for authentication between the Management Server and managed host targets. Preferred credentials let you perform operations, such as provisioning applications or starting Oracle WebLogic Server domains, on managed targets without being prompted to log in to the target. The credentials are stored in the Enterprise Manager Cloud Control repository.

Host preferred credentials are defined according to the following aspects:

- Target specificity:
  - Default: Applies to all host targets.
  - Target-specific: Applies to a specific host target.

  Target-specific credentials override the default credentials. Default credentials apply to any targets that do not have target-specific credentials defined.
- Privilege level:
  - Normal: Used for simple administration tasks.
  - Privileged: Used for privileged administration tasks that require root access.

Application Management Pack for Oracle Communications requires both normal and privileged credentials for each host.

- User specificity:
  - Global: Applies to all Enterprise Manager Cloud Control users. Only administrators with the required privileges can set global preferred host credentials.
  - User-specific: Applies only to the user who is currently logged in.

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

Setting Host Preferred Credentials

To set 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. From the **Target Type** column, select **Host**.
4. Click **Manage Preferred Credentials**.
5. Do one of the following:
   - To set global host preferred credentials, click the **Global Preferences** tab.
   - To set user-specific host preferred credentials, click or stay on the **My Preferences** tab.
6. From the lists of default or target preferred credentials, select the row for which you want to set host credentials.
7. Click **Set**.
8. Do one of the following:
   - To use an existing named credential:
     a. From the **Credential Name** menu, select a named credential.
     b. Verify the details.
     c. Click **Save**.
   - To create a new named credential:
     a. Select the **New** option.
     b. Enter the user name and password.
     c. From the **Run Privilege** menu, select the relevant run privilege.
     d. In the **Save As** field, enter a name for the new credential.
     e. Click **Save**.

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

Ensuring Correct Preferred Credentials Permissions on Host Targets

Remote procedures and administrative tasks launched from the Management Server run 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 run 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 and ECE 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 are 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. Do one of the following, based on the Enterprise Manager Cloud Control version you are using:
   - For 12c, from the Instruction options, select **Add Host Targets**, and then click **Add Host**.
   - For 13c, click **Install Agent on Host**.
4. In the **Add Host Targets: Host and Platform** wizard, click **Add**.
5. In the **Host** field, enter the new target's host name.
6. From the **Platform** menu, select the correct operating system platform.
7. Click **Next**.
8. 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.
9. 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.
10. Select a **Named Credential** for Management Agent installation on the new target. See "About Host Preferred Credentials" for information about setting up host credentials.
11. Confirm the **Privileged Delegation Setting** and **Port**, as well as any **Optional Details** needed in your installation.
12. Click **Next**.
13. Confirm the value in the **Host Information** field and click **Deploy Agent**.
14. 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 and ECE Hosts

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

To set the required permissions:

1. On the BRM or ECE host operating system, add the agent user and the BRM or ECE host user to the same user group.
2. Give the BRM or ECE 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 or ECE is installed.
4. As the root user, 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 Application Integration Architecture (Oracle AIA) (Oracle Communications Integration target type) Oracle Communications Billing and Revenue Management (BRM) and the following BRM components: ■ Elastic Charging Engine (ECE) ■ Pricing Design Center (PDC) Oracle Communications Network Charging and Control (NCC) Oracle Communications Offline Mediation Controller Oracle Communications operations support systems (OSS) applications: ■ Oracle Communications ASAP ■ Oracle Communications Order and Service Management (OSM) ■ Oracle Communications Unified Inventory Management (UIM)
Guided	ASAP BRM Offline Mediation Controller OSS applications: ■ ASAP ■ OSM ■ UIM PDC

When you discover targets deployed on WebLogic Server domains, such as OSM, UIM, ASAP, and PDC, Enterprise Manager Cloud Control automatically discovers the 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.

When you discover BRM targets, you discover both included components, such as the BRM Batch Controller, and custom components, such as cloned Data Managers and Connection Managers. All actions supported for included components are supported for custom components, including monitoring, process control, and configuration management.

When you discover PDC targets, you can also discover a target representing a PDC transformation engine. If the transformation engine and the main PDC instance are on the same host, you discover them at the same time using the same module. If they are on different hosts, you discover them using two separate modules and associate them using the main PDC module.

Discovering applications involves the following tasks:

1. Pre-Discovery Tasks
2. One of the following discovery methods:
   - Discovering Targets Automatically
   - Discovering and Rediscovering Targets Using Guided Discovery

- Adding Existing Oracle Communications Applications Using Monitoring Properties

3. Post-Discovery Tasks

Pre-Discovery Tasks

Perform the tasks described in this section before discovery.

For all target types, see "Common Pre-Discovery Tasks".

For BRM targets, see "BRM Pre-Discovery Tasks".

For ECE targets, see "ECE Pre-Discovery Tasks".

For Oracle Communications Integration targets, see "Oracle Communications Integration Pre-Discovery Tasks".

Common Pre-Discovery Tasks

Before discovering Oracle Communications applications, perform the following tasks:

1. Back up existing configurations files, such as **pin.conf** and **pin_ctl.conf** for BRM or **oms-config.xml** for OSM.
2. Obtain information from your system administrator about the application instances, such as installation locations, user credentials, and database and server connection details.

   You will enter this information into the Enterprise Manager Cloud Control administration console during discovery.

   For details about the application information you will enter in the console fields, see the section for the type of discovery you will use:

   - For guided discovery, see "Guided Discovery Fields".
   - For automatic discovery, see "Automatic Discovery Fields" and "Target Promotion Fields".

BRM Pre-Discovery Tasks

Before manually discovering BRM targets, 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.

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 where the **tnsnames.ora** file referencing the database used by BRM is located.
PIN_LOG_DIR	The BRM directory where logs are stored. Set **PIN_LOG_DIR** to: *BRM_home*/var

Table 3–2 (Cont.) Required pin_ctl.conf Variables for Guided Discovery

Variable	Description
LD_LIBRARY_PATH	Set **LD_LIBRARY_PATH** to: *Oracle_home*/lib64:*Oracle_Home*/lib:*Database_Home*/lib:*Database_home*/rdbms/lib:$LD_LIBRARY_PATH
LD_LIBRARY_PATH_64	Set **LD_LIBRARY_PATH_64** to: *Oracle_home*/lib64:*Oracle_home*/lib:*Database_home*/lib:*Database_home*/rdbms/lib:$LD_LIBRARY_PATH
PATH	Set **PATH** to: *Oracle_Home*/bin:$PATH
EVENT_HANDLER_PORT	For BRM Pipeline Manager only. Set **EVENT_HANDLER_PORT** to the port to which the Pipeline Manager Event Handler listens.

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** section.

   f. Click **Apply**.

Oracle Communications Integration Pre-Discovery Tasks

Before configuring automatic discovery for Oracle Communications Integration targets:

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

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

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

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
- Offline Mediation Controller
- OSS:
  - ASAP
  - OSM
  - UIM
- PDC (includes PDC transformation targets)

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

Discovering Targets Using Guided Discovery

To discover and promote existing Oracle Communications application targets:

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

   The Add Targets Manually page appears.
3. Do one of the following, based on the Enterprise Manager Cloud Control version you are using:
   - For 12c:
     a. From the Instruction options, select **Add Targets Using Guided Process**.
     b. From **Target Types**, select the type of target to discover.

        For ASAP, OSM, or UIM, select **Oracle Communications OSS Applications Discovery**.

        For PDC transformation targets, if the transformation target is on the same host as the main PDC target, select **Oracle Communications Pricing Design Center Discovery**. If the transformation target is on a different host than the main PDC target, select **Oracle Communications Pricing Design Center Transformation Discovery**.
     c. Click **Add Using Guided Process**.
   - For 13c:
     a. Click **Add Using Guided Process**.

        The Add Using Guided Process dialog box appears.
     b. Select the type of target to discover.

        For ASAP, OSM, or UIM, select **Oracle Communications OSS Applications Discovery**.

        For PDC transformation targets, if the transformation target is on the same host as the main PDC target, select **Oracle Communications Pricing Design Center Discovery**. If the transformation target is on a different

host than the main PDC target, select **Oracle Communications Pricing Design Center Transformation Discovery**.

c. Click **Add**.

4. In the **Choose Targets** wizard, click **Add**.
5. Select the host on which the existing application is installed, and then click **Select**.
6. Select one of the following options for the application to discover:
   - **BRM**
   - **OMC** (Offline Mediation Controller)
   - **OSS** (OSM, UIM, and ASAP)
   - **PDC** (includes PDC transformation nodes)

   You cannot discover both OSS and BSS targets (including BRM, Offline Mediation Controller, and PDC) at the same time.
7. For Offline Mediation Controller and PDC, skip this step.

   For BRM targets, from the **Select Product Type** menu, select the type of BRM system to discover.

   For OSS targets, from the **Select Application** menu, select the applications to discover.
8. Enter the required information in the **Application Information** fields. See the following for information about these fields:
   - For BRM targets, see Table 3–3, " BRM Guided Discovery Fields".
   - For Offline Mediation Controller targets, see Table 3–4, " Offline Mediation Controller Guided Discovery Fields".
   - For OSS targets (ASAP, OSM, and UIM), see Table 3–5, " OSS Guided Discovery Fields".
   - For PDC targets, see Table 3–6, " PDC Guided Discovery Fields".
9. To rediscover the BRM base target, select the **Overwrite existing BRM Targets** option. See "Rediscovering BRM Targets Using Guided Discovery" for more information about rediscovery.
10. (Optional) To register the database for monitoring and topology view for ASAP, PDC, and UIM targets, and BRM and OSM targets without an Oracle Real Application Clusters (Oracle RAC) database:

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

    b. Provide the connection details and user credentials for the database in the **Database Registration Details** fields. See Table 3–7, " BRM Database Association Fields" and Table 3–8, " Application Database Association Fields" for information about these fields.

    If you are discovering multiple OSS products, enter the database details for each product.

    If you are discovering an ASAP, UIM, or PDC target installed on an Oracle RAC database, selecting this option registers the database as a single-instance database. You cannot register a multi-instance database with these target types.

Note: For BRM or OSM with an Oracle RAC database, do not select the **Register DB** option. Instead, associate the database manually as part of the post-discovery tasks.

11. (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.
12. (Optional) To include the target in a dynamic group, enter values in the **TargetProperties** fields. For example:
    - To include the target in a dynamic group of production environments, select **Production** from the **Lifecycle Status** menu.
    - To include the target in a dynamic group of OSS targets, enter **OSS** in the **Line of Business** field.
13. Click **Submit**.
14. 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.
15. 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*.

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.

You must rediscover a BRM target after:

- Provisioning or uninstalling an individual BRM component
- Editing BRM configuration
- Patching BRM

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

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.

Guided Discovery Fields

This section describes the information required for guided discovery.

Table 3–3 describes the guided discovery fields for BRM targets.

Table 3–3 BRM Guided Discovery Fields

Field	Description
Select Product Type	The type of BRM system to discover (base or Pipeline).
PipelineIFWhome or Portalbase Pinhome	The path to the directory where BRM is installed.
ThirdPartyLocation	The path to the directory where the BRM third party software 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 where the **tnsnames.ora** file that points to your database is located.
BRM Host UserName	The BRM host user.
BRM Host Password	The password for the BRM host user.
BRM Registry File Name	The names of the registry files, such as **wireless.reg** or **wirelessRealtime.reg**. Required for pipeline targets only. To discover both batch rating and real-time rating pipeline targets, enter both registry files separated by a comma. For example: `wireless.reg,wirelessRealtime.reg`

Table 3–4 describes the guided discovery fields for Offline Mediation Controller targets.

Table 3–4 Offline Mediation Controller Guided Discovery Fields

Field	Description
Install Location	The path to the directory where Offline Mediation Controller is installed.

Table 3–5 describes the guided discovery fields for OSS targets (ASAP, OSM, and UIM).

Table 3–5 OSS Guided Discovery Fields

Field	Description
Select Application	The OSS application to discover.
EM repository Owner	The user name of the Enterprise Manager repository owner.

Table 3–5 (Cont.) OSS Guided Discovery Fields

Field	Description
EM repository Owner Password	The password of the Enterprise Manager repository owner.
WebLogicHostname	The host name of the domain on which the targets are deployed.
WebLogicPort	The port number of the host on which the targets are deployed.
WebLogicAdminUser	The administrator user name with which to connect to the WebLogic Server host.
WebLogicAdminPassword	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.
ASAPEnvironmentID	The unique identifier for your ASAP environment. Required for ASAP targets only.
ASAP_HOME	The path to the directory where ASAP is installed. Required for ASAP targets only.
UIM_HOME	The path to the directory where UIM is installed. Required for UIM targets only.

Table 3–6 describes the guided discovery fields for PDC targets.

Table 3–6 PDC Guided 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.
WebLogicHostname	The host name of the domain on which the targets are deployed.
WebLogicPort	The port number of the host on which the targets are deployed.
WebLogicAdminUser	The administrator user name with which to connect to the WebLogic Server host.
WebLogicAdminPassword	The administrator password with which to connect to the WebLogic Server host.
Transformation Home	(Optional) The path to the directory where the PDC transformation configuration is stored. For example: *BRM_Integration_Pack_Home*/**apps/transformation** where *BRM_Integration_Pack_Home* is the directory where the BRM-PDC integration pack is installed. Provide the path to monitor the log files for the PDC transformation target in addition to the PDC target.
BRM Host	(Optional) The discovered host of the BRM target with which the PDC target is integrated. Provide the path to monitor the log files for the PDC transformation target in addition to the PDC target.
PDC Home	The path to the directory where PDC is installed.

