

Oracle® Enterprise Manager Ops Center

Administration Guide

12c Release 2 (12.2.2.0.0)

E38534-08

February 2015

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	ix
Audience	ix
Documentation Accessibility	ix
Related Documents	ix
Conventions	x
1 Introduction to Administration	
2 Infrastructure	
Introduction to Infrastructure	2-1
Viewing Infrastructure	2-2
Viewing Agent Controllers	2-2
Viewing Proxy Controllers	2-2
Viewing the Enterprise Controller Configuration	2-3
Using Connection Modes	2-4
Switching to Disconnected Mode	2-4
Switching to Connected Mode	2-4
Using the Harvester	2-4
Identifying a Harvester System	2-5
Downloading the Harvester Bundle	2-5
Using the Harvester Script	2-5
Copying Content to the Enterprise Controller in Disconnected Mode	2-8
Copying a Knowledge Base Bundle	2-8
Copying a Knowledge Base Bundle and All Patches	2-8
Copying a Knowledge Base Bundle and Incremental Patches	2-8
Configuring Local Agent Controllers	2-9
Configuring the Local Agent Controller on the Enterprise Controller	2-9
Unconfiguring the Local Agent Controller on the Enterprise Controller	2-9
Configuring a Local Agent Controller on a Proxy Controller	2-10
Unconfiguring a Local Agent Controller on a Proxy Controller	2-10
Configuring Oracle Configuration Manager	2-10
Registering the Enterprise Controller	2-11
Running a Self Diagnosis	2-11
Viewing and Changing the Enterprise Controller and Proxy Controller Status	2-12
Checking the Status of the Enterprise Controller	2-12

Starting the Enterprise Controller.....	2-12
Stopping the Enterprise Controller	2-13
Checking the Status of a Proxy Controller	2-13
Starting a Proxy Controller	2-14
Stopping a Proxy Controller	2-14
Putting a Proxy Controller in Maintenance Mode	2-14
Removing a Proxy Controller from Maintenance Mode	2-15
Managing Proxy Controller Networks	2-15
Associating Networks With a Proxy Controller	2-15
Enabling or Disabling Networks for a Proxy Controller.....	2-15
Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration	2-16
Configuring DHCP and Subnets for OS Provisioning.....	2-16
About DHCP	2-17
Configuring DHCP	2-18
About Subnets	2-19
Configuring Subnets.....	2-19
About External DHCP Servers.....	2-20
Configuring External DHCP Servers	2-22
Configuring the Enterprise Controller for WAN Boot	2-23
Checking the WAN Boot Status	2-23
Changing the Default Port for Oracle Solaris 11 WAN Boot.....	2-23
Enabling or Disabling WAN Boot	2-24
Editing Oracle Solaris 11 Credentials.....	2-24
Retaining Migration Scripts in Server Pools	2-25
Generating a Default Set of OS Provisioning Profiles and Plans	2-25
Displaying Related Assets In Groups	2-25
Changing the HTTP Proxy.....	2-26

3 Database Management

Introduction to Database Management	3-1
Installing and Configuring a Customer-Managed Database	3-2
Migrating to a Customer-Managed Database.....	3-4
Changing the Customer-Managed Database Location	3-5
Verifying the Database	3-7
Upgrading a Customer-Managed Database.....	3-7
Changing the Database Credentials	3-7
Changing the Database Credentials for the Ops Center User	3-7
Changing the Database Credentials for the Read-Only User	3-8
Defragmenting an Embedded Database.....	3-9
Consolidating Reports Data on a Customer-Managed Database	3-10

4 General Administration

Introduction to General Administration	4-1
Viewing and Understanding Service Statuses	4-1
Viewing Service Status	4-2
Viewing Logs	4-2
Adding a Product Alias	4-3

Adding or Editing Authentications	4-3
Editing the Energy Cost	4-4

5 OCDocor

Introduction to the OCDocor.....	5-1
Downloading the OCDocor	5-1
Performing Preinstallation Checks.....	5-2
Performing Troubleshooting and Tuning.....	5-2
Updating the OCDocor	5-3
Determine the Number of Asset Access Points.....	5-4
Viewing the Access Point Count for Your Environment	5-4
Viewing the Access Point List for Each Proxy Controller.....	5-5
Viewing the Access Point Types for Each Proxy Controller.....	5-5
Viewing All Access Point Data	5-5

6 Auto Service Request

Introduction to ASR.....	6-1
Overview of ASR.....	6-1
Prerequisites.....	6-2
How ASR Activation Works.....	6-3
How ASR Creation Works.....	6-3
Viewing ASR Status for an Asset.....	6-4
Providing Contact Information	6-4
Providing Default Contact Information.....	6-4
Providing Contact Information for an Asset or Group	6-5
Enabling ASR.....	6-5
Disabling ASR	6-6
Blacklisting an Asset	6-6
Testing ASR.....	6-6

7 User and Role Management

Introduction to User and Role Management	7-1
Adding a User	7-2
Deleting a User	7-2
Viewing User Role Details	7-2
Adding a Directory Server.....	7-3
Synchronizing Remote Users and Roles.....	7-4
Synchronizing Remote Users and Roles With One Directory Server.....	7-5
Synchronizing Remote Users and Roles With All Directory Servers.....	7-5
Deleting a Directory Server.....	7-5
About Roles and Permissions	7-5
How Roles are Mapped to Permissions.....	7-5
How Permissions are Mapped to Tasks	7-16
Managing Roles	7-21
Replicating a User	7-21
About Notification Profiles	7-22

Configuring a Notification Profile	7-22
Deleting a Notification Profile	7-23
Viewing the Audit Log	7-24

8 Backup and Recovery

Introduction to Backup and Recovery	8-1
Backing Up and Restoring an Enterprise Controller	8-2
Backing Up an Enterprise Controller	8-2
Restoring an Enterprise Controller	8-3
Backing Up and Restoring a Proxy Controller	8-5
Backing Up a Proxy Controller	8-6
Restoring a Proxy Controller	8-6

9 High Availability

Introduction to High Availability	9-1
Enterprise Controller High Availability	9-1
Proxy Controller High Availability	9-3
Enabling and Using Enterprise Controller High Availability	9-3
Converting a Single Enterprise Controller to High Availability	9-4
Preparing for High Availability with Oracle Clusterware	9-4
Making the Current Enterprise Controller the Primary Node	9-5
Installing a Standby Node	9-5
Converting a High Availability Configuration to a Single Enterprise Controller	9-9
Performing a Manual Relocate	9-9
Managing HA Network Resources	9-10
Adding a Network Resource	9-10
Modifying a Network Resource	9-10
Removing a Standby Enterprise Controller Node	9-11
Checking the Status of the Enterprise Controller Cluster	9-11
Shutting Down the Enterprise Controller Temporarily Without Relocating	9-11
Accessing the Cluster Management UI	9-11
Enabling and Using Proxy Controller High Availability	9-12
Enabling Automatic Failover	9-12
Disabling Automatic Failover	9-12
Setting the Relative Power for Proxy Controllers	9-13
Recovering After an Automatic Failover	9-14
Migrating Assets Between Proxy Controllers	9-14
Migrating Assets from a Failed Proxy Controller	9-15

10 Upgrading

Introduction to Upgrading	10-1
Versions Supported for Upgrade	10-1
Upgrading From Version 12.2	10-1
Upgrading From Version 12.1	10-1
Upgrading From Version 11g	10-2
Planning The Upgrade	10-2

Database Requirements.....	10-3
Upgrading Your Environment.....	10-3
11 Uninstalling and Unconfiguring	
Introduction to Uninstalling and Unconfiguring	11-1
Uninstalling and Unconfiguring Agent Controllers	11-1
Uninstalling and Unconfiguring Agent Controllers from the User Interface	11-1
Uninstalling and Unconfiguring Agent Controllers from the Command Line	11-2
Uninstalling and Unconfiguring a Proxy Controller	11-3
Unconfiguring and Uninstalling a Proxy Controller from the User Interface	11-3
Removing a Proxy Controller from the User Interface.....	11-3
Unconfiguring a Proxy Controller from the Command Line	11-4
Uninstalling a Proxy Controller from the Command Line	11-4
Uninstalling and Unconfiguring the Enterprise Controller	11-5
Unconfiguring the Enterprise Controller	11-5
Uninstalling the Enterprise Controller.....	11-5
A Command Line Administration	
Configuring the Enterprise Controller: ecadm	A-1
Synopsis.....	A-1
Options	A-1
Subcommands	A-1
Subcommand options.....	A-3
Exit status	A-7
Configuring the Proxy Controller: proxyadm	A-7
Synopsis.....	A-7
Options	A-7
Subcommands	A-8
Subcommand options.....	A-8
Exit status	A-9
Configuring the Agent Controller: agentadm	A-9
Synopsis.....	A-9
Usage.....	A-10
Options	A-10
Subcommands	A-10
Subcommand options.....	A-11
Index	

Preface

The Oracle® Enterprise Manager Ops Center Administration Guide describes advanced management and administration tasks.