Table 3–6 (Cont.) PDC Guided Discovery Fields

Field	Description
JMX Protocol	The connection protocol to use when connecting to the WebLogic server.

Table 3–7 describes the fields used when associating a database with a BRM target running on a non-Oracle RAC database.

Table 3–7 BRM Database Association Fields

Field	Description
DB HostName	The host on which the BRM database resides.
DB Port No	The port number for the host on which the BRM database resides.
DB SID	The system ID for the BRM database.
DB UserName	The BRM database user.
SYS DB Password	The password for the BRM database user.

Table 3–8 describes the fields used when associating a database with an ASAP, NCC, OSM, PDC, or UIM target running on a non-Oracle RAC database.

Table 3–8 Application Database Association Fields

Field	Description
target SYSDBA User	Where *target* is ASAP, NCC, OSM, PDC, or UIM, depending on the target type you are discovering. The database user for the application.
target SYSDBA Password	Where *target* is ASAP, NCC, OSM, PDC, or UIM, depending on the target type you are discovering. The password for the database user for the application.

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:

- BRM
- ECE
- NCC
- Offline Mediation Controller
- Oracle Communications Integration (Oracle AIA)
- OSS:

  - ASAP
  - OSM
  - UIM
- PDC (includes PDC transformation targets)

Automatic discovery involves the following tasks:

- For all targets:
  - Pre-Discovery Tasks
  - Configuring Automatic Discovery
  - Running Automatic Discovery On Demand
  - Viewing Automatic Discovery Errors
  - Promoting Discovered Targets
- For BRM and OSM targets on Oracle RAC databases:
  - Associating Oracle RAC Database Targets with BRM and OSM Targets

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 discovery module for the type of target you want to discover.

   You can select more than one module at a time.

   For PDC transformation targets, if the transformation target and main PDC target are on the same host, select only the PDC module. If the targets are on different hosts, also select the PDC Transformation module.
7. For NCC targets, skip this step.

   For all other target types, click **Edit Parameters** and in the Edit Parameters dialog box, enter information in the fields for the application you want to discover. See the following for details about these fields:

   - For BRM targets, see Table 3–9, " BRM Automatic Discovery Fields".
   - For ECE targets, see Table 3–10, " ECE Automatic Discovery Fields".
   - For Offline Mediation Controller targets, see Table 3–11, " Offline Mediation Controller Automatic Discovery Fields".
   - For Oracle Communications Integration targets (Oracle AIA), see Table 3–12, " Oracle Communications Integration Automatic Discovery Fields".
   - For OSS targets (ASAP, UIM, and OSM), see Table 3–13, " OSS Automatic Discovery Fields".

- For PDC targets, see Table 3–14, " PDC Automatic Discovery Fields".

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

8. Click **OK** in the Edit Parameters dialog box.
9. Click **OK**.

   The list of managed hosts appears.

Automatic Discovery Fields

This section describes the information required for automatic discovery.

Table 3–9 describes the automatic discovery fields for BRM targets.

Table 3–9 BRM Automatic Discovery Fields

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

Table 3–10 describes the automatic discovery fields for ECE targets.

Table 3–10 ECE Automatic Discovery Fields

Field	Description
Enter ECE Home	The path to the directory where ECE is installed.
Enter Java Home	The path to the directory where Java is installed.
Enter JMX Port	The JMX port number of the ECE management node.
Enter Hostname	The host name of the ECE management node.
Enter Service Name	The service name of the ECE management node.
ECE JMX UserName for Coherence MBean Server	The user name for the Coherence management JMX server.
ECE JMX Password for Coherence MBean Server	The password for the Coherence management JMX server user.

Table 3–11 describes the guided discovery fields for Offline Mediation Controller targets.

Table 3–11 Offline Mediation Controller Automatic Discovery Fields

Field	Description
Enter Install Location	The path to the directory where Offline Mediation Controller is installed.

Table 3–12 describes the automatic discovery fields for Oracle Communications Integration targets (Oracle AIA).

Table 3–12 Oracle Communications Integration Automatic Discovery Fields

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

Table 3–13 describes the automatic discovery fields for OSS targets (ASAP, OSM, and UIM).

Table 3–13 OSS Automatic Discovery Fields

Field	Description
Enter Weblogic HostName	The host on which the target is deployed.
Enter WeblogicPort	The port number of the host on which the target is deployed.
Enter Weblogic User Name	The user name with which to connect to the WebLogic Server host.
Enter Weblogic Password	The password with which to connect to the WebLogic Server host.
Enter t3/t3s Protocol	The connection protocol to use when connecting to the WebLogic server.
Enter Deployment Names	A colon-separated list of the types of OSS products to discover. The default value is **oms:asap:oracle.communications.inventory**.
Enter UIM HOME Directory	The path to the directory where UIM is installed. Required for UIM targets only.
Enter ASAP HOME Directory	The path to the directory where ASAP is installed. Required for ASAP targets only.
Enter Comms Plugin Version	The version of Application Management Pack for Oracle Communications that you are using.

Table 3–14 describes the automatic discovery fields for PDC targets.

Table 3–14 PDC Automatic Discovery Fields

Field	Description
Enter Weblogic HostName	The host on which the target is deployed.
Enter Weblogic Port	The port number of the host on which the target is deployed.
Enter Weblogic User Name	The user name with which to connect to the WebLogic Server host.
Enter Weblogic Password	The password with which to connect to the WebLogic Server host.
Enter t3/t3s Protocol	The connection protocol to use when connecting to the WebLogic server.
Enter BRMHostName	(Optional) The discovered host of the BRM target with which the PDC target is integrated. If the main PDC target and the transformation target are on the same host, you discover both at the same time by specifying the transformation home and BRM host in the main PDC module. If the main PDC target and the transformation target are on different hosts, you discover the targets separately by using the PDC transformation module and the main PDC module. You can associate the two by specifying the transformation home and BRM host of the transformation target in the main PDC discovery module.
Enter Transformation Path	(Optional) The path to the directory where the PDC transformation configuration is stored. For example: *BRM_Integration_Pack_Home*/**apps/transformation** where *BRM_Integration_Pack_Home* is the directory where the BRM-PDC integration pack is installed. If the main PDC target and the transformation target are on the same host, you discover both at the same time by specifying the transformation home and BRM host in the main PDC module. If the main PDC target and the transformation target are on different hosts, you discover the targets separately by using the PDC transformation module and the main PDC module. You can associate the two by specifying the transformation home and BRM host of the transformation target in the main PDC discovery module.
Enter PDC Home	The path to the directory where PDC is installed.
Enter Comms Plugin Version	The version of Application Management Pack for Oracle Communications that you are using.

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 the following:

- 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.
- If the servers in the SOA cluster on which your Oracle AIA instance is deployed are configured with IP, host, and domain, an Oracle Communications Integration target is discovered for several combinations of IP and host.

  For example, if your administration server is configured on **samplehost.example.com:7001** and its IP equivalent, **192.0.2.1:7001**, the following targets are discovered:

  – Communications_Integration_192.0.2.1_7001
  – Communications_Integration_samplehost_7001
  – Communications_Integration_samplehost.example.com_7001

  You only need to promote one target for each cluster. For complete monitoring functionality, Oracle recommends promoting a target for the server on which Oracle AIA is installed.

5. Click **Promote**.

   The Promote *target_type* Target(s) page appears.

6. For BRM and NCC targets, skip this step.

   For all other target types, enter the required information for the target. See the following for details about the required information and fields:

   - For ECE targets, see Table 3–15, " ECE Promotion Fields".
   - For Oracle Communications Integrations (Oracle AIA) targets, see Table 3–16, " Oracle Communications Integration Promotion Fields".
   - For OSS targets (ASAP, OSM, and UIM), see Table 3–17, " OSS Promotion Fields".
   - For PDC targets, see Table 3–18, " PDC Promotion Fields".

7. For all target types other than BRM, 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 user name and password for the user with permissions for the BRM environment.
   d. Click **Save**.

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

8. (Optional) To register the database for monitoring and topology view:

   If you are promoting an ASAP, ECE, NCC, PDC, or UIM target installed on an Oracle RAC database, selecting this option registers the database as a single-instance database. You cannot register a multi-instance database with these target types.

   - For ASAP, ECE, NCC, PDC, and UIM targets, and BRM and OSM targets without an Oracle RAC database:

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

b. Provide the connection details and user credentials for the database in the **Database Registration Details** fields. See Table 3–19, " BRM Database Association Fields" and Table 3–20, " Application Database Association Fields" for information about these fields.

- For Oracle Communications Integration targets:

a. Under **Communication Integration (FP/Cross Reference) Database Detail** or **SOA (Infra) Database Detail**, select the **Register DB for Monitoring** option.

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

b. Provide values for the **System User-Name** and **System Password** fields. See Table 3–21, " Oracle Communications Database Association Fields" for information about these fields.

Note: For BRM or OSM with an Oracle RAC database, do not select the **Register DB** option. Instead, associate the database manually as a post-discovery task.

---

9. For Oracle Communications Integration targets, skip this step.

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

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

   b. Do one of the following:

      – Create a new logical group for the target by entering a unique logical group name.

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

10. (Optional) To include the target in a dynamic group, enter values in the **TargetProperties** fields. For example:

    - To include the target in a dynamic group of production environments, select **Production** from the **Lifecycle Status** menu.
    - To include the target in a dynamic group of OSS targets, enter **OSS** in the **Line of Business** field.

11. Click **Promote**.

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

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

Target Promotion Fields

This section describes the information required for promoting automatically discovered targets.

Table 3–15 describes the promotion fields for ECE targets.

Table 3–15 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 3–16 describes the required fields for Oracle Communications Integration targets (Oracle AIA).

Table 3–16 Oracle Communications 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 where SOA 11g is installed. Not required for SOA 12c.
Communications Integration Home (Pre-built/AIA Home)	The path to the directory where the Oracle AIA pre-built integrations are installed. Required only for integration targets that are installed on the same host as the Management Agent.
Communications Integration OPatch File Location	The path to the directory where the OPatch utility is located. Required only for integration targets running on SOA 12c that are installed on the same host as the Management Agent. Not required for targets running on SOA 11g.
Host-Name	The host name of the database. You can enter values for this field under both Communications Integration and SOA database details.
Port	The port number of the database. You can enter values for this field under both Communications Integration and SOA database details.

Table 3–16 (Cont.) Oracle Communications Integration Promotion Fields

Property	Description
SID	The unique identifier of the database. You can enter values for this field under both Communications Integration and SOA database details.
User-Name	The user name of the database user. You can enter values for this field under both Communications Integration and SOA database details.
Password	The password of the database user. You can enter values for this field under both Communications Integration and SOA database details.

Table 3–17 describes the promotion fields for OSS targets (ASAP, OSM, and UIM).

Table 3–17 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.
WebLogicAdminPassword	The password of the WebLogic Server administrator account.
ASAPEnvironmentID	For ASAP targets only. The unique identifier for your ASAP environment.

Table 3–17 describes the promotion fields for PDC targets.

Table 3–18 PDC 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.
WebLogicAdminPassword	The password of the WebLogic Server administrator account.

Table 3–19 describes the fields used when associating a database with a BRM target running on a non-Oracle RAC database.

Table 3–19 BRM Database Association Fields

Fields	Description
DB HostName	The host on which the BRM database resides.
DB Port No	The port number for the host on which the BRM database resides.
DB SID	The system ID for the BRM database.
DB UserName	The BRM database user.

Table 3–19 (Cont.) BRM Database Association Fields

Fields	Description
SYS DB Password	The password for the BRM database user.

Table 3–20 describes the fields used when associating a database with an ASAP, NCC, OSM, PDC, or UIM target running on a non-Oracle RAC database.

Table 3–20 Application Database Association Fields

Fields	Description
target SYSDBA User	Where *target* is ASAP, NCC, OSM, PDC, or UIM, depending on the target type you are discovering. The database user for the application.
target SYSDBA Password	Where *target* is ASAP, NCC, OSM, PDC, or UIM, depending on the target type you are discovering. The password for the database user for the application.

Table 3–21 describes the fields used when associating a database with an Oracle Communications Integration target.

Table 3–21 Oracle Communications Database Association Fields

Property	Description
System User-Name	The user name of the database system user. You can enter values for this field under both Communications Integration and SOA database details.
System Password	The password of the database system user. You can enter values for this field under both Communications Integration and SOA database details.

Post-Discovery Tasks

For some Oracle Communications applications, you must perform additional tasks before you can monitor them. See the following sections for the tasks to perform:

- For BRM targets, see "Adding BRM Components to the pin_ctl.conf File".
- For BRM Pipeline Manager batch rating and real-time rating pipeline targets, see "Configuring SNMP for BRM Pipeline Targets".
- For application targets installed with Oracle databases, see "Associating Application Targets with Database Targets".
- For application targets installed with Oracle RAC databases, see "Associating Oracle RAC Database Targets with BRM and OSM Targets".
- For UIM targets in a Communications suite, see "Adding the UIM Database Password to the Communications Suite Target".
- For OSM targets in clustered environments, see "Configuring Compliance for OSM Clusters".

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 the **pin_ctl.conf** file:

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 *BRM_home***/bin/pin_ctl.conf** file.
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. Under the target's name, from the target type 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 Application Targets with Database Targets

After discovering and promoting BRM, NCC, OSM system, and PDC targets and their related Oracle Database targets, you can associate the application target with the database target so that the database appears on the application target's topology page.

To associate an application target with a database target:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the target home page, as described in "Viewing Home Pages".
3. Under the target name, from the target type menu, select **Target Setup** and then **Monitoring Configuration**.
4. In the **DB Host** field (**BRM Database Host** for BRM targets), enter the host for the database that you are associating.
5. In the **DB SID** field (**BRM Database SID** for BRM targets), enter the system ID for the database that you are associating.

6. Click **OK**.

   A message appears confirming that the settings were saved.

7. Click **OK**.

8. Under the target's name, from the target type menu, select **Monitoring** and then **Associate Database**.

   The Associate Database region appears.

9. Click **Associate Database**.

   A message appears confirming that the database was associated.

10. Click **OK**.

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

Associating Oracle RAC Database Targets with BRM and OSM Targets

When your BRM or OSM 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.

You can associate an Oracle RAC database with BRM and OSM only. For other applications, although you can register the Oracle RAC database when discovering or promoting the target, it will be shown as a single-instance database on the topology page.

To associate an Oracle RAC database with a BRM or OSM 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 or OSM target as described in "Adding Oracle Communications Targets". During discovery or while promoting automatically discovered targets, do not select the **Register DB** option.

2. Do one of the following:

   - On the BRM target home page, click **AssociateRACDB**.
   - On the OSM target home page, click **Associate RAC Database**.

3. Confirm that the database was successfully associated by viewing the BRM or OSM 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 OSM Clusters

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 processes 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
- NCC SLC Target
- NCC SMP Target
- NCC VWS 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 Communications Integration
- Oracle ECE Node
- Oracle OMC NodeManager
- Order and Service Management Node
- PDC
- Unified Inventory Management

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 instructions.
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 instructions.
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. Do one of the following, depending on the version of Enterprise Manager Cloud Control you are using:
   - For 12c:
     a. Select **Add Targets Declaratively by Specifying Target Monitoring Properties**.
     b. From **Target Types**, select the Oracle Communications application or process.

c. Click the magnifying glass and search for the monitoring agent running on the host where the Oracle Communications application or process is running.

   The Search and Select: Targets dialog box appears.

d. Select the Management Agent running on the Oracle Communications application or process host.

e. Click **Select**.

f. Click **Add Manually**.

- For 13c:

  a. Click **Add Target Declaratively**.

  b. Click the magnifying glass and search for the host where the Oracle Communications application or process is running.

     The Select host dialog box appears.

  c. Select a host from the list and click **Select**.

  d. Select a target type from the list and click **Add**.

6. 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.
7. Click **OK** to add the new target.
8. 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.

Database Password Restrictions

When provisioning targets that require a database, you provide the credentials for the database users. For example, with OSM, you provide credentials for the database system user, the application schema database user, and the reporting schema database user.

If the password provided for any database user starts with **$$**, Application Management Pack for Oracle Communications cannot connect to the database. You must ensure that the database user passwords for your applications do not start with **$$**.

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, Suites, and Solutions" 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:

- Business support systems (BSS):
  - Oracle Communications Billing and Revenue Management (BRM) including Elastic Charging Engine (ECE), Pipeline Configuration Center (PCC), and Pricing Design Centre (PDC).
  - Oracle Communications Network Charging and Control (NCC)
  - Oracle Communications Offline Mediation Controller
- Operations support systems (OSS):
  - Oracle Communications ASAP
  - Oracle Communications Order and Service Management (OSM)
  - Oracle Communications Unified Inventory Management (UIM)
- Integrations:
  - Oracle Application Integration Architecture for Communications (Oracle AIA)

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, Suites, and Solutions" for information about supported Oracle Communications applications and versions.

Table 4–1 Supported Application Management Pack for Communications Actions

Action	ASAP	BRM	ECE	NCC	Offline Mediation Controller	OSM	PDC	PCC	UIM	Oracle AIA
Discover	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Provision	Yes	Yes	No	No	No	Yes	Yes	Yes	Yes	No
Start/Stop Processes	No	Yes	Yes	Yes	Yes	No	Yes	No	No	No
Patch/Roll back patches	No	Yes	No	No	No	No	No	No	No	No
Upgrade	No	No	No	No	No	No	Yes	No	No	No
Monitor	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
View/Compare Configurations	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Edit Configurations	No	Yes	No	No	No	No	No	No	No	No
Manage Alerts	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
View Topology	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Manage Compliance	No	No	No	No	No	Yes	No	No	Yes	Yes

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 and OSM 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:
  - ASAP
  - BRM
  - OSM
  - PCC
  - PDC
  - UIM
- OSS Service Fulfillment suite:
  - ASAP

- OSM
- UIM

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".

Important: If you are provisioning an OSM cluster on a WebLogic Server domain that uses a shared storage system such as Network File System (NFS), ensure that the user IDs are consistent across all WebLogic Server client machines that access the shared storage.

For more information about best practices for WebLogic Server on shared storage, see the Oracle Maximum Availability white paper, available at the following link:

`http://www.oracle.com/au/products/database/fusion-middleware-maa-155387.html`

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 where 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 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. The **ADMIN** row also lets you provide details for the Fusion Middleware Repository Creation Utility (RCU).

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

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.

   The RCU fields are required for OSM, UIM, and ASAP on Fusion Middleware 12c. On Fusion Middleware 11g, they are required for UIM only. Any values provided in these fields when provisioning OSM or ASAP on Fusion Middleware 11g are ignored.

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.

Note: Using the **Remove** button can result in invalid configurations, such as an OSM cluster with no nodes. When provisioning a cluster, do not remove the individual application rows. When provisioning a highly-available suite, you can remove all of the rows representing an entire cluster, but do not remove only the individual application rows within the cluster.

---

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: Passwords for database users must not begin with **$$**.

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 "About 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 Account Synchronization DM	AccountSynchTool_ release_OS	oracle_brm_cm
BRM Base	Batch Controller CM Proxy CMMP Connection Manager Email Data Manager Formatter Invoice Data Manager Oracle Data Manager 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 EAI Data Manager 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
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

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

BRM ISMP Package	Installable Components	Source Component Name Format	Base Component
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 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 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 GSM Manager GPRS AAA Manager GPRS Manager Number Manager RRF Manager Services Framework Manager Services Framework AAA Manager SIM Manager 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.

About Provisioning Multischema BRM Systems

You can use the Communications Suite Installation Procedure to provision multischema systems with up to nine secondary database schemas.

To provision multischema systems, you must run the Communications Suite Installation Procedure twice with the BRM Basic option. First you run the procedure for all secondary schemas, then you run it again for the primary schema.

See "Provisioning a Basic BRM System" for more information about how to run the Communications Suite Installation Procedure with the BRM Basic option.

See the discussion of managing a multischema system in *BRM System Administrator's Guide* and the discussion of installing a multischema system in *BRM Installation Guide* for more information about multischema architecture and management.

Provisioning a Basic BRM System

Use the BRM Basic option in the Communications Suite Installation Procedure to provision a basic system. 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:

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 and the Host Configurations area 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 Installers 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. To install a multischema system:
    a. Select **Enable MultiDB**.
    b. From the **No Of Schemas** list, select the number of additional schemas.
    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. For each additional schema, provide values for the fields described in Table 4–4.

Table 4–4 Secondary Schema Fields

Field	Description
db_no	The unique database number for the secondary schema. For example, **0.0.0.2**.
pin_owner	The user name for the primary database schema. For example, **PIN**.
pin_dm_secondary_owner	The user name for the secondary database schema. For example, **PINB**.
pin_dm_secondary_passwd	The password for the secondary database schema user.
pin_dm_secondary_dbname	The alias for the secondary database schema. For example, **pindb***hostname*.
pin_dm_secondary_hostname	The machine name where the secondary DM is running.
pin_dm_secondary_port	The DM port number for the secondary database schema.
sec_pin_home	The directory on the secondary installation machine where to install BRM. For example, **/home/oracle/pinhome2** This must match the value you entered in the **BRM Home Directory** field for the secondary schema in the BRM Configuration area under Host Configurations. The staging location for the secondary installation is the immediate child of this directory.
login_user	The user for the secondary installation system.
login_password	The password for the secondary installation system user.

    e. Click **Save**.
14. (Optional) Expand **Advanced** and edit the default port numbers for the BRM components.
15. Click **Next**.

The Credentials page appears.

16. Provide the preferred credentials for the target host. See "About 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 4–5.

    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 4–5 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. Enter Yes to have the installer add 12 monthly partitions, a historic partition, and a last partition to your event tables. 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. This sets the $CREATE_PARTITIONS parameter in the pin_setup.values file to Yes. This prompt is displayed only if you enter Yes to Partition event tables.	YES
EnablePartition	Specify whether you want to enable partitioning. 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. This sets the $ENABLE_PARTITION parameter to Yes in the pin_setup.values file. Important 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. If you plan to use Rated Event Loader to load prerated events, you must partition your event tables. 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. You cannot partition classes after you run the **pin_setup** utility	NA
SetupDropAllTables	Enter whether you want to drop the database tables. 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. If you select **NO**, the installer uses your existing BRM tables. In test systems, select **YES** to reinitialize the database.	YES
CreateDatabaseTables	Enter whether you want the installer to create default BRM tablespaces for you. 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 "About 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".

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, 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 Manager Patches

You can roll back the patch that was most recently applied to a BRM component or system. You can roll back patches on multiple BRM components at a time. See "Rolling Back BRM Patches".

Patching Multischema BRM Systems

To patch multischema systems:

1. Patch the target on the primary schema. See "Patching BRM".
2. Grant permissions for each secondary schema user as follows:
   a. Log in to the primary database schema as a privileged user.
   b. Run the following commands:

```
GRANT ALL ON DD_OBJECTS_T TO secondary_schema_user;
GRANT ALL ON DD_OBJECTS_FIELDS_T TO secondary_schema_user;
GRANT ALL ON DD_TYPES_T TO secondary_schema_user;
```

```
GRANT ALL ON DD_FIELDS_T TO secondary_schema_user;
```

3. Patch the targets on the secondary schemas.
4. Perform post-patch tasks for all the schemas. See "BRM Post-Patch Tasks".

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. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.

   The Deployment Procedure Manager page appears.
4. Select **BRM Patching Procedure** and click **Launch**.
5. Under **Choose Targets and Patches**, click **Add**.

   The Search and Select: Targets window appears.
6. 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 **On Host** field, enter the host name.
7. Click **Search**.
8. Select the BRM target to patch.
9. Click **Select**.

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

    The **Choose BRM Patches** window appears.
11. Specify search criteria for the patch and click **Search Patches**.

    A list of patches meeting the search criteria appears.
12. (Optional) Click the link in the ReadMe column for detailed patch information from Oracle Support.
13. Select the correct patches to apply and click **Add Patches**.
14. Under **Target Configuration**, provide the information required about your BRM target. Typically, this information includes the location of your BRM installation and database credentials.
15. Click **Next**.

    The Credentials page appears.

16. Provide the preferred credentials for the target host. See "About 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**.
21. Monitor the status of the patching process as described in "Monitoring BRM Patching Status".
22. 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.

Ignoring Steps During BRM Patching

You can safely ignore failed BRM patching procedure steps in the following situations:

- If a patch does not included upgrade packages, the patching procedure automatically ignores the upgrade step. However, the post-patch step may attempt to run scripts that the upgrade package would have created. Because these scripts are missing, the step fails.
- When patching BRM on Solaris environments using Patch Set 10 with Patch 19921037, the following steps fail:
  - Stage BRM Solaris Patches
  - Unzip Solaris BRM Patches

To ignore a step:

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

   The Deployment Procedure Manager page appears.
3. In the **Run** column, click the name of the failed patching procedure.

   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. Select the check box beside the failed step.

   A tab with details about the step appears.
6. From the Actions menu, select **Ignore**.

   The patching procedure continues automatically.

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 Manager 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 Manager Patches

To view the list of patches that have been applied to a BRM CM or Pipeline Manager 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.

Rolling Back BRM Patches

To roll back the most recently applied patch on one or more BRM targets:

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

   The Deployment Procedure Manager page appears.
3. From the Procedure Library table, select **BRM Patching RollBack Procedure**.
4. Click **Launch**.
5. Under **Choose Targets and Patches**, click **Add**.

   The Select Targets dialog box appears.
6. Select the BRM target for whose patch you want to roll back. You can select multiple targets.
7. Click **Select**.

   The BRM target appears in the Choose Targets and Patches table.
8. Click **Next**.

   The Patch Analysis Report page appears, showing the BRM targets on the same host that will be rolled back.
9. Review the information on the page and click **Next**.

   The Credentials page appears.

10. Enter the user name and password for the BRM host and click **Next**.

    The Schedule page appears.

11. Specify when the procedure should run and click **Next**.

    The Review page appears.

12. Verify the schedule and patch information and click **Finish**.

    The Procedure Activity page appears.

13. (Optional) Monitor the status of the rollback as follows:

    a. In the **Run** column, click the name of the rollback procedure.

       The Procedure Steps table for the selected BRM patching procedure appears.

    b. In the **Name** column, expand the **BRM Patching RollBack Phase** and host name entries.

       All of the steps for the rollback procedure appear.

    c. In the **Status** column, review the status of the steps.

    d. In the **Select** column, select any step for which you want to view more details.

    e. Click **Refresh**.

       The status of all steps is updated.

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 and Managing Log Files
- Configuring Alerts
- Configuring Metric Monitoring Thresholds and Alerts
- Configuring Collection Schedules
- Monitoring Groups of Targets

See "About Conditions that Trigger Notifications" for information about the formatting of the metric conditions.

Using the Communications Applications Landing Page

Application Management Pack for Oracle Communications provides a landing page where you can view summary information about all discovered Oracle Communications targets in one place.