Audience

This document is intended for senior system administrators.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle Enterprise Manager Ops Center 12c documentation set:

- *Oracle Enterprise Manager Ops Center Release Notes*
- *Oracle Enterprise Manager Ops Center Concepts Guide*
- *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*
- *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*
- *Oracle Enterprise Manager Ops Center Feature Reference Guide*
- *Oracle Enterprise Manager Ops Center Feature Reference Appendix Guide*
- *Oracle Enterprise Manager Ops Center Command Line Interface Guide*
- *Oracle Enterprise Manager Ops Center Deploy How To Library*
- *Oracle Enterprise Manager Ops Center Operate How To Library*
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle Enterprise Manager Ops Center Guide*

For more information, see the other documents in the Oracle Enterprise Manager Ops Center 12c Release 2 documentation set, located at this site:
http://docs.oracle.com/cd/E40871_01/index.htm

Conventions

The following text conventions are used in this document:

Convention	Meaning
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands, file names, and directories within a paragraph, and code in examples.

Introduction to Administration

This document provides an explanation of the Oracle Enterprise Manager Ops Center administration features.

Oracle Enterprise Manager Ops Center includes a variety of administrative features that you can use to maintain and manage the software. You can use these functions to ensure that the software is working effectively and meeting the needs of your environment.

Oracle Enterprise Manager Ops Center is composed of an Enterprise Controller (or multiple Enterprise Controller nodes in a high availability environment), a product database, one or more Proxy Controllers, Agent Controllers that manage operating system assets, and the Knowledge Base. You can monitor, manage, and update this infrastructure to keep the software working.

You can configure Oracle Enterprise Manager Ops Center to create Auto Service Requests (ASRs) for qualified assets when certain incidents occur.

As part of administering your environment, you can add and manage the users that are known to Oracle Enterprise Manager Ops Center, and control what jobs they can launch and what data they can see by giving them roles.

If necessary, you can also uninstall the different pieces of the Oracle Enterprise Manager Ops Center infrastructure.

The following topics are covered:

- **Infrastructure:** Explains how to manage the Enterprise Controller, Proxy Controllers, Agent Controllers, and Knowledge Base.
- **Database Management:** Explains how to manage the embedded or customer-managed product database.
- **General Administration:** Explains how to use several administrative tools, view logs, and supply authentications.
- **OCDoctor:** Explains how to use the OCDoctor tool to check prerequisites and troubleshoot.
- **Auto Service Request:** Explains how to enable Auto Service Requests (ASRs) for qualified assets.
- **User and Role Management:** Explains how to add users from the local system or from a remote directory server and assign them roles.
- **Backup and Recovery:** Explains how to back up the Enterprise Controller and recover it from a backup file.

-
- [High Availability](#): Explains how to set up and manage a high availability configuration for your Enterprise Controller, and how to manage the Proxy Controller high availability feature.
 - [Upgrading](#): Explains how to upgrade to the latest available version of Oracle Enterprise Manager Ops Center.
 - [Uninstalling and Unconfiguring](#): Explains how to uninstall and unconfigure Oracle Enterprise Manager Ops Center.

Infrastructure

The Oracle Enterprise Manager Ops Center infrastructure is the software and connections used by the product. You can manage that infrastructure through the user interface and from the command line.

The following features and topics are covered in this chapter:

- [Introduction to Infrastructure](#)
- [Viewing Infrastructure](#)
- [Using Connection Modes](#)
- [Using the Harvester](#)
- [Configuring Local Agent Controllers](#)
- [Configuring Oracle Configuration Manager](#)
- [Registering the Enterprise Controller](#)
- [Running a Self Diagnosis](#)
- [Viewing and Changing the Enterprise Controller and Proxy Controller Status](#)
- [Managing Proxy Controller Networks](#)
- [Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration](#)
- [Configuring DHCP and Subnets for OS Provisioning](#)
- [Configuring the Enterprise Controller for WAN Boot](#)
- [Editing Oracle Solaris 11 Credentials](#)
- [Retaining Migration Scripts in Server Pools](#)
- [Generating a Default Set of OS Provisioning Profiles and Plans](#)
- [Displaying Related Assets In Groups](#)
- [Changing the HTTP Proxy](#)

Introduction to Infrastructure

This chapter explains how to set up and manage the Oracle Enterprise Manager Ops Center infrastructure.

The Enterprise Controller, Knowledge Base, Proxy Controllers, and Agent Controllers make up the Oracle Enterprise Manager Ops Center infrastructure. The Enterprise Controller generates the UI, routes jobs, communicates with the Knowledge Base, and stores Oracle Enterprise Manager Ops Center data in the Enterprise Controller

Database. The Proxy Controllers directly manage specific assets and carry out jobs. Agent Controllers enable the full range of operating system update and monitoring capabilities on managed operating systems.

You can view and maintain the infrastructure, make changes to its configuration, and configure the connection mode.

Some of the procedures described in this section use the `ecadm`, `proxyadm`, and `agentadm` commands. See [Appendix A, "Command Line Administration"](#) for more information about these commands.

- On Oracle Solaris systems, these commands are in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, these commands are in the `/opt/sun/xvmoc/bin/` directory.

Viewing Infrastructure

You can view the Proxy Controllers and Agent Controllers currently known to Oracle Enterprise Manager Ops Center and see information about their version and status.

Viewing Agent Controllers

You can install Agent Controllers on operating systems and virtualization tools to manage them. You can view them to see information about Agent Controllers, including:

- Asset Name
 - Zone Type
 - Agent Version
 - Upgrade Version
 - Downgrade Version
 - Agent Status (Online or Offline)
1. Click the Assets section of the Navigation pane.
 2. Select a group that contains managed operating systems.
 - Select an operating system smart group from the Operating Systems category, then click the **Summary** tab.
 - Select a user-defined group that contains operating systems, then click the **Membership** tab.
 3. Click the **Agent Controllers** tab.
- Agent Controller information is displayed.

Viewing Proxy Controllers

Proxy Controllers manage assets and perform jobs. You can view the Proxy Controllers to see information about them, including:

- Status (Online or Offline)
- Current Version
- Available Upgrades
- IP Address

- Registration Date

To view a Proxy Controller's configuration:

1. Click the Proxy Controller in the Administration section of the Navigation pane.
2. Click the **Configuration** tab in the Center pane.

The Proxy Controller's configuration is displayed.

Viewing the Enterprise Controller Configuration

You can view and manage the configuration of the Enterprise Controller. The configuration displays the settings for the subsystems that make up the Enterprise Controller.

To view the Enterprise Controller configuration, select the Enterprise Controller in the Administration section of the Navigation pane, then click the configuration tab. Select one of the subsystems listed below to display its settings.

Note: Do not modify these settings unless directed by Oracle.

- Agent Provisioning: Manages the provisioning of Agent Controllers.
- Auto Service Requests: Manages the Auto Service Request (ASR) settings.
- Database: Manages the database used by Oracle Enterprise Manager Ops Center.
- EC Manager: Manages the Enterprise Controller.
- Firmware Provisioning: Manages firmware downloads.
- Job Manager: Manages the way that jobs are run.
- My Oracle Support (MOS): Manages Oracle Enterprise Manager Ops Center's communications with MOS.
- Network/Fabric Manager: Manages networks and fabrics.
- OCDoctor: Manages the OCDoctor location and updates.
- OS Provisioning: Manages network and fabric settings.
- Permission Cache: Manages cache sizes.
- Power: Manages energy cost settings.
- Proxy Manager: Manages the interactions between the parts of the infrastructure.
- Quartz Scheduler: Manages the quartz scheduler.
- Role Preferences: Manages role settings.
- Update: Manages the settings for the Oracle Solaris 11 IPS repository.
- Zone Controller: Manages the zone management settings.
- Auto Service Request: Manages the Auto Service Request (ASR) feature.
- Storage Library Configuration: Manages the settings for storage libraries.
- Virtualization: Manages Oracle VM Server for SPARC failover settings.

Using Connection Modes

Oracle Enterprise Manager Ops Center can operate in either Connected or Disconnected Mode. In Connected Mode, the software communicates with Oracle web sites and other vendors, gathering patch and update information. In Disconnected Mode, the software operates autonomously using a knowledge base bundle downloaded on a separate system using a harvester script and a local Oracle Solaris 11 repository if you are using Oracle Solaris 11, and does not need an Internet connection.

You can switch between connection modes at any time.

Switching to Disconnected Mode

If you are in Connected Mode, or have not selected a connection mode, you can switch to Disconnected Mode. To use Disconnected Mode, you must download a Knowledge Base bundle.

See the *Oracle Enterprise Manager Ops Center Using Disconnected Mode* guide for more information about using Disconnected Mode.

Before switching to disconnected mode, you must obtain a Knowledge Base bundle using the Harvester script. This procedure is described below.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click **Setup Connection Mode** in the Actions pane.
3. Enter the absolute path of the Knowledge Base bundle that you want to use, then click **Load Bundle**. Use the **Browse** button to locate the Knowledge Base bundle if you do not know the absolute path.
4. Click **Switch to Disconnected Mode**.
A confirmation window is displayed.
5. Click **Yes**.

The connection mode is switched to Disconnected Mode.

Switching to Connected Mode

If you are in Disconnected Mode, or have not selected a connection mode, you can switch to Connected Mode. You must have a valid set of My Oracle Support (MOS) credentials in your authentications to use Connected Mode.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click **Setup Connection Mode** in the Actions pane.
3. Click **Switch to Connected Mode**.
A confirmation window is displayed.
4. Click **Yes**.