The Communications Applications landing page shows a list of all discovered Oracle Communications targets. Targets that are members of systems or dynamic groups are organized under their parent system or group. You can expand systems, groups, and individual targets to see related targets, including infrastructure components such as databases and WebLogic Server domains.

To use the Communications Applications landing page:

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

   The Communications Applications landing page appears.
3. Do any of the following:
   - Review the availability of all Oracle Communications targets.
   - Filter the list of targets by target name and lifecycle status.
   - Expand top-level systems, groups, or targets to see the status of related targets.
   - View the availability chart and incidents and violations table for an individual target or system by highlighting its row in the list of targets.
   - View details about an incident or violation by clicking its name in the Incidents and Violations table.
   - View the home page for a target, system, or group by clicking its name in list of targets.
   - Set up data discrepancy reports by clicking **Data Discrepancy**. See "Identifying Discrepancies in Shared Data" for more information.
   - Discover new Oracle Communications targets by clicking **Add**. See "Discovering and Rediscovering Targets Using Guided Discovery" for more information.
   - Edit configurations for a target by highlighting its row in the list of targets and clicking **Configure**. See "Managing Configuration" for more information.
   - View details about infrastructure components by clicking the **Infrastructure Targets** tab.

Viewing Home Pages

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

To view a home page:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Do either of the following:
   - To select the target from the list of all targets:
     a. From the **Targets** menu, select **All Targets**.

b. In the Target Type tree, select the type of target you want to view.

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

The target's home page appears.

- To select the target from the Communications Applications landing page, which contains a list of Oracle Communications targets only:

a. From the **Targets** menu, select **Communications Applications**.

The Communications Applications landing page appears.

b. From the list of targets, click the name of the target you want to view.

The target's home page appears.

You can customize target home pages by adding new regions and changing the page layout. Not all regions that you can add are applicable to all targets. For example, if you add an ECE-related region to the home page for an OSM target, there will be no data to display in that region.

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

Viewing Target Metrics

You can view the details about individual metrics collected for Oracle Communications targets, including values, severity, and alerts that are triggered for that metric.

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 navigation tree, expand the metric category and select the metric you want to view.

Monitoring Log Files

You can use Application Management Pack for Oracle Communications to monitor application log files for specific error patterns and send alerts for targets when patterns are found.

For BSS targets, you can view log files within the Enterprise Manager Cloud Control administration console. See "Viewing and Managing Log Files".

For BRM, ECE, NCC, Offline Mediation Controller, Oracle AIA, and OSM targets, Application Management Pack for Oracle Communications provides default error pattern templates for generating alerts based on log files. You can edit the templates to add custom error patterns.

The maximum number of alerts generated and shown for the log file monitoring metric for Oracle Communications targets is different for different target types:

- For targets that have large log files that are not regularly rotated, such as BRM, the maximum number of alerts generated for one error pattern is set to 20. After 20 occurrences of one pattern, the log file monitoring metric skips that pattern and

checks the next pattern. This prevents performance degradation when processing large log files with many occurrences of the same error pattern.

- For targets that rotate log files (external to Enterprise Manager Cloud Control), such as OSM, the maximum is set much higher. Processing time is not a performance issue for regularly-rotated log files.

You can also include error pattern templates in monitoring templates. For more information about log file monitoring and using monitoring templates, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Viewing and Managing Log Files

You can view and manage log files for BSS targets.

To view and manage log files:

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 log files, as described in "Viewing Home Pages".
3. In the **Log Files Contents** or **Quick Links** region, click **View Log Files**. For PDC, you choose between domain logs, synchronization logs, and transformation engine logs.

   The list of log files for the target appears.
4. (Optional) Filter the list by entering a value in **Filter log files** field and clicking **Filter log files**.
5. Select a log from the list to view the contents.
6. (Optional) Click **Download** to save a copy of the log file to your local machine.
7. (Optional) Click **Clear Log File** to clear the contents of the log file.
8. (Optional) For BRM Connection Manager targets:
   - Click **EnableDebugging** to enable debugging.
   - Click **DisableDebugging** to disable debugging.

   Enabling debugging sets the log to debug dynamically without needing to invoke a BRM utility to restart the target. If you disable debugging, you must manually debug and restart the target.

Applying Error Pattern Templates to Targets

To apply error pattern templates to targets:

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. Select **AMS Error Patterns Editing Procedure** and click **Launch**.

   The Choose Targets page appears.
4. From the **Select Application** menu, select the target type for which you are editing or applying error templates.

   The content from the error pattern file for that target type appears.

5. (Optional) Add custom error patterns and pattern help to the error pattern file content. Use the following format for patterns and help:

```
@target_PATTERNS = (
"common_string##common_string",
...
%target_ERROR_HELP = (
"common_string##common_string" => "help_message",
```

where:

- *target* is different for different target types. For example, for BRM and NCC, *target* is **PCM**. This line appears automatically in the file.
- *common_string* is the common content that always appears for this error.
- *help_message* is a short description to help interpret the error.

For example, the following error line appears in the diagnostic log for an OSM node, where the bold content is the common content:

```
[OSM_managed_server] [ERROR] []
[oracle.communications.ordermanagement.compliance.agent.ComplianceAgent] [tid:
[STANDBY].ExecuteThread: '2' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: user] [ecid: id] [APP: oms] Skipping copy to /osm_
domain_home/osm_compliance/scripts/copyComplianceWLSTScripts.bat since target
is newer than source.
```

To monitor the OSM logs for this error pattern, the pattern appears in the file content as follows:

```
@PCM_1_PATTERNS = (
...
"agent.ComplianceAgent##Skipping copy to##since target is newer than source.",
...
%PCM_1_ERROR_HELP = {
...
"agent.ComplianceAgent##Skipping copy to##since target is newer than source."
=> "Compliance",
...
```

6. Click **Next**.

   The **Selected Targets** page appears.

7. Review the list of targets to which the error pattern will be applied and click **Next**.

   The Schedule page appears.

8. Under Schedule Configuration, specify when the procedure should run.
9. Click **Next**.
10. Review the error patterns and targets and click **Finish**.

    Any changes made to the error patterns are saved and the error patterns are applied to the specified targets.

11. (Optional) Review the status of the procedure on the **Procedure Activity** tab.
12. (Optional) Customize thresholds for alerts and configure corrective actions for log file pattern matching. See "Configuring Alerts" for more information.

Configuring Alerts

Application Management Pack for Oracle Communications lets you configure when to generate alerts and notify administrators. You can generate alerts based on thresholds for individual metrics and based on larger incidents. You can specify automated responses to alerts by using corrective actions and automatically escalate incidents using incident rules.

About Incident Management

In addition to configuring alerts for specific metrics, you can use the Enterprise Manager Cloud Control incident management functionality to monitor larger trends in service disruption that can impact multiple targets and domains.

For example, if you are monitoring a host and an individual metric such as CPU utilization exceeds the acceptable threshold, it may or may not indicate a larger issue with the host. However, if all metrics related to the host exceed acceptable thresholds, it indicates extreme load on the host and represents a larger problem. You can use incident management to monitor such issues together.

You can also automate the creation, assignment, priority, notification, and escalation of incidents by using incident rules.

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

Configuring Metric Monitoring Thresholds and Alerts

Application Management Pack for Oracle Communications provides 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 alert thresholds for Oracle Communications 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 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*.

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 Monitored Objects, click **Edit**.
6. Under **Corrective Actions** for Warning or Critical, click **Add**.

   The Add Corrective Action page appears.
7. From the menu, select a corrective action.
8. Click **Continue**.
9. Enter the required information to define the corrective action.
10. Click **Continue**.

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.

Extending Monitoring Metrics

You can extend the ready-to-use metrics by using Enterprise Manager Cloud Control metric extensions. Metric extensions are metrics that you create to fit the needs of your environment. You can apply metric extensions to individual targets or large numbers of targets by using monitoring templates.

See "Creating Metric Extensions" for detailed examples of how to create metric extensions to monitor custom log files for a BRM target and Java Messaging Service (JMS) for an OSM system target.

See *Oracle Enterprise Manager Cloud Control Administrator's Guide* for information about using monitoring templates and metric extensions.

Creating Metric Extensions

The examples in the following procedure demonstrate how to create metric extensions to monitor a custom log file for a BRM target or JMS for an OSM system target.

To create metric extensions:

1. For custom log file monitoring, create a script to parse the error patterns in your custom log files. You can use the default scripts available with the plug-in as a template. The default scripts are located in the *AMP_home***/agent/scripts** directory.
2. Log in to the Enterprise Manager Cloud Control administration console.
3. From the **Enterprise** menu, select **Monitoring** and then **Metric Extensions**.

   The Metric Extensions page appears.
4. From the **Create** menu, select **Metric Extension**.

   The Create New: General Properties page appears.
5. Enter the values for the general properties:
   a. From the Target Type menu, select the target type for which you are creating a metric extension.

      For example:

      – For BRM custom log file monitoring, **Oracle BRM DMO**
      – For OSM JMS monitoring, **Order and Service Management System**

   b. In the **Name ME$** field, enter a name for the metric extension.

      This name must be unique for this target type. The name is prefixed with ME$.

      For example:

      – For BRM log file monitoring, **BRM_CDR_SAMPLE**
      – For OSM JMS monitoring, **OSM_JMS_SAMPLE**

   c. In the **Display Name** field, enter a display name for the metric extension. _ SAMPLE.

      This name must be unique for this target type, but the value can be the same as for the **Name ME$** field because the display name is not prefixed with ME$.

      For example:

      – For BRM log file monitoring, **BRM_CDR_SAMPLE**
      – For OSM JMS monitoring, **OSM_JMS_SAMPLE**

   d. From the **Adapter** menu, select an adapter type.

      For example:

      – For BRM log file monitoring, **OS Command - Multiple Columns**
      – For OSM JMS monitoring, **Java Management Extensions (JMX)**

   e. In the **Description** field, enter a description of the metric.

6. Enter the values for collection schedule properties:
   a. From the **Data Collection** options, select **Enabled**.
   b. From the **Use of Metric Data** options, select **Alerting and Historical Trending**.
   c. In the **Upload Interval** field, enter **1**.
   d. From the **Collection Frequency** menu, select **By Minutes**.
   e. In the **Repeat Every** field, enter **15**.
7. Click **Next**.

   The Adapter page appears.
8. Enter the values for the properties:

   For example:

   – For BRM log file monitoring:
      a. In the **Command** field, enter **%perlBin%%/perl**.
      b. In the **Script** field, enter the path to the log file parsing script using the available variables.

         For example, **%scriptsDir%/parse_cdr_log.pl "%installLoc%" "new_comp_log" %scriptsDir%**
      c. Leave the **Arguments** field blank.
      d. In the Delimiter field, enter a vertical bar (|).
      e. In the **Starts With** field, enter **em_result=**.
      f. In the Upload Custom Files region, click **Upload**.
      g. Click **Choose File**.
      h. Navigate to the log file parsing script and select it.
      i. Click **OK**.
   – For OSM JMS monitoring:
      a. Click **Browse MBeans**.

         The Select MBean and Attributes dialog box appears
      b. In the Select Target field, search for and select the OSM system for which you want to create the monitoring extension.
      c. Click List **MBeans**.

         The MBeans for the selected target appear.
      d. Select the **osmWsJmsWorkManager** MBean.
      e. Select the following attributes:

         FairShareRequestClass

         Type

         ResponseTimeRequestClass

         MinThreadsConstraint

         MaxThreadsConstraint

         WorkManagerShutdownTrigger

IgnoreStuckThreads

DeploymentOrder

f. Click **Select**.

The MBean is added to the Metric field and the attributes are added to the Column Order field in the order that you selected them.

9. Click **Next**.

The Columns page appears.

10. Add new metric columns corresponding to the adapter output.

For example:

– For BRM log file monitoring, use the order and details in Table 4–6.

Table 4–6 BRM Log File Monitoring Metric Extension Column Properties

Name	Display Name	Column Type	Value Type	Comparison Operator	Warning	Critical
log_file_name	Oracle BRM Log File Path	Data Column	String	NA	NA	NA
log_file_match_pattern	Match pattern in Perl	Key Column	String	NA	NA	NA
log_file_match_pattern_desc	Error message help	Data Column	String	NA	NA	NA
log_file_match_count	Log file patern match occurance count	Data Column	Number	>	1	2

– For OSM JMS monitoring, use the order and details in Table 4–7. Leave the alert threshold columns blank.

Table 4–7 OSM JMS Monitoring Metric Extension Column Properties

Name	Display Name	Column Type	Value Type
FairShareRequestClass	FairShareRequestClass	Data Column	String
Type	Type	Data Column	String
ResponseTimeRequestClass	ResponseTimeRequestClass	Data Column	String
MinThreadsConstraint	MinThreadsConstraint	Data Column	String
MaxThreadsConstraint	MaxThreadsConstraint	Data Column	String
WorkManagerShutdownTrigger	WorkManagerShutdownTrigger	Data Column	String
IgnoreStuckThreads	IgnoreStuckThreads	Data Column	String
DeploymentOrder	DeploymentOrder	Data Column	Number

11. Click **Next**.

12. From the **Host Credentials** options, select **Use Default Monitoring Credentials**.

13. Test the metric extension:

a. Click **Next**.

The Test page appears.

b. In the **Add Targets** table, click **Add**.

   The Select Targets dialog box appears.

c. Select a target for which to test the metric extension and click **Select**.

d. Click **Run Test**.

e. Review the results in the Test Results region.

14. Click **Finish**.

    The metric extension is created.

15. Highlight the newly-created metric extension.

16. From the **Actions** menu, select **Save As Deployable Draft**.

17. Highlight the newly-saved metric extension.

18. From the **Actions** menu, select **Publish Metric Extension**.

    The metric extension is ready to be deployed to targets.