The connection mode is switched to Connected Mode.

Using the Harvester

The harvester is a script that you can run on an Internet-facing system to create a Knowledge Base bundle and to download OS update and firmware content. To use

disconnected mode, you must use the harvester to obtain a Knowledge Base bundle. In connected mode, you can use the harvester to obtain specific content and upload that content to the Enterprise Controller using the Bulk Upload action in the update library. See the Software Libraries chapter of the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for information about uploading content in bulk.

To obtain a KB bundle, use the following general procedure:

1. Identify a system that can connect to the Internet.
2. Download the harvester bundle.
3. Use the harvester script to download content.
4. Copy the KB bundle and OS update content onto the Enterprise Controller system using portable media.

Identifying a Harvester System

Select a system from which to run the harvester script. This system must use either Oracle Solaris or Linux and must be Internet-facing.

Downloading the Harvester Bundle

The harvester bundle contains the script `harvester.sh` and signing utilities for signature checking and generation of the downloaded software. To download the script:

1. On the internet-facing system, download the harvester script from https://updates.oracle.com/OCDoctor/harvester_bundle-latest.zip.
2. Unpack the bundle `harvester_bundle-latest.zip`.

Using the Harvester Script

You can use the harvester script to obtain a KB bundle and OS update content.

1. Run the harvester script using one or more of the options described below. You can edit the `config.ini` file to store some of these values. Values entered in the `config.ini` do not need to be provided when the harvester script is run.
 - `--user` *My Oracle Support user name*: Specify the valid My Oracle Support user name. You can set this value in the `HTTP_USER=" "` field of the `config.ini` file. This option is required if you have not added the MOS user name to the `config.ini` file.
 - `--password-file` *password file*: Specify the full path name of a file that contains only the MOS password. You can set either the password or the location of the password file in the `HTTP_PASSWD=" "` field of the `config.ini` file. This option is required if you have not added the password to the `config.ini` file.
 - `--proxy-server` *proxy server URL*: Specify the URL of the proxy server. You can set this value in the `PROXY_URL=" "` field of the `config.ini` file.
 - `--proxy-user` *proxy server user name*: Specify a username for the proxy server. You can set this value in the `PROXY_USER=" "` field of the `config.ini` file.
 - `--proxy-password-file` *proxy server password file*: Specify the full path name of a file that contains only the proxy server password. You can set either the password or the location of the password file in the `PROXY_PASSWD=" "` field of the `config.ini` file.

- `--storage-dir directory`: Specify the temporary directory for storing the downloaded contents. The default location is `/var/tmp/offline`. You can set this value in the `STANDALONE_DIR=""` field of the `config.ini` file.
- `--mark-new-patches`: The harvester script creates a dated folder which includes hard links to all the patches that were downloaded in the current run. All patches still go to the storage directory. This flag is useful in incremental downloads to identify which are the newly downloaded files. Using hardlinks eliminates the need for a full copy of each file. You can set this value in the `MARK_NEW_PATCHES=` field of the `config.ini` file.
- `--kb-only`: Download only the Knowledge Base bundle without downloading any patches.
- `--download-patches list`: Specify the distributions for which you want to download all the Oracle Solaris patches. Specify a quoted, space separated list of the names of Oracle Solaris OS distributions for which you want to download patches. If the distribution is not specified, the patches for all Oracle Solaris distributions are downloaded. Available distributions are:
 - `SOLARIS_10_0_SPARC`
 - `SOLARIS_10_0_X86`
 - `SOLARIS_9_0_SPARC`
 - `SOLARIS_8_0_SPARC`
 - `FIRMWARE`

The disk space requirement on the Internet-facing system and the Enterprise Controller to run the harvester script with the `--download-patches` option is approximately 150 GB for a distribution.

Note: The harvester script might take several hours to finish running with the `--download-patches` option. You can upload the patches in bulk from the EIS DVD.

- `--download-baseline ID`: Specify the Oracle Solaris baseline ID to download.

Note: When you use the `--download-baseline` option, you must use the `--download-patches` option. You can use the option only for one distribution.

- `--show-baselines distribution`: This option displays the baselines for a given distribution. You can enter only one distribution at a time. Valid distributions are:
 - `SOLARIS_10_0_SPARC`
 - `SOLARIS_10_0_X86`
 - `SOLARIS_9_0_SPARC`
 - `SOLARIS_8_0_SPARC`
- `--revisions number`: Specify the number of revisions of a patch to download. By default, the revision number is 100. You can set this value in the `REVISIONS=` field of the `config.ini` file.

- `--from-date mm-yyyy`: Only download patches that are newer than the specified date.
- `--patches-from-file file`: Download all the patches from a file. The format of the file must be one patch per line without the .zip extension.
- `--instructions`: Use this option to display instructions for moving downloaded Knowledge Base bundles and patches to the Enterprise Controller system.
- `--update`: Use this option to check for updates for the harvester script.

Example 2-1 Running Harvester Script with MOS Account

Running the harvester script to download only the knowledge base bundle.

```
# ./harvester.sh --kb-only
Ops Center Harvester version 2.10 (Jun 18 2012 [Build 57]) (SunOS)
Download log file is located in /var/tmp/harvester-wget.log
Checking for connectivity...
[OK] Connected successfully. No updates were found (current: 2.10, online: 2.10).
[OK] Directory /var/tmp/offline not found. This directory will be created.
[Channels list (channels.xml)] Downloaded successfully
Stage 1: Downloading/refreshing required Knowledge Base files
[AS_3_0_AMD64 Knowledge] Downloaded successfully
[AS_4_0_S390 Knowledge] Downloaded successfully
[AS_3_0_IA32 Knowledge] Downloaded successfully
[ES_3_0_IA32 Knowledge] Downloaded successfully
[ES_3_0_AMD64 Knowledge] Downloaded successfully
[FIRMWARE Knowledge] Downloaded successfully
[ES_4_0_AMD64 Knowledge] Downloaded successfully
[AS_4_0_IA32 Knowledge] Downloaded successfully
[AS_4_0_AMD64 Knowledge] Downloaded successfully
[OS_IMAGES Knowledge] Downloaded successfully
...
...
```

Example 2-2 Running Harvester Script to Download Oracle Solaris 10 SPARC patches

Running the harvester script to download Oracle Solaris 10 patches up to four revisions for a SPARC distribution

```
./harvester.sh --download-patches "SOLARIS_10_0_SPARC SOLARIS_10_0_X86"
--revisions 4
```

Example 2-3 Running Harvester Script to Display Baselines for Oracle Solaris 10 SPARC

Running the harvester script to display the available Oracle Solaris baselines for an Oracle Solaris 10 SPARC distribution.

```
./harvester.sh --download-patches SOLARIS_10_0_SPARC --download-baseline
```

Example 2-4 Running Harvester Script to Download Security Baselines for Oracle Solaris 10 SPARC

Running the harvester script to download the security baseline DEC-2009 for an Oracle Solaris 10 SPARC distribution.

```
./harvester.sh --download-patches SOLARIS_10_0_SPARC --download-baseline 40030030
```

Copying Content to the Enterprise Controller in Disconnected Mode

When you have downloaded the Knowledge Base bundle or OS update content, move it to the Enterprise Controller system using portable media. If you are using disconnected mode, use these procedures to copy the content into Oracle Enterprise Manager Ops Center. If you are using connected mode, see the Software Libraries chapter of the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for information about uploading content in bulk.

Copying a Knowledge Base Bundle

This procedure uploads a new knowledge base bundle to the Enterprise Controller. Follow this procedure if you used the `--kb-only` option.

1. Copy the `standalone-<timestamp>.tar.gz` to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory.
2. Click the Enterprise Controller in the Administration section of the Navigation pane.
3. Click **Setup Connection Mode** in the Actions pane.
4. Enter the absolute path of the Knowledge Base bundle that you want to use, then click **Load Bundle**. Use the **Browse** button to locate the Knowledge Base bundle if you do not know the absolute path.

Copying a Knowledge Base Bundle and All Patches

This procedure uploads a new knowledge base bundle to the Enterprise Controller and uploads patch content.

1. Copy the `standalone-<timestamp>.tar.gz` to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory.
2. Copy the `all_unsigned` folder, which includes all patches, to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory. You can split this folder across multiple DVDs if needed.
3. Click the Enterprise Controller in the Administration section of the Navigation pane.
4. Click **Setup Connection Mode** in the Actions pane.
5. Enter the absolute path of the Knowledge Base bundle that you want to use, then click **Load Bundle**. Use the **Browse** button to locate the Knowledge Base bundle if you do not know the absolute path.
6. Run the `copy_patches_to_oc.sh` script. This script is located in the `all_unsigned` folder.

Copying a Knowledge Base Bundle and Incremental Patches

This procedure uploads a new knowledge base bundle to the Enterprise Controller and uploads specific patch content. You can follow this procedure if you used the `--mark-new-patches` option or set the `MARK_NEW_PATCHES` field in the `config.ini` file to 1.