You can deploy metric extensions to individual targets by using the Actions menu. You can deploy metric extensions to multiple targets, including groups of targets, by adding them to monitoring templates and applying the monitoring templates to targets.

For information about deploying metric extensions, creating monitoring templates, adding metric extensions to monitoring templates, and applying monitoring templates to targets, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

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 4–8 describes each attribute in a condition.

Table 4–8 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.

Table 4–8 (Cont.) Condition Attributes

Attribute	Description
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.
Operator	The comparison method Enterprise Manager Cloud Control uses to evaluate the metric value against the threshold values. ■ LE: Less than or equals ■ EQ: Equals ■ LT: Less than ■ GT: Greater than ■ NE: Not equal ■ CONTAINS: ■ OCCURENCES ■ MESSAGE ■ 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 4–9 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 4–9 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%

Using Blackouts

Blackouts let you suspend data collection for targets. You can use blackouts for targets during scheduled maintenance or downtime, or predictable peak usage time to keep your monitoring data consistent and prevent Enterprise Manager Cloud Control from generating alerts during known periods of abnormal system activity.

You can define blackouts for individual targets, groups of targets on different hosts, and all targets on the same host. You can schedule on-demand blackouts, one-time blackouts, and recurring blackouts. You can schedule blackouts with definite and indefinite duration, and change the duration of blackouts currently in effect.

See the chapter about using blackouts in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for more information.

Monitoring Groups of Targets

You can use Enterprise Manager Cloud Control systems and groups for monitoring groups of targets in the administration console.

Application Management Pack for Oracle Communications creates system targets when you discover the following applications:

- ASAP (Comms Suite target)
- BRM (Billing and Revenue Management target)
- ECE (Oracle ECE Cluster target)
- OSM (Comms Suite target)
- UIM (Comms Suite target)

Enterprise Manager Cloud Control also creates infrastructure system targets, such as Oracle WebLogic Domain and SOA Infrastructure targets.

In addition to the ready-to-use systems, you can create generic systems and dynamic groups. See "About Generic Systems" and "About Dynamic Groups".

Each generic or read-to-use system has a home page from which you can monitor metrics related to the system members. See "Viewing System Home Pages".

About Generic Systems

Generic systems are groups of managed targets. Only targets that you specify as members of a generic system are added to the system.

You can use generic systems to group:

- Targets that comprise a collection of integrated products, as in an Oracle Rapid Service Design and Order Deliver (RSDOD) or Rapid Offer Design and Order Delivery (RODOD) solution
- Targets in a highly-available BRM environment with services across hosts used for different deployment model

You create a new generic system and add members to it 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 already discovered targets to it. See the overview of relationships in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

Viewing System Home Pages

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 console.
2. From the **Targets** menu, select **Systems**.
3. In the **Search** list, select **Billing and Revenue Management**, **Comms Suite**, or **Generic System**.
4. Do one of the following:
   - For 12c, click the right arrow icon.
   - For 13c, click the magnifying glass 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 4–10.

Table 4–10 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.

Table 4–10 (Cont.) Regions on the Generic System Home Page

Region	Description
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 Dynamic Groups

Dynamic groups are groups to which targets are added automatically based on membership criteria. You define the membership criteria and, when new targets that meet the criteria are discovered, they are automatically added to the dynamic group.

You can create a hierarchy of dynamic groups by assigning a parent dynamic group. See "Creating Hierarchical Dynamic Groups". By using hierarchical dynamic groups, you can automatically group functionally distinct target types, such as BSS and OSS targets, into one solution, such as RODOD.

Each dynamic group that you create has its own monitoring home page, which you can use to monitor all members of the group in one place. You can customize the group home page to include additional relevant monitoring metrics. See "Viewing Group Home Pages".

The Oracle Communications Applications landing page in Enterprise Manager Cloud Control also shows Communications targets organized in dynamic groups.

Application Management Pack for Oracle Communications includes target properties that you can use as membership criteria for dynamic groups. These properties let you group targets in a variety of ways, for example, by target lifecycle status (development or production system), or line of business (BSS or OSS).

You can enter values for these properties during target discovery and promotion, or from the home page of a target that has already been discovered. See "Adding Targets to Dynamic Groups".

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

Creating Hierarchical Dynamic Groups

This section describes how to create a hierarchy of dynamic groups. The procedure includes examples that create a parent dynamic group for RODOD applications and subgroups for OSS and BSS development and production systems.

To create a hierarchy of dynamic groups:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Targets** menu, select **Groups**.
3. (Optional) Create a parent group. See the discussion of managing groups in *Oracle Enterprise Manager Cloud Control Administrator's Guide*. The parent group can be a regular or dynamic group.
4. From the **Create** menu above the list of groups, select **Dynamic Group**.

   The Create Dynamic Group page appears.
5. In the **Name** field, enter a name for the group.

For example:

- **BSS Production**
- **BSS Development**
- **OSS Production**
- **OSS Development**

6. (Optional) If you are using hierarchical groups:
   a. Next to the **Parent Groups** field, click **Add**.

      The Search and Select: Targets dialog box appears.

   b. Select a parent group, for example **RODOD Parent**, and click **Select**.

      The group is added to the **Parent Groups** field.
7. Click **Define Membership Criteria**.

   The Define Membership Criteria page appears.
8. Next to any applicable the fields, click the magnifying glass icon. For example:
   - To create groups for BSS or OSS systems, select the icon next to the **Line of Business** field.
   - To create groups for production or development systems, select the icon next to the **Lifecycle Status** field.
9. Move elements from the list of available values to the list of selected values. For example:
   - For BSS groups, move the **BSS** element from the list of available values to the list of selected values.
   - For OSS groups, move the **OSS** element from the list of available values to the list of selected values.
   - For development groups, move the **Development** element from the list of available values to the list of selected values.
   - For production groups, move the **Production** element from the list of available values to the list of selected values.
10. Click **Select**.

    The values are added to the fields.
11. Click **OK**.

    The membership criteria are added.
12. Click **OK**.

    The group is created and a success message appears. Any targets that meet the membership criteria are automatically added to the group.
13. Click **OK**.

Adding Targets to Dynamic Groups

You can provide values for the target properties used to define dynamic group membership, such as **Line of Business** and **Lifecycle Status**, during discovery or promotion. You can also edit target properties after discovering and promoting targets to add them to dynamic groups.

To edit target properties after discovery and promotion:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the home page for the target that you want to add to a dynamic group, as described in "Viewing Home Pages".
3. From the target type menu, select **Target Setup** and then **Properties**.

   The Target Properties page appears.
4. Click **Edit**.
5. Edit the target properties as relevant. For example:
   - In the **Line of Business** field, enter **BSS** or **OSS**.
   - From the **Lifecycle Status** menu, select **Development** or **Production**.
6. Click **OK**.

   The properties are saved and the target is added to any dynamic groups for which it meets the membership criteria.

Viewing Group Home Pages

Group home pages display information about all targets that are members of the group. To view a group's home page:

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

   The Groups page appears.
3. Click the name of the group for which you want to view the home page.

   The group's home page appears.

By default, a group home page includes regions that give general information about the group members. You can customize group home pages by adding new regions for the specific target types within the group.

For example, for a RODOD group you can add regions for monitoring metrics for the following elements:

- Incoming orders, order and task throughput, order lifecycle times, and order fallout
- Error backlog trends and fault summaries
- Database usage and alerts
- Status of all group members
- Versioning and patching information

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

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.

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`

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 BSS Processes
- Starting and Stopping Domains Hosting Oracle Communications Applications

Starting and Stopping BSS Processes

You can start, stop, and restart application processes for BSS targets in the Enterprise Manager Cloud Control administration console. See one of the following sections, depending on the application:

- See "Starting and Stopping BRM, ECE, NCC, and Offline Mediation Controller Processes" for:
  - BRM systems and components, including custom components.
  - ECE nodes.
  - NCC components.
  - Offline Mediation Controller administration server and nodes.
- See "Starting and Stopping PDC Processes" for PDC targets.

Starting and Stopping BRM, ECE, NCC, and Offline Mediation Controller Processes

You start, stop, and restart processes for BRM, ECE, NCC, and Offline Mediation Controller from the home page of the target in the Enterprise Manager Cloud Control administration console.

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

If you have custom BRM components, such as cloned data managers, start and stop scripts for these must exist and they must be included in the **pin_ctl.conf** file. See *Oracle Communications Billing and Revenue Management Developer's Guide* for more information about custom 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 processes:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. Navigate to the home page of the target for which you want to start or stop processes as decribed in "Viewing Home Pages".
3. To stop or start all BRM processes from the home page for the BRM system target:
   a. Click either **STOP ALL** or **START ALL**.
   b. (Optional) Monitor the status of the processes under **Status**.
4. To start or stop and restart an individual BRM component or other BSS target from the home page for the target:
   a. In the Summary area, click **Start**, **Stop**, or **Restart**. You may need to scroll down to see the buttons.
   b. (Optional) Monitor the status of the process under **Status**.

Starting and Stopping PDC Processes

You start and stop PDC processes from the home page of the administration server target to which PDC is deployed.

To start or stop PDC processes:

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

2. Navigate to the PDC target's home page as described in "Viewing Home Pages".
3. In the **Quick Links** region, select **Process Management**.

   The home page for the PDC administration server within the WebLogic Server domain appears.
4. Click **Start Up** or **Shut Down**.

   The Start Up or Shut Down page appears.
5. Provide details as needed for your environment and click **OK**.

   See the discussion of shutting down, starting up, or restarting a Middleware target in *Oracle Enterprise Manager Cloud Control Oracle Fusion Middleware Management Guide* for information about the details you can provide on the Start Up or Shut Down page.

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.

Managing Configuration

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

- Viewing Configurations: Applies to BRM, ECE, NCC, Offline Mediation Controller, OSM, PDC, and UIM.
- Editing BRM Configurations: Applies to BRM system and component targets.
- Comparing Configurations: Applies to BRM, ECE, NCC, Offline Mediation Controller, OSM, PDC, and UIM.

You can view, edit, and compare configuration of custom BRM components, such as cloned data managers, in the same way as for ready-to-use components. Configuration management for custom components requires that a **pin.conf** file exists in the *BRM_*

home/**sys**/*custom_component* directory, where *custom_component* is the name of the custom component.

Enterprise Manager Cloud Control retains configuration changes and history as part of Configuration Management. See the chapter about 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 Configurations

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

To view configurations:

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 configurations, as described in "Viewing Home Pages".
3. Under the target's name, from the target type menu, select **Configuration** and then one of the following:
   - For 12c, **Last Collected**.
   - For 13c, **Latest**.

   The configuration viewer for the selected target appears.

Table 4–11 describes the configuration viewer tabs.

Table 4–11 Configuration Viewer Tabs

Tab	Description
Configuration Properties	Displays general configurations for the target, including host information, configuration parameters, and important directories. Selecting elements or system members in tree table displays the configurations related to those elements.
System Structure	Shown for system targets, contains an expandable and selectable listing of the system's installed and managed targets.
Immediate Relationship	Displays the immediate relationships of the target to other selectable targets.
Member Of	Lists selectable target component's membership in system targets.
Uses	Lists selectable targets used by the target.
Used By	Lists selectable targets using the target.

Editing BRM Configurations

You can edit configuration files for BRM targets by using Enterprise Manager Cloud Control.

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 "About 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.

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 about BRM configuration files and parameters.

Comparing Configurations

You can compare two or more target configurations of the same type, as well as 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.

When comparing target configurations, you can use comparison templates. Comparison templates let you control which configuration parameters to compare. Application Management Pack for Oracle Communications provides a set of templates that you can use and extend.

If you are using Enterprise Manager Cloud Control 13c, you apply comparison templates dynamically to thousands of targets and review overall results in the Drift dashboard.

For more information about configuration comparisons, including instructions for using the Comparison Wizard and drift management, see the overview of comparisons and templates in *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

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 and OSM targets deployed on Oracle RAC databases, you must manually associate the database with the target from the BRM or OSM target's home page. See "Associating Oracle RAC Database Targets with BRM and OSM 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. Navigate to the home page for the target for which you want to view topology, as described in "Viewing Home Pages".
     b. 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.

Application Management Pack for Oracle Communications provides the following ready-to-use compliance frameworks which you can use to evaluate whether your configurations conform to Oracle's recommendations:

- OSS Compliance Framework: For OSM and UIM deployments on Fusion Middleware 11g and 12c.
- Communications Integration Compliance Framework: For Oracle AIA deployments on Fusion Middleware 11g and 12c.

The OSS and integrations compliance frameworks let you ensure that the targets and in your production systems are configured consistently across multiple systems and environments. You can use the provided frameworks to create similar frameworks 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.

The OSS and integrations frameworks are extensions of 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*.

About the Compliance Frameworks

The OSS and integrations compliance frameworks consists of the following compliance standards:

- OSS Compliance Framework:
  - 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.
  - UIM Compliance Standard: Defines compliance rules applicable to UIM targets.
  - UIM Compliance Standard - WebLogic Patches: Defines compliance rules applicable to WebLogic Server domain targets. The rules evaluate whether the appropriate patches for UIM have been applied to the WebLogic Server domains.
- Communications Integration Compliance Framework:
  - Communications Integration Compliance Standard: Defines compliance rules applicable to Oracle AIA targets.

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 compliance frameworks are intended for production systems. If your configuration differs for development or test systems, you can copy the system-defined frameworks and use them 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.