1. Copy the `standalone-<timestamp>.tar.gz` to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory.
2. Copy the `all_unsigned-<timestamp>` folder, which includes the patches downloaded on the day specified by the timestamp, to the Enterprise Controller

system. By default, this file is in the `/var/tmp/offline` directory. You can split this folder across multiple DVDs if needed.

3. Click the **Enterprise Controller** in the **Administration** section of the Navigation pane.
4. Click **Setup Connection Mode** in the Actions pane.
5. Enter the absolute path of the Knowledge Base bundle that you want to use, then click **Load Bundle**. Use the **Browse** button to locate the Knowledge Base bundle if you do not know the absolute path.
6. Run the `copy_patches_to_oc.sh` script. This script is located in the `all_unsigned-<timestamp>` folder.

Configuring Local Agent Controllers

A local Agent Controller is an Agent Controller installed on the Enterprise Controller or Proxy Controller OS. The operating systems and hardware that support the Enterprise Controller and Proxy Controllers are always managed, but configuring a local Agent Controller enables additional monitoring, reports, and jobs. See the *Feature Reference Guide* for more information about the advantages of managing assets using an Agent Controller.

Note: Any job that would cause the Enterprise Controller system to restart, such as an OS update job that requires a reboot, cannot be performed through Oracle Enterprise Manager Ops Center.

Configuring the Local Agent Controller on the Enterprise Controller

Configuring the Local Agent Controller on the Enterprise Controller system provides additional monitoring data on the system that supports the Enterprise Controller and enables some additional jobs.

1. Click the **Enterprise Controller** in the **Administration** section of the Navigation pane.
2. Click **Configure Local Agent** in the Actions pane.
A confirmation page is displayed.
3. Click **OK**.
A job is launched to configure the local Agent Controller.

Unconfiguring the Local Agent Controller on the Enterprise Controller

You can unconfigure the Local Agent Controller to halt monitoring of the Enterprise Controller system.

1. Click the **Enterprise Controller** in the **Administration** section of the Navigation pane.
2. Click **Unconfigure Local Agent** in the Actions pane.
A confirmation page is displayed.
3. Click **OK**.
A job is launched to unconfigure the local Agent Controller.

Configuring a Local Agent Controller on a Proxy Controller

Configuring the Local Agent Controller on a Proxy Controller system lets you monitor the system that supports the Proxy Controller and launch jobs that target it.

1. Click a Proxy Controller in the **Administration** section of the Navigation pane.
2. Click **Configure Agent on Proxy** in the Actions pane.

A confirmation window is displayed.

3. Click **OK**.

A job is launched to configure the local Agent Controller.

Unconfiguring a Local Agent Controller on a Proxy Controller

You can unconfigure the Local Agent Controller to halt monitoring of the Proxy Controller system.

1. Click a Proxy Controller in the **Administration** section of the Navigation pane.
2. Click **Unconfigure Agent on Proxy** in the Actions pane.

A confirmation window is displayed.

3. Click **OK**.

A job is launched to unconfigure the local Agent Controller.

Configuring Oracle Configuration Manager

Oracle Configuration Manager is a tool that customizes and enhances the support experience by collecting configuration information and uploading it to the Oracle repository. When the configuration data is uploaded on a regular basis, customer support representatives can analyze this data and provide better service.

Oracle Configuration Manager is installed with Oracle Enterprise Manager Ops Center. If you did not configure Oracle Configuration Manager during installation, you can do so using the command line.

This procedure requires that Java 7 be configured on the Enterprise Controller.

1. As root, log in to the Enterprise Controller system.
2. Run the `setupCCR` command.

```
# /var/opt/sun/xvm/ocm/ccr/bin/setupCCR
```

3. The Oracle Configuration Manager installation text is displayed. Enter the My Oracle Support user name or email address that you want to associate with Oracle Enterprise Manager Ops Center.

```
Provide your email address to be informed of security issues, install and
initiate Oracle Configuration Manager. Easier for you if you use your My
Oracle Support Email address/User Name.
```

```
Visit http://www.oracle.com/support/policies.html for details.
```

```
Email address/User Name:
```

4. If you want security updates to appear on your My Oracle Support page, enter your My Oracle Support password. Press Enter.

```
Provide your My Oracle Support password to receive security updates via your My
Oracle Support account.
```

```
Password (optional):
```

Oracle Configuration Manager is configured.

Registering the Enterprise Controller

You can register your Enterprise Controller with Oracle. This lets you register your assets, which associates the asset data with a My Oracle Support (MOS) account and makes the assets visible in the MOS portal. This option is not available if the Enterprise Controller was registered during the initial configuration.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click **Register Enterprise Controller** in the Actions pane.
The Introduction page is displayed.
3. View the introduction information, then click **Next**.
The HTTP Proxy page is displayed.
4. If the Enterprise Controller requires an HTTP Proxy to reach the Internet, enter the HTTP Proxy information, then click **Next**.
 - **Server:** Enter the server name for the HTTP Proxy.
 - **Port:** Enter the port number to be used.
 - **User:** Enter a user name if one is required by the server.
 - **Password:** Enter a password if one is required by the server.
5. Enter a valid My Oracle Support user name and password, then click **Next**. The Enterprise Controller is registered with the specified user name.
6. Review the registration information, then click **Finish**.
The Enterprise Controller is registered.

Running a Self Diagnosis

You can run a self-diagnosis on the Enterprise Controller, on Proxy Controllers, or on operating system assets. The self-diagnosis runs the OCDocor's `--troubleshoot` option, which can identify some common issues and aid in troubleshooting.

1. Select the target asset in the Assets section or Administration section of the Navigation pane.
2. Click **Self Diagnosis** in the Actions pane.
3. Select a task.
 - Select **Run New Self Diagnosis** to launch a new self diagnosis job.
If the target operating system supports the Enterprise Controller or a Proxy Controller, you can also select **Optimize Enterprise Controller** or **Proxy Controller**. This option uses the `--tuning` option to optimize the system for Enterprise Controller or Proxy Controller performance.
 - Select **Work on Previous Self Diagnosis** and select a prior self diagnosis job to review the data from a prior self diagnosis.
4. If you selected **Work on Previous Self Diagnosis**, the data from the prior self diagnosis is displayed. Review the data, then select a task.

- Select **re-run Self Diagnosis** to re-run the prior Self Diagnosis.
You can also check Attempt to Fix Issues to automatically fix certain issues.
 - Select **Collect Logs** to collect logs from the system.
Click Next.
5. Review the summary information, then click **Finish** to launch the job.
 6. Review the job details or rerun the wizard and select **Work on Previous Self Diagnosis** to view the data gathered by the self diagnosis.

Viewing and Changing the Enterprise Controller and Proxy Controller Status

You can check the status of the Enterprise Controller and Proxy Controllers from the command line, and stop or start them if necessary. Oracle Enterprise Manager Ops Center only functions while the Enterprise Controller is online, and each Proxy Controller must be online for the product to interact with its managed assets.

Checking the Status of the Enterprise Controller

The Enterprise Controller can be in one of two states. In the online state, the Enterprise Controller is running normally. In the offline state, the Enterprise Controller is stopped and cannot be used.

You can check the status of the Enterprise Controller using the `ecadm` command.

1. As root, log in to the Enterprise Controller system.
2. Use the `ecadm` command with the `status` subcommand to check the status of the Enterprise Controller.

For example:

```
# ./ecadm status  
online
```

The status of the Enterprise Controller is displayed.

Starting the Enterprise Controller

The Enterprise Controller can be in a stopped state due to a system reboot or maintenance. While the Enterprise Controller is stopped, Oracle Enterprise Manager Ops Center does not function.

You can start the Enterprise Controller using the `ecadm` command.

1. As root, log in to the Enterprise Controller system.
2. Use the `ecadm` command with the `start` subcommand to start the Enterprise Controller.

The following options may be used:

- `-h | --help`: Displays the usage synopsis for the subcommand.
- `-w | --wait`: `ecadm` does not exit until all services have been started.
- `-t | --temporary`: The state change is made temporary until next reboot.
- `-v | --verbose`: Displays verbose error and informational messages.

- `-l | --logfile <logfile>`: Captures any output from `ecadm` in the `<logfile>`.

For example:

```
# ./ecadm start -vw
ecadm: Starting Enterprise Controller with SMF...
ecadm: ... milestone "satellite-enable" succesfully enabled
ecadm: ... Waiting for Enterprise Controller services to go "online"
ecadm: Enterprise Controller services have started
#
```

The Enterprise Controller is started.

Stopping the Enterprise Controller

When the Enterprise Controller is online, Oracle Enterprise Manager Ops Center functions normally. However, certain maintenance tasks can only be performed when the Enterprise Controller is offline.

You can stop the Enterprise Controller using the `ecadm` command.

1. As root, log in to the Enterprise Controller system.
2. Use the `ecadm` command with the `stop` subcommand to stop the Enterprise Controller.

The following options may be used:

- `-h | --help`: Displays the usage synopsis for the subcommand.
- `-w | --wait`: `ecadm` does not exit until all services have been started.
- `-t | --temporary`: The state change is made temporary until next reboot.
- `-v | --verbose`: Displays verbose error and informational messages.
- `-l | --logfile <logfile>`: Captures any output from `ecadm` in the `<logfile>`.

For example:

```
# ./ecadm stop -vw
ecadm: Shutting down Enterprise Controller using SMF...
ecadm: ... milestone "satellite-enable" successfully disabled
ecadm: ... waiting for services to go "offline"
ecadm: Enterprise Controller services have stopped
#
```

The Enterprise Controller is stopped.

Checking the Status of a Proxy Controller

You can check the status of a Proxy Controller using the `proxyadm` command.

1. As root, log in to the Proxy Controller system.
2. Use the `proxyadm` command with the `status` subcommand to check the status of the Proxy Controller.

For example:

```
# ./proxyadm status
online
```

The status of the Proxy Controller is displayed.

Starting a Proxy Controller

You can start a Proxy Controller using the `proxyadm` command.

1. As root, log in to the Proxy Controller system.
2. Use the `proxyadm` command with the `start` subcommand to start the Proxy Controller.

The following options may be used:

- `-h | --help`: Displays the usage synopsis for the subcommand.
- `-w | --wait`: `proxyadm` does not exit until all services have been started.
- `-t | --temporary`: The state change is made temporary until next reboot.
- `-v | --verbose`: Displays verbose error and informational messages.
- `-l | --logfile <logfile>`: Captures any output from `proxyadm` in the `<logfile>`.

For example:

```
# ./proxyadm start -w
proxyadm: Starting Proxy Controller with SMF...
proxyadm: Proxy Controller services have started
#
```

The Proxy Controller is started.

Stopping a Proxy Controller

You can stop a Proxy Controller using the `proxyadm` command.

1. As root, log in to the Proxy Controller system.
2. Use the `proxyadm` command with the `stop` subcommand to stop the Proxy Controller.

The following options may be used:

- `-h | --help`: Displays the usage synopsis for the subcommand.
- `-w | --wait`: `proxyadm` does not exit until all services have been started.
- `-t | --temporary`: The state change is made temporary until next reboot.
- `-v | --verbose`: Displays verbose error and informational messages.
- `-l | --logfile <logfile>`: Captures any output from `proxyadm` in the `<logfile>`.

For example:

```
# ./proxyadm stop -w
proxyadm: Shutting down Proxy Controller using SMF...
proxyadm: Proxy Controller services have stopped
#
```

The Proxy Controller is stopped.

Putting a Proxy Controller in Maintenance Mode

You can put a Proxy Controller in maintenance mode. While in maintenance mode, a Proxy Controller cannot discover new assets or act as a target for asset migration, and incidents are not generated for the Proxy Controller. However, the Proxy Controller continues to manage its current assets.

1. In the Administration pane, select a Proxy Controller.
2. Click **Put in Maintenance Mode** in the Actions pane.
A confirmation window is displayed.
3. Click **OK**.

The Proxy Controller is placed in maintenance mode.

Removing a Proxy Controller from Maintenance Mode

You can remove a Proxy Controller from maintenance mode. When a Proxy Controller is removed from maintenance mode, it can discover assets and act as a target for asset migration as normal.

1. In the Administration pane, select a Proxy Controller.
2. Click **Clear Maintenance Mode** in the Actions pane.
A confirmation window is displayed.
3. Click **OK**.

The Proxy Controller is removed from maintenance mode.

Managing Proxy Controller Networks

Proxy Controllers must have access to networks to manage the assets on those networks. You can associate Proxy Controllers with specific networks and enable or disable those networks.

Note: If a Proxy Controller is connected to an asset using multiple networks, but management traffic between the Proxy Controller and agent must use a specific network, the Proxy Controller must have a NIC whitelisting file to identify the usable NICs.

Associating Networks With a Proxy Controller

You can associate networks with a Proxy Controller. A Proxy Controller can manage assets on any network that has been associated with it. You can only associate a network with a Proxy Controller if the network is reachable from the Proxy Controller.

1. In the Administration pane, select the Proxy Controller where you want to associate networks.
2. Click **Associate Networks** in the Actions pane.
The Network/Proxy Controller Associations page is displayed.
3. Use the arrow buttons to add networks to, or remove networks from, the Associate with Proxy Controller list.
4. Click **Finish** to associate the selected networks with the Proxy Controller.

When the job is completed, the Proxy Controller can manage and provision the assets that use these networks.

Enabling or Disabling Networks for a Proxy Controller

You can enable or disable specific networks for a Proxy Controller. Networks are enabled by default when they are associated with a Proxy Controller.

Enabled networks are used normally. Proxy Controllers cannot manage assets on disabled networks. If you attempt to disable a network on a Proxy Controller that is being used to manage assets, you are asked to migrate those assets to a different Proxy Controller before you can disable the network.

1. In the Administration pane, select the Proxy Controller.
2. Click **Enable/Disable Networks** in the Actions pane.
3. Use the arrow buttons to add networks to the Enabled and Disabled networks lists.
4. Click **Finish**.
5. If you are disabling networks that are being used to manage assets, the migrate assets popup is displayed. Click **Yes** to launch the Migrate Assets Wizard, or click **No** to leave the assets associated with their current Proxy Controller in an unmanaged state.
6. If you launched the Migrate Assets Wizard and another Proxy Controller is available, the Migrate Assets page is displayed. Select another Proxy Controller for the assets, then click **Migrate**.

The selected networks are enabled or disabled.

Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration

If you want to discover assets that use a strong cipher suite configuration, you must download two policy files and move them to your Proxy Controller systems.

1. On an Internet-facing system, navigate to <http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>.
2. Select Accept License Agreement.
3. Click the UnlimitedJCEPolicyJDK7.zip link and download the file.
4. Unzip the UnlimitedJCEPolicyJDK7.zip file.
5. Move the local_policy.jar and US_export_policy.jar files to the /usr/jdk/jdk<latest version>/jre/lib/security/ directory on the Proxy Controller.
6. Restart the Proxy Controller system.

Configuring DHCP and Subnets for OS Provisioning

Oracle Enterprise Manager Ops Center uses DHCP services or WAN boot to support OS provisioning.

DHCP servers enable you to obtain the IP configuration and the rest of the information needed on the NIC. WAN boot enables you to provision Oracle Solaris 10 or 11 on a SPARC platform across the network. With WAN boot, the software explicitly configures the information in the Open Boot PROM (OBP) and uses WAN boot for installation. See [Configuring the Enterprise Controller for WAN Boot](#) for more information about WAN boot.

Oracle Solaris 10 uses the Oracle DHCP server with a Proxy Controller that is running Oracle Solaris 10. Oracle Solaris 11 uses an ISC DHCP server. You can configure DHCP directly, or direct a Proxy Controller to use an external DHCP server. You can also configure subnets to work with specific DHCP servers.

Note: Configure the DHCP services in the Oracle Enterprise Manager Ops Center user interface, not from the command line.

The following information is included in this section:

- [About DHCP](#)
- [About Subnets](#)
- [About External DHCP Servers](#)

About DHCP

You can configure and enable DHCP services on a Proxy Controller. DHCP configuration configures and enables basic DHCP services on the Proxy Controller to support OS provisioning operations. The Proxy Controller must be in the same subnet as the target hosts for OS provisioning to work.

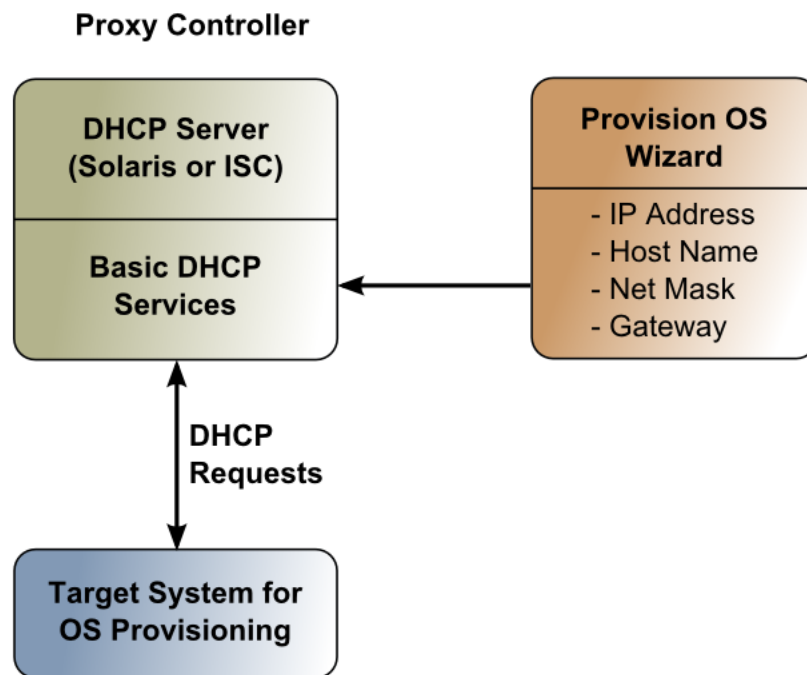
The DHCP Config action configures and enables either an Oracle Solaris DHCP server, or an Internet Standards Consortium (ISC) DHCP server, on the Proxy Controller that you select.