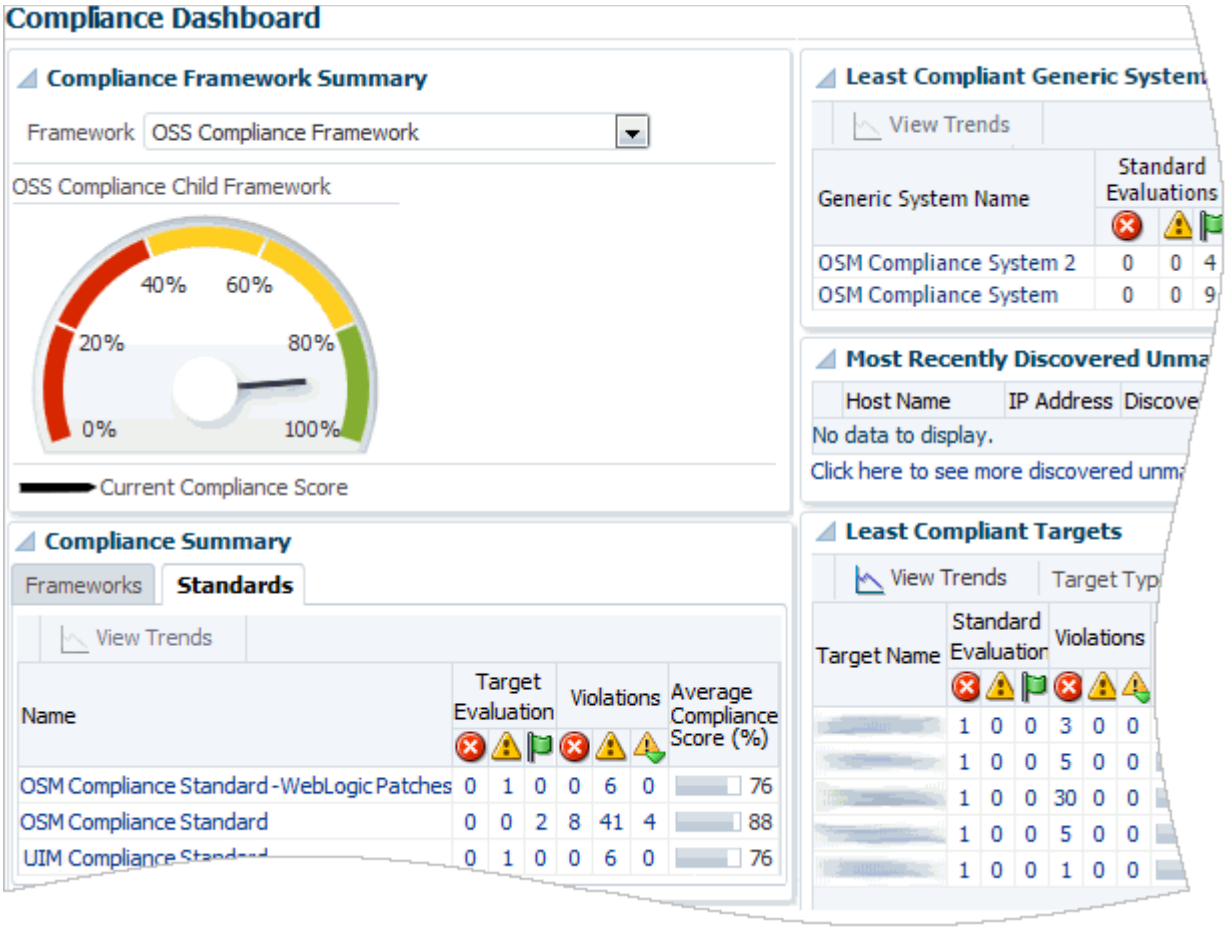
About Monitoring Compliance

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 Compliance".

For an overall view of the compliance for all the targets associated with the standards within a compliance framework, you use the Compliance Dashboard. Figure 4–1 shows the Compliance Dashboard for the OSS compliance framework.

Figure 4–1 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 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.

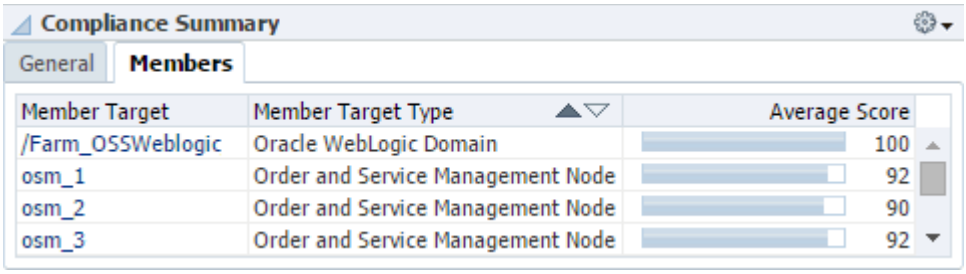
See *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for detailed information about accessing compliance features and using the compliance dashboard and results pages effectively.

About Monitoring OSM Compliance

In addition to monitoring the compliance of individual OSM nodes, you can use a generic system to monitor the compliance of an entire OSM system. The generic system should include 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. See "Creating Generic Systems for Monitoring OSM System Compliance".

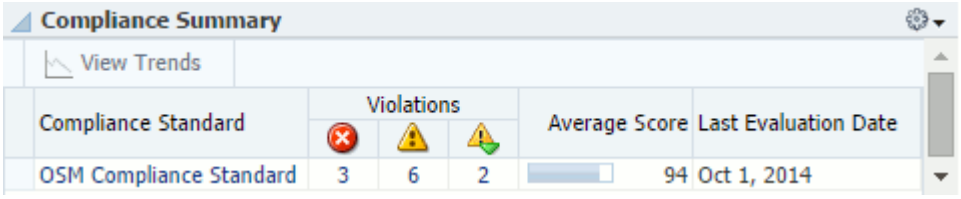
The Compliance Summary region, shown in Figure 4–2, provides an overall compliance score for the entire generic system, and an individual score for each member of the system.

Figure 4–2 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 4–3, provides a summary of compliance evaluations, violations, and scores for the selected OSM node.

Figure 4–3 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.

For information about OSM compliance rules, see *Oracle Communications Order and Service Management System Administrator's Guide*.

Monitoring Compliance

Monitoring compliance includes the following tasks:

- (Optional) Viewing Compliance Standards and Rules
- (Optional) Creating Generic Systems for Monitoring OSM System Compliance
- Associating Compliance Standards with Targets
- Monitoring Compliance Summary and Results

Viewing Compliance Standards and Rules

You can view compliance standards and the rules that they include at any time, whether or not you have associated them with targets.

To view compliance standards and the rules that they include:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Enterprise** menu, select **Compliance** and then **Library**.
3. Do any of the following:
   - To view the list of rules within a compliance standard, 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**, **UIM Compliance Standard**, or **Communications Integration Compliance Standard** and click **Search**.

        A list of compliance standards appears.
     c. Select the link for the compliance standard for which you want to view rules.

        The list of rules within the selected compliance standard appears.
     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, UIM, or Oracle AIA targets:
     a. Click the **Compliance Standard Rules** tab.
     b. In the Search region, from the **Applicable To** list, select **Order and Service Management Node**, **Unified Inventory Management**, or **Oracle Communications Integration**.
     c. From the **System-Defined** menu, select **Yes**.
     d. Click **Search**.

        All system-defined rules that can apply to the selected target type 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 or UIM WebLogic patches standards. To determine which rules are part of the OSM and UIM WebLogic patches standards, 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 Compliance Standards with Targets

If you want to monitor compliance for OSM 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 compliance standards with targets:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. From the **Enterprise** menu, select **Compliance,** and then **Library**.
3. Click the **Compliance Standards** tab.
4. In the Search area, enter **OSM Compliance Standard**, **UIM Compliance Standard**, or **Communications Integration Compliance Standard** and click **Search**.

   A list of compliance standards appears.
5. From the list of compliance standards, highlight the relevant compliance standard and click the **Associate Targets** button.

   The Target Association for Compliance Standard page appears.
6. Click the **Add** button.
7. Select the targets for which you want to evaluate compliance and click **Select**.
8. Click **OK**.

   The compliance standard is associated with the targets.
9. For OSM and UIM targets only:
   a. From the list of compliance standards, highlight **OSM Compliance Standard - WebLogic Patches** or **UIM Compliance Standard - WebLogic Patches** and click the **Associate Targets** button.
   b. Click the **Add** button.
   c. Select the WebLogic Server domain target on which the OSM or UIM targets are deployed and click **Select**.
   d. Click **OK**.

      The compliance standard is associated with the WebLogic Server domain targets.

Monitoring Compliance Summary and Results

To monitor compliance results:

1. Log in to the Enterprise Manager Cloud Control administration console.
2. 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** or **Communications Integration Compliance Framework**.

   The overall score for the compliance framework appears.

c. In the Least Compliant Targets region, from the **Target Type** menu, select any of the following options, then click anywhere outside the menu:

   – **Oracle Communications Integration**

   – Order and Service Management Node

   – Oracle WebLogic Domain

   – Unified Inventory Managemen

   The table shows only the selected target type.

   Note: When you select Oracle WebLogic Domain, some domains that appear may not be domains on which OSM or UIM 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 compliance frameworks:

   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, UIM, or integration compliance standard.

      – Click the **Compliance Frameworks** tab, and then click **OSS Compliance Framework** or **Communications Integration Compliance Framework.**

      The results for the compliance or 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.

Identifying Discrepancies in Shared Data

The applications integrated by Oracle AIA share account, product, and asset data, and Oracle AIA maintains cross-references for the shared data. Over time, inconsistencies can develop in the shared data, and entities that exist in one application may be inaccurately referenced or entirely missing in another. Data inconsistency problems can be difficult to diagnose and resolve, resulting in failed orders and increased operational expense.

Application Management Pack for Oracle Communications helps you locate inconsistent data by using the Enterprise Manager Cloud Control administration console.

You can generate data discrepancy reports to locate inconsistency in shared data, including missing or invalid references in Oracle AIA and the integrated applications. You can schedule jobs to run regular data discrepancy reports, configure email notifications, review reports in HTML format, and purge reports when they are no longer needed.

After reviewing the reports to locate data inconsistency, you resolve the inconsistency manually.

Data discrepancy reports are not supported if you are using split cross-reference tables.

Configuring Environments for Data Discrepancy Reports

Configuring environments involves the following tasks:

- Adding Environments

- Modifying Environments
- Disabling and Enabling Environments
- Deleting Environments

Adding Environments

To add an Oracle AIA environment for data DISCREPANCY reports:

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

   The Communications Applications landing page appears.
3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.
4. In the Environments region, click **Add**.
5. In the Environment Details region, enter information about the environment in the following fields:
   - **Environment Name**: Enter three letters to represent a name for the environment. Use a distinct name from any other environments you have added to the region.
   - **Description**: Enter a description for the environment.
6. In the Data Sources region, enter information about the databases in the following rows:
   - **Cross Ref. DB**: Enter the host name, port, and system ID for the Oracle AIA cross-reference database. Enter the user name and password for the database user.
   - **Siebel DB**: Enter the host name, port, and system ID for the Siebel customer relationship management (Siebel CRM) database. Enter the user name and password for the database user.
   - **BRM DB**: Enter the host name, port, and system ID for the BRM database. Enter the user name and password for the database user.
7. In the Output Folder region, enter information about where to store the reports in the following fields:
   - (Optional) If you want to store data discrepancy reports on a remote host, enter the details in the following fields:
     - **Host-Name**: Enter the URL of the remote host.
     - **Login User-Name**: Enter the user name for the remote host.
     - **Login Password**: Enter the password of the user name for the remote host.
   - **Location to store the report**: Enter the complete path to the directory where you want to store data discrepancy reports.

   The reports will be stored in the specified location and on the Enterprise Manager Cloud Control server.
8. Click **Save Environment**.

   The environment details are saved in the table and reports for account, asset, and product data discrepancy are added to the Available Reports region.

Modifying Environments

To modify an existing environment:

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

   The Communications Applications landing page appears.
3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.
4. In the Environments region, do one of the following:
   - Modify an individual value:
     a. Select the value that you want to modify.
     b. Enter a new value.
     c. Press **Enter**.
   - Modify multiple values for a single environment:
     a. Highlight an existing environment and click **Modify**.

        The Modify an Environment dialog box appears.
     b. Enter new values for any fields you want to modify and click **Save Environment**.

     The environment details are saved.

Disabling and Enabling Environments

You can temporarily disable all data discrepancy reports for an environment by disabling the environment and enabling it again later.

To disable or enable an environment:

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

   The Communications Applications landing page appears.
3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.
4. In the Environments region, highlight the environments that you want to disable or enable and click **Enable/Disable**.

   The environments are disabled or enabled.

When you disable an environment in this way, it is disabled only in the context of data discrepancy reports. Metric collection, monitoring, and other Enterprise Manager Cloud Control functionality is not disabled.

Deleting Environments

To delete an Oracle AIA environment from the data discrepancy page:

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

   The Communications Applications landing page appears.

3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.

4. In the Environments region, highlight the environments that you want to delete and click **Delete**.

   The environment details are deleted and the environment is removed from the table.

When you delete an environment in this way, it is deleted only in the context of data discrepancy reports. The Oracle AIA target and application targets are not deleted from Enterprise Manager Cloud Control.

Configuring Data Discrepancy Reports

By default reports to identify discrepancies in account, asset, and product data are scheduled to run for each enabled environment every 24 hours. To avoid overloading the databases, the time that each report runs is offset by one hour for each data type. The default reports compare data from the last 7 days.

You can perform the following tasks to configure data discrepancy reports:

- Changing Report Schedules
- Running On-Demand Reports
- Disabling and Enabling Reports

You can also view the percentage of successful and failed reports by viewing the Report Statistics region of the Oracle Communications Data Discrepancy page.