The DHCP Config action requires that you specify the Ethernet interface through which the Proxy Controller should provide DHCP services, for example bge0. You can establish DHCP services on all the Ethernet interfaces in the Proxy Controller. The Proxy Controller's Ethernet interface that you specify must be connected to the network where the target systems for OS provisioning are connected. In the same way, the Ethernet interface that you select in the Boot Network Device field of the Provision OS Wizard must be connected to the network where the Proxy Controller is providing DHCP services.

The DHCP Config and External DHCP Servers actions are mutually exclusive. Use one of these actions to configure DHCP services to support OS provisioning operations. The DHCP Config action is more commonly used, and is simpler to implement.

The Provision OS Wizard supplies the specific identity information that the target system requests, using the basic DHCP services that you establish on the Proxy Controller.

[Figure 2–1, "Basic DHCP Configuration"](#) shows the basic DHCP configuration.

Figure 2–1 Basic DHCP Configuration

Configuring DHCP

1. In the Administration pane, select the Proxy Controller where you want to configure DHCP services.
2. Click **DHCP Config** in the Actions pane.
The DHCP Configuration window is displayed.
3. In the DHCP Server menu, select either ISC or Oracle Solaris to implement either the Internet Standards Consortium (ISC) reference DHCP server, or the Oracle Solaris native DHCP server.
4. In the interfaces list, use the arrow buttons to add the correct Proxy Controller interface or interfaces to the list of selected interfaces. DHCP services are provided on the selected interface or interfaces. DHCP configuration is possible for multiple Ethernet interfaces in the Proxy Controller.
5. Click **Configure DHCP** to save the DHCP configuration that you specified.
6. A warning indicates that the procedure removes existing subnets in the DHCP configuration. Click **Yes** to accept that action and continue.

When the job completes successfully, DHCP services become available.

Note: You can configure DHCP server on the Proxy Controller to listen to multiple Ethernet interfaces. For example, consider the following network configuration for the Proxy Controller:

```
e1000g0 203.0.113.2
e1000g1 192.0.2.2
e1000g2 198.51.100.2
```

If you configure the DHCP server to listen to e1000g1 and e1000g2, then the target system must have the IP address in the range of 192.0.2.0/24 or 198.51.100.0/24.

About Subnets

You can configure subnets to use the DHCP server on a Proxy Controller for purposes in addition to OS provisioning, or to define subnets that are used with external DHCP servers.

Configuring subnets is not required to establish the basic DHCP services that are required for OS provisioning, unless you are using an external DHCP server.

You configure subnets for the following reasons:

- To provide IP address, DNS server, and router information to systems that can request them on the same network where the Proxy Controller is providing basic DHCP services for OS provisioning;
- If you configure an external DHCP server instead of configuring a DHCP server on a Proxy Controller, you must configure a subnet for each network from which you might receive relayed DHCP requests.

Specifying IP Address Ranges

Use the Subnets action to specify an IP address range that the DHCP server can use to assign IP addresses to systems that request them. The IP addresses that you specify in the Low IP Address and High IP Address fields for the subnet define the boundaries of the IP address range.

The IP addresses within the range that you specify cannot be used for OS provisioning operations. For example, if you specify 192.0.2.2 and 192.0.2.128 as the low and high IP addresses, you could not use any of the IP addresses within that range, including the low and high addresses, as values for the IP Address or IP Address Ranges fields in the Provision OS Wizard.

Configuring Subnets

1. In the Administration pane, select the Proxy Controller where you want to configure a DHCP subnet.
2. Select **Subnets** in the Actions pane. The DHCP Subnets Configuration window is displayed.
3. Select a subnet from the drop-down list. To create a new subnet, select **Create New Subnet**. To modify an existing subnet, select the existing subnet from the drop-down list. Click **Refresh** to update the list of subnets.
4. In the DHCP Subnets Configuration dialog box, provide the following information:

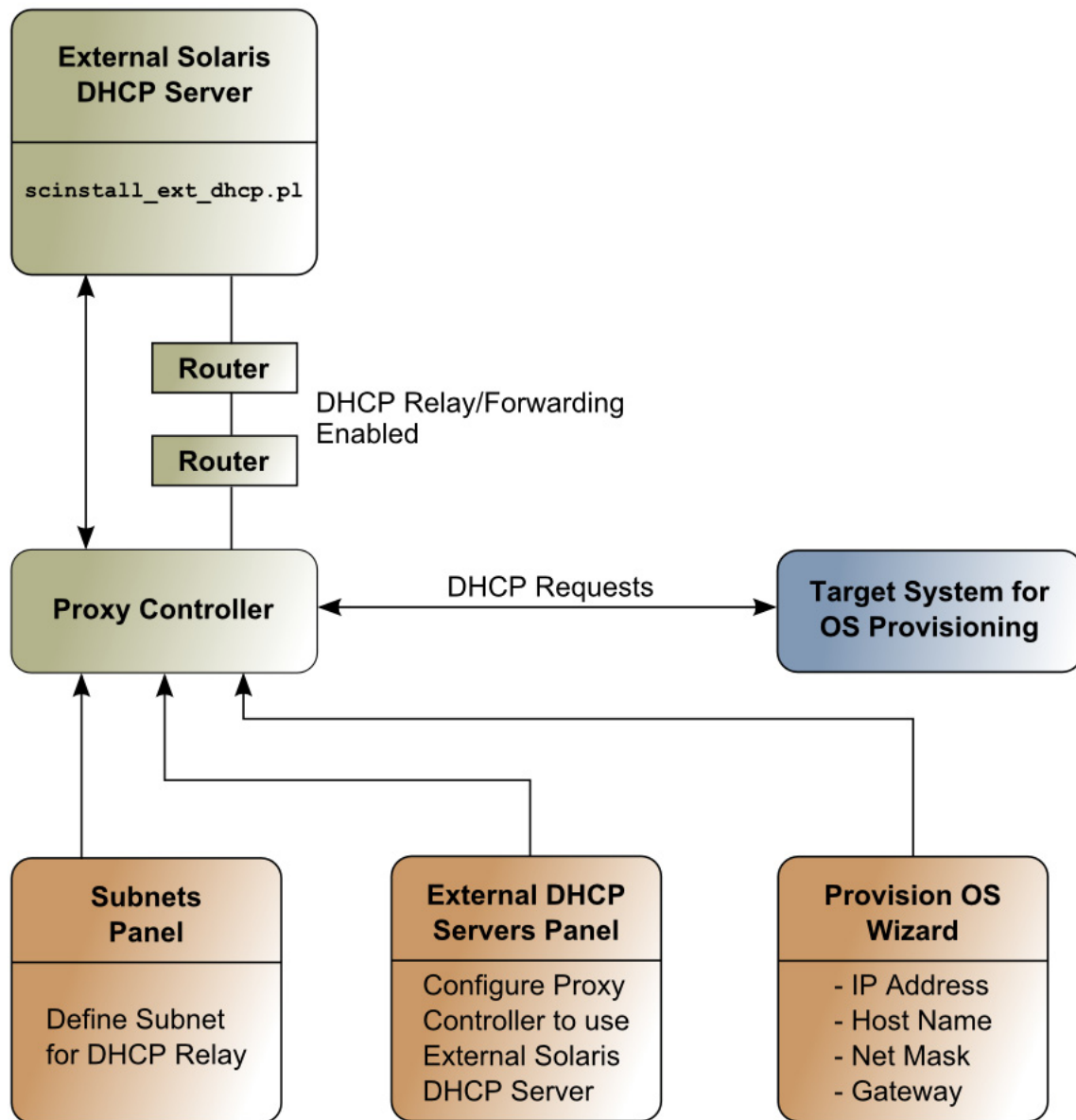
- **Subnet Name:** Enter the name of the subnet where you want to establish or modify DHCP services.
 - **Network IP:** Enter the network address.
 - **Network Interface:** Select the network interface.
 - **Netmask:** Enter the netmask for the network.
 - **Gateway IP:** Enter the gateway IP.
 - **IP Range:** Enter the IP addresses to use as the lower and upper limits of the IP address range that systems on this subnet can use.
 - **Name Server:** Enter the IP addresses of the DNS servers that systems should use.
 - **Domain Name:** Enter the names of the DNS domains that systems should use to resolve host names.
5. Click **Create Subnet** to create the subnet configuration that you specified, or click **Save Subnet** to save your changes to an existing subnet. A message indicates that a job to create the subnet was submitted. Click **OK** to dismiss the message.

About External DHCP Servers

You can use DHCP servers that are external to Proxy Controllers to provide the DHCP services that OS provisioning operations require.

The DHCP Config and External DHCP Servers actions are mutually exclusive. Use only one of these two actions to configure DHCP services to support OS provisioning operations. The DHCP Config action is more commonly used, and is simpler to implement.

[Figure 2–2, "DHCP Configuration Using External DHCP Servers"](#) illustrates DHCP configuration using External DHCP servers.

Figure 2–2 DHCP Configuration Using External DHCP Servers

You run the `scinstall_ext_dhcp.pl` script on the External DHCP server to establish communication between the Proxy Controller and the External DHCP server. The Subnets pane allows you to define subnets where DHCP relay traffic is expected. The External DHCP Servers pane configures the Proxy Controller to relay DHCP configuration information that the Provision OS Wizard supplies. The Provision OS Wizard supplies the specific identity information that the target system requests. The target system makes its DHCP requests, which are relayed to the External DHCP server. The routers or other network asset that connects the External DHCP server to the Proxy Controller must have DHCP relay capabilities enabled.