Changing Report Schedules

To change a data discrepancy report schedule:

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

   The Communications Applications landing page appears.

3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.

4. In the Available Reports region, highlight a report and click **Schedule**.
5. From the **Schedule Time** menu, select the frequency with which to generate reports. The default is 24 hours.
6. From the **Fetch** menu, select the duration of time during which to collect data for the reports. The default is the last 7 days.
7. For Accounts reports only, from the **Account Type** menu, select the account type for which to generate reports.
8. Click **Save**.

   The scheduling details are saved.

Running On-Demand Reports

To run a data discrepancy report on-demand:

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

2. From the **Targets** menu, select **Communications Applications**.

   The Communications Applications landing page appears.

3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.

4. In the Available Reports region, highlight the reports that you want to run and click **Run Now**.

   The reports are run.

5. Review the report status in the Report Activity region.

Disabling and Enabling Reports

You can temporarily disable individual data discrepancy reports for an environment and enable them again later.

To disable or enable an environment:

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

   The Communications Applications landing page appears.

3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.

4. In the Available Reports region, highlight the reports that you want to disable or enable and click **Enable/Disable**.

   The reports are disabled or enabled.

Viewing Data Discrepancy Reports

To view data discrepancy reports:

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

   The Communications Applications landing page appears.

3. Under the availability chart, click **Data Discrepancy**.

   The Oracle Communications Data Discrepancy page appears.

4. In the Report Activities region, select the link for the report you want to view in the Report/Error Location column.

   The report is downloaded to your local machine.

5

Monitoring Billing and Revenue Management

This chapter describes how to monitor Oracle Communications Billing and Revenue Management (BRM) and BRM components using the home pages 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, including custom components such as cloned data managers. 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".

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. Use this region to determine if unavailable components are causing problems.
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. 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. 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. 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. Use this region to identify configuration changes that could be causing problems.
Database	Displays graphs illustrating the database CPU usage, the number of times the database is queried for each transaction, the number of rollbacks over time, tablespace allocated and tablespace used. These graphs will also show any associated Oracle Real Application Clusters databases that you have discovered.

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 and OSM 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".

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. Use this region to determine whether a particular process is causing problems by identifying fluctuations in process performance.
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. 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. 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. 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.

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. 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.

About Viewing Collection Items and Metrics

You can view a list of all metrics collected for a BRM component target and view details about individual metrics, including values, severity, and alerts that are triggered for that metric. See "Viewing Target Metrics".

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.

6

Monitoring Elastic Charging Engine

This chapter describes how to monitor Oracle Billing and Revenue Management (BRM) Elastic Charging Engine (ECE) component targets by using the home pages 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 System Targets

The home page for an ECE system target displays metrics data that you can use to monitor the health of your ECE cluster 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".

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

Table 6–1 Regions on the ECE System Target Home Page

Region	Description
Summary	Displays summary information about the ECE cluster. Contains the **Refresh Cluster** button, which refreshes targets in the cluster with the latest status. You may need to scroll down to see this button.
OMC Instance Type Coherence Aggregate Information	Displays graphs for metrics related to the Oracle Communications Offline Mediation Controller instance integrated with the ECE system.
Host Coherence Performance Indicators	Displays a graph showing the aggregated memory consumed bu and available to the system.

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

Region	Description
System Availability	Displays the number of nodes in the cluster that are up and down and gives details about the nodes affected most in the last 24 hours. Use this region to identify which nodes are causing problems and to access the home pages for those nodes.
ECE Oracle Coherence Information	Displays the status of the Oracle Coherence targets in the ECE cluster.
Incidents/Violations	Displays the number of critical, warning, and escalated incidents and violations. Use this region to identify problems based on high numbers of incidents.
Quick Links	Provides links to the topology viewer and performance metrics for the ECE cluster.
Log Files Contents	Provides a link to the ECE cluster log files.

About the Monitoring Home Page for ECE Node Targets

The home page for an ECE node 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 ECE node home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Table 6–2 describes the regions on the home page for ECE node targets.

Table 6–2 Regions on the ECE Node Target Home Page

Region	Description
Summary	Displays summary information about the ECE node. Contains **Stop** and **ReStart** buttons for controlling the ECE node.
Availability Summary	Displays the availability of the target in the last 24 hours.
Incidents/Violations	Displays the number of critical, warning, and escalated incidents and violations. Use this region to identify problems based on high numbers of incidents.
ECE Coherence Cache Objects	Displays information about the Oracle Coherence cache objects for the ECE node.
Key Indicators	Displays graphs showing available and used memory, the size of the send queue, and the send and receive success rates.
Quick Links	Provides links to the topology viewer and performance metrics for the ECE cluster.
Log Files Contents	Provides a link to the ECE cluster log files.

About Viewing Collection Items and Metrics

You can view a list of all metrics collected for an ECE system or node target and view details about individual metrics, including values, severity, and alerts that are triggered for that metric. See "Viewing Target Metrics".

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.

7

Monitoring Network Charging and Control

This chapter describes how to monitor Oracle Communications Network Charging and Control (NCC) targets by using the home pages 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".

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.
Availability	Displays the number of components that are up and down and gives details about the components affected most in the last 24 hours. 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. 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 NCC is deployed, including CPU and memory use. Use this region to determine whether a particular host is causing problems by identifying fluctuations in host performance.
Database	Displays graphs illustrating the database CPU usage, the number of times the database is queried for each transaction, the number of rollbacks over time, tablespace allocated and tablespace used.

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

Table 7–2 Regions on the NCC Component Home Pages

Region	Description
Summary	Displays details about the NCC component target, including instance name, host, and installation and log directories. Contains **Stop** and **Restart** buttons for controlling the NCC component.
Configuration Changes	Displays the number of configuration changes and provides a link to the list of configuration changes for the target. Use this region to view configuration changes that could be causing problems.
Availability Summary	Displays the availability of the target in the last 24 hours.
Quick Links	Provides links to Enterprise Manager Cloud Control tasks related to the target. If a database was registered for this target during discovery and promotion, a link to the database monitoring page appears here.

Table 7–2 (Cont.) Regions on the NCC Component Home Pages

Region	Description
Incidents/Violations	Displays details about incidents and violations for the component. Use this region to identify and resolve incidents.
Log Files Contents	Provides a link to the log files for the component.
Host Performance Data	Displays graphs of queue length, memory and CPU utilization, and disk and network usage.

About Viewing Collection Items and Metrics

You can view a list of all metrics collected for an NCC or NCC component target and view details about individual metrics, including values, severity, and alerts that are triggered for that metric. See "Viewing Target Metrics".

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.

8

Monitoring Offline Mediation Controller

This chapter describes how to monitor the Oracle Communications Offline Mediation Controller by using the home page provided by Oracle Application Management Pack for Oracle Communications.

About Monitoring Offline Mediation Controller

Application Management Pack for Oracle Communications enables monitoring Offline Mediation Controller systems and nodes 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 Offline Mediation Controller 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 Offline Mediation Controller System Targets

The Offline Mediation Controller system is represented by an Offline Mediation Controller administration server target. The home page for the administration server target displays metrics data that you can use to monitor the health of your Offline Mediation Controller system and identify problems. See "Viewing Home Pages" for information about accessing Offline Mediation Controller home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Table 8–1 describes the regions on the home page for Offline Mediation Controller administration server targets.

Table 8–1 Regions on the Administration Server Home Page

Region	Description
Summary	Displays the instance name, type, host, and port, the JRE version, the report output directory and format, and the Offline Mediation Controller version number. Contains **Stop** and **Restart** buttons for controlling the Offline Mediation Controller system.
OMC Member Status	Displays the percent of nodes in the system that are up and down. Contains **Stop**, **Start**, and **Restart** buttons for controlling the nodes selected in the table. Use this region to determine if unavailable nodes are causing problems and to stop, start, and restart nodes.
Configuration Changes	Displays the number of configuration changes and provides a link to the list of configuration changes for the target. Use this region to view configuration changes that could be causing problems.
Availability Summary	Displays the number of nodes in the system that are up and down and gives details about the nodes affected most in the last 24 hours. Use this region to identify which nodes are causing problems and to access the home pages for those nodes.
Quick Links	Provides links to Enterprise Manager Cloud Control tasks related to the target, such as viewing detailed performance metrics.
Process CPU and Memory Utilization	Displays the CPU and memory usage of the Offline Mediation Controller processes.
Log Files Contents	Provides a link to the Offline Mediation Controller log files.
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. Use this region to identify and resolve incidents.
Host Performance Data	Displays performance information, including CPU and memory usage, for the host on which the target is deployed.
NodeManagers List	Displays summary information about the nodes in the system. Includes status, target name, port, and host. Use this region to get a high-level view of all the nodes in your Offline Mediation Controller system.

About the Monitoring Home Page for Offline Mediation Controller Nodes

The home page for an Offline Mediation Controller node 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 Offline Mediation Controller node home pages. You can access the target's configuration topology from the home page as described in "Viewing Topology".

Table 8–2 describes the regions on Offline Mediation Controller node home pages.

Table 8–2 Regions on Offline Mediation Controller Node Home Pages

Region	Description
Summary	Displays the instance name, type, host, and port, the JRE version, the setting for Node Manager control, and the Offline Mediation Controller version number. Contains **Stop** and **Restart** buttons for controlling the node.
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. Use this region to identify configuration changes that could be causing problems.
Availability Summary	Displays the availability of the target in the last 24 hours.
Node Details	Displays details about the node, including ID, name, type, file, cartridge name, status, and a link to the log files.
Process CPU and Memory Utilization	Displays the CPU and memory usage of the Offline Mediation Controller processes.
Log Files Contents	Provides a link to the log files for the node.
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. Use this region to identify and resolve incidents.
Host Performance Data	Displays performance information, including CPU and memory usage, for the host on which the target is deployed.

Viewing Collection Items and Metrics

You can view a list of all metrics collected for an Offline Mediation Controller system or target and view details about individual metrics, including values, severity, and alerts that are triggered for that metric. See "Viewing Target Metrics".

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.

9

Monitoring Pricing Design Center

This chapter describes how to monitor the Oracle Communications Billing and Revenue Management (BRM) Pricing Design Center (PDC) component by using the home page provided by Oracle Application Management Pack for Oracle Communications.

About Monitoring PDC

Application Management Pack for Oracle Communications enables monitoring PDC 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 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 PDC

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

Table 9–1 describes the regions on the home page for PDC targets.

Table 9–1 Regions on the PDC Home Page

Region	Description
Summary	Displays summary information about the target, including important directories and names.
Configuration Changes	Displays the number of configuration changes and provides a link to the list of configuration changes for the target.
Availability Summary	Displays the availability of the target in the last 24 hours.
Quick Links	Provides links to Enterprise Manager Cloud Control tasks related to the target.

Table 9–1 (Cont.) Regions on the PDC Home Page

Region	Description
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.
System Availability	Displays information about the availability of servers related to the target, currently and over the last 24 hours.
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. Use this region to identify and resolve incidents.
Log Files Contents	Provides a link to the PDC log files, including logs for the domain, synchronization, and the transformation engine.
Host Performance Data	Displays performance information for the host on which NCC is deployed, including CPU and memory use. Use this region to determine whether a particular host is causing problems by identifying fluctuations in host performance.
Database	Displays graphs illustrating the database CPU usage, the number of times the database is queried for each transaction, the number of rollbacks over time, tablespace allocated and tablespace used.

About Viewing Collection Items and Metrics

You can view a list of all metrics collected for a PDC target and view details about individual metrics, including values, severity, and alerts that are triggered for that metric. See "Viewing Target Metrics".

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.

10

Monitoring Operations Support Systems

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

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".

Table 10–1 describes the regions on the home page for communications suite targets.

Table 10–1 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.
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".

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.

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.

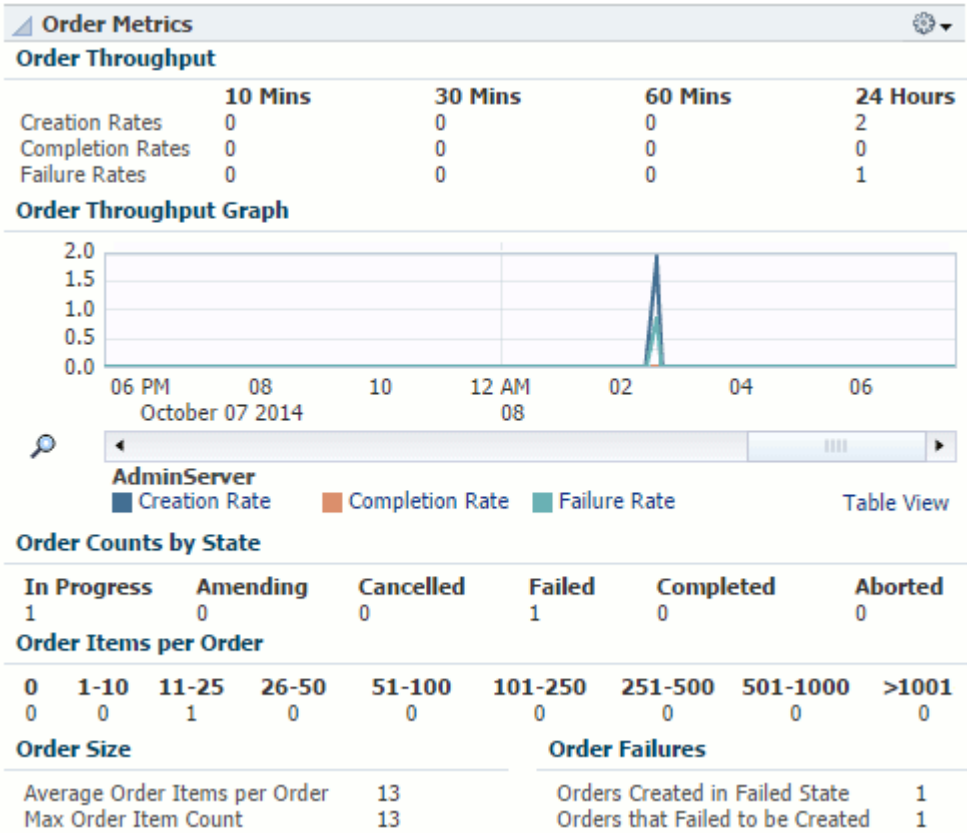
About the Order Metrics Region

The Order Metrics region helps you assess how well your system is processing orders.