The External DHCP Servers action is only compatible with Oracle Solaris DHCP server and not with ISC DHCP server. External DHCP Servers are only compatible with Proxy Controllers installed on Oracle Solaris 10.

Configuring External DHCP Servers

1. Use `wget` to get the `scninstall_ext_dhcp.pl` script from the Proxy Controller to the External DHCP server.
 - a. On the external DHCP server, execute the following command to get the `scninstall_ext_dhcp.pl` script from the Proxy Controller.

```
# wget http://proxy_ip:8004/pub/scninstall_ext_dhcp.pl
```

Where `proxy_ip` is the IP address of the Proxy Controller.
 - b. Grant execute permissions for the script.

```
# chmod +x scninstall_ext_dhcp.pl
```
 - c. Install the script as root user.

```
# ./scninstall_ext_dhcp.pl install
```

This performs the following actions:
 - Sets up `scnospadmin` user.
 - Downloads the `SUNWscnosp-extdhcp` package from the proxy directory.
 - Sets up the configuration file for limited commands to run from `scnospadmin` user.
 - Sets up SSH keys to allow SSH/SCP commands from the Proxy Controller to the external DHCP server without requiring passwords.
2. In the Administration pane, select the Proxy Controller where you want to configure an external DHCP server.
3. Select **External DHCP Servers** in the Actions pane. The External DHCP Servers Configuration dialog box is displayed.
4. Select a DHCP server. To create a new DHCP server on the selected Proxy Controller, select **Create New DHCP Server**. To modify an existing DHCP server, select the existing DHCP server from the drop-down list. Click **Refresh** to update the list of DHCP servers.
5. In the External DHCP Servers Configuration dialog box, provide the following information:
 - **DHCP Server Name:** Enter the name of the DHCP server.
 - **DHCP Server IP:** Enter the IP address of the DHCP server.
 - **Network IP:** Enter the network address where you want to establish or modify DHCP services.
 - **Network Interface:** Select a Network Interface.
 - **DHCP Type:** Select either ISC or Oracle Solaris to implement either the Internet Standards Consortium (ISC) reference DHCP server, or the Oracle Solaris native DHCP server.
 - **Netmask:** Enter the netmask for the network where you want to establish or modify DHCP services.
 - **Gateway IP:** Enter the gateway IP.
 - **IP Range:** Enter the IP addresses to use as the lower and upper limits of the IP address range that systems on this subnet can use.

- **Name Server:** Enter the IP addresses of the DNS servers that systems should use.
 - **Domain Name:** Enter the names of the DNS domains that systems should use to resolve host names.
6. Click **Create DHCP Server** to create the DHCP server configuration that you specified. A message indicates that a job to create the external DHCP server was submitted. Click **OK** to dismiss the message.

Configuring the Enterprise Controller for WAN Boot

WAN Boot lets you use HTTP to boot and install software on SPARC systems over a wide area network (WAN). The security features are designed to protect data confidentiality while installing the Oracle Solaris OS on SPARC-based systems over a large public network. You can use DHCP or WAN boot for Oracle Solaris 10 provisioning, but WAN boot is the default connection for Oracle Solaris 11 provisioning on SPARC systems.

When you install Oracle Enterprise Manager Ops Center on a SPARC-based ILOM, ALOM, or M-series system that is running on an Oracle Solaris OS, the software configures the Enterprise Controller to be a WAN boot server.

Checking the WAN Boot Status

The Oracle Solaris 10 and Oracle Solaris 11 WAN Boot status is indicated in the user interface. A value of `true` indicates that WAN boot is enabled for the specified operating system, while a value of `false` indicates that it is disabled.

1. Expand the **Administration** section in the Navigation pane, then click **Enterprise Controller**.
2. Click the **Configuration** tab.
3. Select **OS Provisioning** from the Subsystem menu.
 - For Oracle Solaris 11, see the following property: `usesS11WANBoot`.
 - For Oracle Solaris 10, see the following property: `usesS10WANBoot`.

Changing the Default Port for Oracle Solaris 11 WAN Boot

The default port for WAN boot and the Oracle Solaris 11 Automated Installer (AI) is 5555.

When the Enterprise Controller is installed on an Oracle Solaris 11 operating system, you can change the default port by editing the configuration in the Service Management Facility (SMF) configuration service. When you change the default port in Oracle Solaris 11, Oracle Enterprise Manager Ops Center resolves the port at deployment time based on the SMF configuration and uses the new port for WAN boot. The `svccfg` command enables you to modify the service configuration.

Note: To ensure that WAN boot downloads the miniroot, the OS profile, and the OS manifest from the same server, Oracle Enterprise Manager Ops Center disables multicastDNS (mDNS) on the Proxy Controller.

The following example changes the port from 5555 to 7000:

1. Open a terminal window on the Oracle Solaris 11 Proxy Controller system.
2. Log in as with the required SMF privileges, such as root.
3. Edit the following service and change 5555 to a different port, in this case to port 7000:

```
# svccfg -s system/install/server:default setprop all_services/port = 7000
```

4. Refresh the service:

```
# svccfg refresh system/install/server:default
```

Enabling or Disabling WAN Boot

1. Expand the **Administration** section in the Navigation pane, then click **Enterprise Controller**.
2. Click the **Configuration** tab.
3. Select **OS Provisioning** from the Subsystem menu.
 - For Oracle Solaris 11, see the following property: usesS11WANBoot.
 - For Oracle Solaris 10, see the following property: usesS10WANBoot.
4. To enable WAN boot, change the value for the property to true.
5. To disable WAN boot, change the value for the property to false.

See the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for information about using a WAN boot connection.

Editing Oracle Solaris 11 Credentials

Oracle Solaris 11 provisioning and updating require an Oracle Solaris 11 Repository. A key file and a certificate file are used to connect to the repository. If these files are missing or have expired, you can provide a new key and certificate.

1. If you do not have valid key and certificate files, go to <https://pkg-register.oracle.com/> and log in using your MOS credentials to download them.
2. Expand the **Administration** section in the Navigation pane, then click **Credentials**.
3. If a set of credentials with the certificate category exists, select it and click the **Edit** icon, then supply the new key and certificate.
 - a. In the Key field, click **Browse** and select the key file on the local system, or enter the full key text.
 - b. In the Certificate field, click **Browse** and select the key file on the local system, or enter the full key text.
 - c. Click **Update**.
4. If no set of credentials with the certificate category exists, click **Create Credentials** in the Actions pane, then enter the new credentials.
 - a. In the protocol field, select Certificate.
 - b. Enter a name for the set of credentials.
 - c. (Optional) Enter a description for the set of credentials.

- d. In the Key field, click **Browse** and select the key file on the local system, or enter the full key text.
- e. In the Certificate field, click **Browse** and select the key file on the local system, or enter the full key text.
- f. Click **Create**.

Retaining Migration Scripts in Server Pools

When you create a server pool, migration scripts in the global zones are deleted to create consistency. You can edit the Enterprise Controller settings to retain these scripts.

1. Expand the **Administration** section in the Navigation pane, then click **Enterprise Controller**.
2. Click the **Configuration** tab.
3. Select **Server Pools** from the Subsystem menu.
4. Change the value of the `keep.migration.script` property to `true`.

Generating a Default Set of OS Provisioning Profiles and Plans

By default, Oracle Enterprise Manager Ops Center does not automatically generate OS Provisioning profiles and plans when a new image is imported or a new update is downloaded. You can enable the automatic generation of these plans and profiles.

1. Expand the **Administration** section in the Navigation pane, then click **Enterprise Controller**.
2. Click the **Configuration** tab.
3. Select **OS Provisioning** from the Subsystem menu.
4. Change the value of the `createS11Profiles` property to `true`.

Displaying Related Assets In Groups

By default, a user-created group only displays assets that have been added to that group. You can edit the group settings so that related assets are displayed using the same format as the main assets tree. For example, if this property is enabled, a server that has been added to a user-created group displays its operating system.

Note: If multiple related assets have been independently added to the same user-created group, duplicate entries may appear.

1. Expand the **Administration** section in the Navigation pane, then click **Enterprise Controller**.
2. Click the **Configuration** tab.
3. Select **BUI** from the Subsystem menu.
4. Change the value of the `com.oracle.sysman.showSubTreeInGroups` property to `true`.

Changing the HTTP Proxy

If your Enterprise Controller accesses the Internet through an HTTP proxy, you can edit the HTTP proxy information.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click **Change HTTP Proxy** in the Actions pane.
The Change HTTP Proxy Wizard is displayed.
3. Enter the HTTP Proxy information, including:
 - **Server:** Enter the HTTP Proxy server address
 - **Port Number:** Enter the port number to access on the HTTP Proxy.
 - **User Name:** Required if the HTTP Proxy requires authentication
 - **Password:** Required if the HTTP Proxy requires authentication
4. Click **Update**.

The HTTP proxy information is updated.

Database Management

Oracle Enterprise Manager Ops Center uses an Oracle Database 11g Enterprise Edition instance to store product data. You can manage this database.