This region, shown in Figure 10–1, 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 10–1 Order Metrics Region of the Dashboard Tab



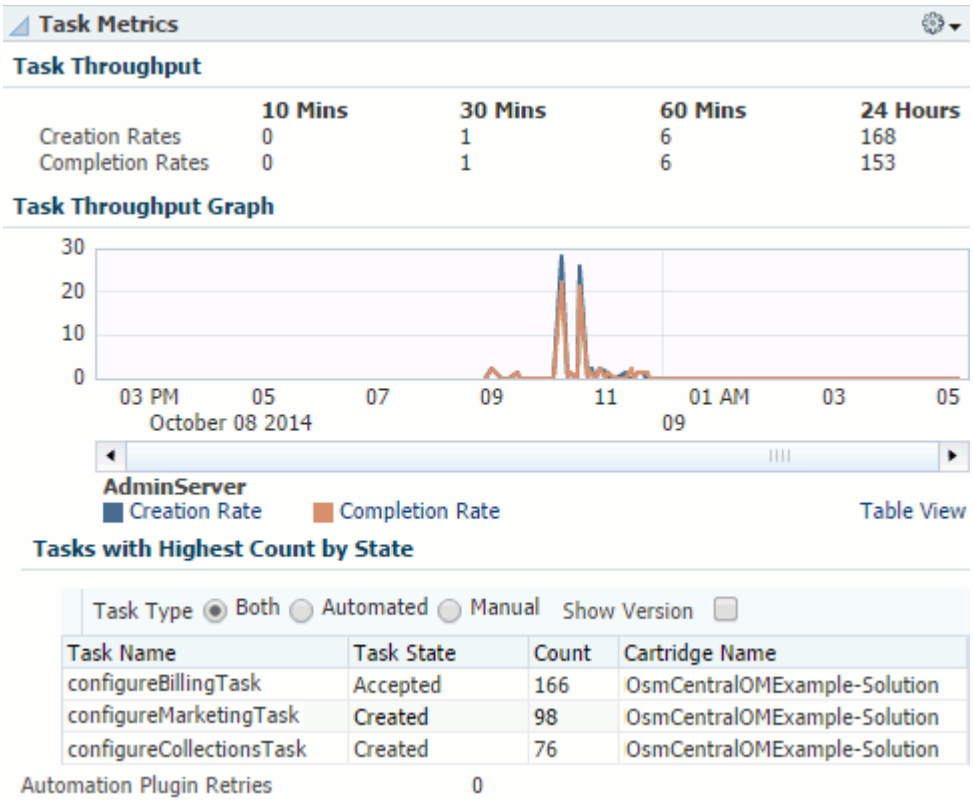
About the Task Metrics Region

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 10–2, 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 10–2 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.

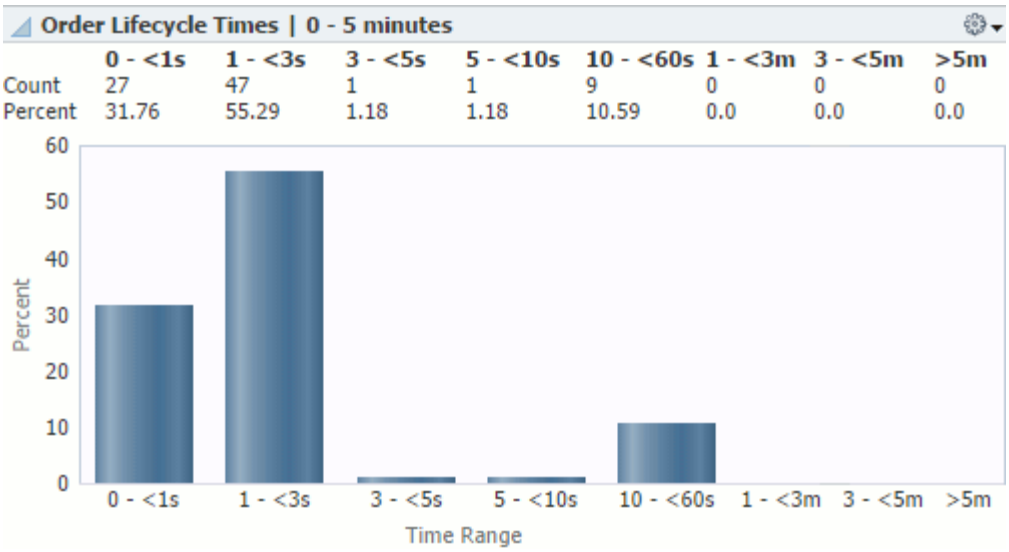
About the Order Lifecycle Times Region

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 10–3, 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 10–3 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.

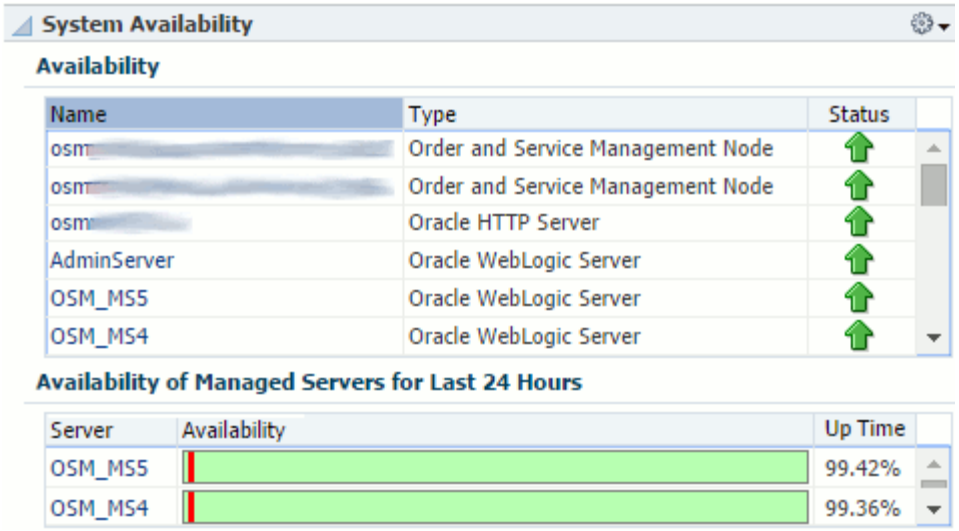
About the System Availability Region

The System Availability region helps you identify problems with individual servers and assess the overall health of your system.

This region, shown in Figure 10–4, 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 10–4 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.

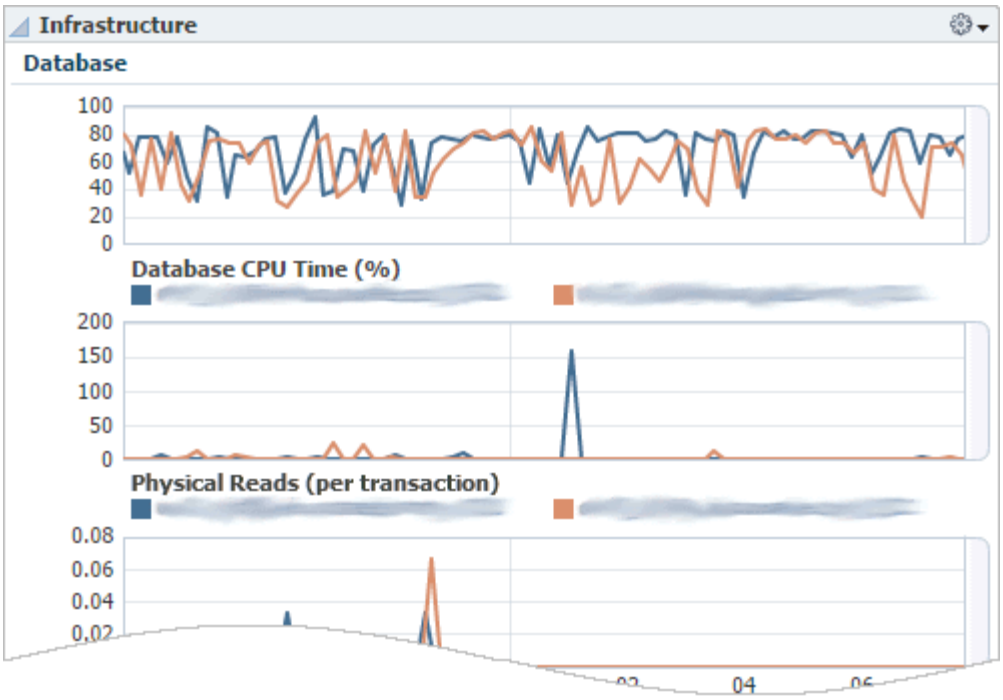
About the Infrastructure Region

The Infrastructure region helps you assess the health and performance of your system's infrastructure components.

This region, as shown in part in Figure 10–5, 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, the number of rollbacks over time, tablespace allocated and tablespace used. These graphs will also show any associated Oracle Real Application Clusters databases that you have discovered.

Figure 10–5 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 Associate RAC Database to OSM Target Region

This region lets you associate an Oracle Real Application Clusters (Oracle RAC) database to the OSM system target for viewing on the topology page.

You associate the Oracle RAC database with the OSM system target by clicking the **Associate RAC Database** button. If the OSM system 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 and OSM Targets" for information about the tasks required to associate an Oracle RAC database with an OSM system target.

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".

Table 10–2 describes the regions on the home page for OSS application targets.

Table 10–2 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.
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.

Table 10–2 (Cont.) Common Regions on OSS Application Home Pages

Region	Description
Compliance Summary	Displays displays a summary of compliance evaluations, violations, and scores for the OSM node. Only appears for OSM nodes. See "Managing 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.

About Viewing Collection Items and Metrics

You can view a list of all metrics collected for an OSS target and view details about individual metrics, including values, severity, and alerts that are triggered for that metric. See "Viewing Target Metrics".

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.

11

Monitoring Oracle Communications Integrations

This chapter describes how to monitor Oracle Communications Integration targets in Enterprise Manager Cloud Control by using the home page provided by Oracle Application Management Pack for Oracle Communications.

About Monitoring Integrations

Oracle Communications 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 Oracle Communications 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 Oracle Communications 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 Oracle Communications 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".

Table 11–1 describes the regions shown on the Dashboard tab of the home page for Oracle Communications Integration targets.

Table 11–1 Regions on the Dashboard Tab of the Integration Home Page

Region	Description
Integration Configuration Summary	Displays version numbers and dates for Oracle AIA and SOA integration packs and patches. Does not appear for Communications Integration targets for which the Oracle AIA instance is not installed on the same host as the Management Agent.
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. Does not appear for Communications Integration targets for which the Oracle AIA instance is not installed on the same host as the Management Agent.
Integrated Edge Applications	Provides the status of the BRM and OSM instances that the Oracle Communications Integration target integrates. 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. Use this region to determine whether a particular host is causing problems by identifying fluctuations in host performance.

Table 11–2 describes the regions on the Fault Order Details tab of the home page for Oracle Communications Integration targets.

Table 11–2 Regions on the Fault Order Details Tab of the Integration Home Page

Region	Description
Integration Fault Summary	Displays the total number and percentage of business, system, and data faults. Use this region to identify and resolve faults. 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. 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.
Order Throughput	Displays the number of incoming and failed orders for the last 24 hours in a list and a graph. 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.

Configuring Integrated Applications for Status Monitoring

After you have discovered an Oracle Communications 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 Oracle Communications 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.
2. Navigate to the home page for the Oracle Communications Integration target for which you want to configure integrated applications, as described in "Viewing Home Pages".
3. In the Integrated Edge Applications region, select an application row and click **Configure Edge Application Details**.
4. In the **Hostname** field, enter the host on which the application is deployed.
5. 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.
6. 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 Oracle Communications 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 Oracle Communications 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. Navigate to the home page for the Oracle Communications Integration target for which you want to view faults, as described in "Viewing Home Pages".
3. Click the **Fault Order Details** tab.
4. 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.
5. 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. Navigate to the home page for the Oracle Communications Integration target for which you want to recover from system faults, as described in "Viewing Home Pages".
3. Click the **Fault Order Details** tab.
4. 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.
5. Click the **Faults and Rejected Messages** tab.
6. In the Search panel, set the search criteria. Ensure that you select **Recoverable** from the **Fault** list.
7. Click **Search**.
8. In the Faults and Rejected Messages table, select up to 5 faults.
9. From the **Recovery Options** menu, select a recovery action.

   A message is displayed indicating whether the recovery job can be submitted successfully.
10. Click **OK**.

    The fault recovery job is run.
11. 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.

About Viewing Collection Items and Metrics

You can view a list of all metrics collected for an Integration target and view details about individual metrics, including values, severity, and alerts that are triggered for that metric. See "Viewing Target Metrics".

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.