The following features and topics are covered in this chapter:

- [Introduction to Database Management](#)
- [Installing and Configuring a Customer-Managed Database](#)
- [Migrating to a Customer-Managed Database](#)
- [Changing the Customer-Managed Database Location](#)
- [Verifying the Database](#)
- [Upgrading a Customer-Managed Database](#)
- [Changing the Database Credentials](#)
- [Defragmenting an Embedded Database](#)
- [Consolidating Reports Data on a Customer-Managed Database](#)

Introduction to Database Management

The Enterprise Controller uses an Oracle Database 11g Enterprise Edition database to store Oracle Enterprise Manager Ops Center data. This can be the embedded database installed with the Enterprise Controller, or a new or existing customer-managed database. You can manage the existing database, change, back up, or recover the database schema, or migrate the data to a customer-managed database.

You can use the backup and recovery actions available in Oracle Enterprise Manager Ops Center to back up an Enterprise Controller with either an embedded or a customer-managed database. These options do not require database administrator privileges. These options are discussed in [Chapter 8, "Backup and Recovery"](#).

Note: If you are using a customer-managed database, you can edit the `createOCSchema_remote.sql` script to restrict the OC schema user from running certain commands on the database. See the *Oracle Enterprise Manager Ops Center Security Guide* for more information.

Note: The OC Dump Directory is set when the Enterprise Controller is installed or when a new Oracle Enterprise Manager Ops Center database is specified. To change the OC Dump Directory, follow the procedure in [MOS document 1543144.1](#).

Some of the procedures described in this section use the `ecadm` command. See [Appendix A, "Command Line Administration"](#) for more information about this command.

- On Oracle Solaris systems, this command is in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, this command is in the `/opt/sun/xvmoc/bin/` directory.

Installing and Configuring a Customer-Managed Database

If you want to use a customer-managed database, you must install and configure it to work with Oracle Enterprise Manager Ops Center. Once you have installed and configured the database, you can migrate to it using the [Migrating to a Customer-Managed Database](#) procedure.

This procedure assumes that the Enterprise Controller has already been installed and configured. If you have not installed and configured an Enterprise Controller, follow the procedures in the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System* or *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*. These documents include procedures for installing and configuring a customer-managed database.

1. Install the database according to the Oracle Database 11g Enterprise Edition installation documentation.
2. Create the following tablespaces on the database:
 - **Default tablespace:** This is the default tablespace for the Oracle Enterprise Manager Ops Center user. Create this tablespace with the name `users`.
 - **Report tablespace:** This is the tablespace used for report data. Create this tablespace with the name `OC_RM_RESOURCE_TS`.
 - **Temporary tablespace:** This is the temporary tablespace for the Oracle Enterprise Manager Ops Center user.
3. Copy the `createOCschema_remote.sql` script from the Enterprise Controller to the database.
 - On Oracle Solaris for x86 systems, this script is in the `/var/tmp/OC/dvd/SunOS_i386/Product/installer/scripts` directory.
 - On Oracle Solaris for SPARC systems, this script is in the `/var/tmp/OC/dvd/SunOS_SPARC/Product/installer/scripts` directory.
 - On Linux systems, this script is in the `/var/tmp/OC/dvd/Linux_i686/Product/installer/scripts` directory.

For example:

```
# scp root@EnterpriseController:/var/tmp/OC/dvd/SunOS_
i386/Product/installer/scripts/createOCschema_remote.sql .
Password:
createOCschema_remote.sql 100% |*****| 1486      00:00
```


4. As the database administrator, run the `createOCschema_remote.sql` script and enter the following information:
 - **Oracle Enterprise Manager Ops Center user name:** This is a database user that is created by the script, which Oracle Enterprise Manager Ops Center uses to access the database.
 - **Oracle Enterprise Manager Ops Center password:** This is the password for the database user.
 - **Oracle Enterprise Manager Ops Center read-only user name:** This is a read-only database user, which Oracle Enterprise Manager Ops Center uses to view the database.
 - **Oracle Enterprise Manager Ops Center read-only password:** This is the password for the read-only database user.
 - **Default tablespace:** This is the default tablespace for the Oracle Enterprise Manager Ops Center user.
 - **Report tablespace:** This is the tablespace used for report data.
 - **Temporary tablespace:** This is the temporary tablespace for the Oracle Enterprise Manager Ops Center user.
 - **Oracle Enterprise Manager Ops Center dump directory:** This directory must exist and must be owned by the `oracle` user. If you are using Oracle RAC, this directory must be shared between all Oracle RAC nodes.

For example:

```
$ sqlplus / as sysdba @createOCSchema_remote.sql
```

```
SQL*Plus: Release 11.2.0.3.0 Production on Thu Dec 15 16:55:34 2011
```

```
Copyright (c) 1982, 2011, Oracle. All rights reserved.
```

```
Connected to:
```

```
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
```

```
Enter username for Ops Center database login: TESTSCHEMA
```

```
Enter password for Ops Center database login:
```

```
Enter username for read only Ops Center database login: TESTSCHEMA_RO
```

```
Enter password for read only Ops Center database login:
```

```
Enter default tablespace for Ops Center user: USERS
```

```
Enter report tablespace for Ops Center user: OC_RM_RESOURCE_TS
```

```
Enter temporary tablespace for Ops Center user: TEMP
```

```
Enter Oracle Data Pump destination directory: /var/tmp/ocdumpdir
```

```
"Done creating OC_SYSTEM_ROLE and OC_RO_ROLE"
```

```
"Done creating Schema 'TESTSCHEMA'. Roles and privileges have been granted."
```

```
"Done creating Schema 'TESTSCHEMA_RO'. Roles and privileges have been granted."
```

```
"Done creating OC_DUMP_DIR at /var/tmp/ocdumpdir"
```

```
"Done granting privs to users and profiles"
```

```
"Testing connectivity to the new schema: 'TESTSCHEMA'"
```

```
Connected.
```

```
"Testing connectivity to the new read only schema: 'TESTSCHEMA_RO'"
```

```
Connected.
```

```
"Create is Complete. OC can now be used with the new schema: 'TESTSCHEMA'"
```

```

Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 -
64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
$

```

Migrating to a Customer-Managed Database

If you are using the embedded database, you can migrate to a customer-managed database. You must install and configure the customer-managed database in the destination location as described in the [Installing and Configuring a Customer-Managed Database](#) procedure before beginning this procedure.

Note: The Enterprise Controller system must be routable by host name from the customer-managed database server for the migration to succeed.

1. Create a customer-managed database properties file on the Enterprise Controller system. The database properties file must contain the location of the customer-managed database and a user name and password that can access the database.

The database information can be found in the `tnsnames.ora` file.

For example:

```

# vi /var/tmp/RemoteDBProps.txt
mgmtdb.appuser=TESTSCHEMA
mgmtdb.password=TESTSCHEMA_PWD
mgmtdb.roappuser=TESTSCHEMA_RO
mgmtdb.ropassword=TESTSCHEMA_RO_PWD
mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<database service
name>

```

The `mgmtdb.dburl` property can be entered in any of these formats:

```

mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<database service
name>
mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>:<SID>
mgmtdb.dburl=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS) (HOST=<host
>) (PORT=<port>)) (CONNECT_DATA=(SERVICE_NAME=<service>)))

```

2. Use the `ecadm` command with the `backup` subcommand to back up the Enterprise Controller. This procedure is described in [Chapter 8, "Backup and Recovery"](#).
3. Use the `ecadm` command with the `migrate` subcommand and the `--remotedbprops <path to properties file>` and `-l <log file>` options to migrate to a customer-managed database. The log file is created in the `/var/opt/sun/xvm/logs` directory.

For example:

```

# ./ecadm migrate --remotedbprops /var/tmp/RemoteDBProps.txt -l migrate.log

```

Changing the Customer-Managed Database Location

You can change the location of the customer-managed database. You must install and configure the database in the destination location as described in the [Installing and](#)

[Configuring a Customer-Managed Database](#) section before beginning this procedure.

You must have root access to the Enterprise Controller system and database administrator access to the source database and destination database to complete this procedure.

1. As root, log in to the Enterprise Controller system.
2. Use the `ecadm` command with the `stop` subcommand and the `-w` option to shut down the Enterprise Controller.

For example:

```
./ecadm stop -w
ecadm: Shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
#
```

3. Edit the database properties file to point to the new database.

For example:

```
# vi /var/opt/sun/xvm/db.properties
...
mgmtbdb.dburl=jdbc:oracle:thin:@<source database host name>:<port>/<source
database service name>
```

The `mgmtbdb.dburl` property can be entered in any of these formats:

```
mgmtbdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<database service
name>
mgmtbdb.dburl=jdbc:oracle:thin:@<database host name>:<port>:<SID>
mgmtbdb.dburl=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCPS) (HOST=<host
>) (PORT=<port>)) (CONNECT_DATA=(SERVICE_NAME=<service>)))
```

Change the `mgmtbdb.dburl` line to point to the new database host name and name.

For example:

```
...
mgmtbdb.dburl=jdbc:oracle:thin:@<destination database host
name>:<port>/<destination database service name>
```

4. As a user with database administrator privileges, log in to the source database.
5. Use the `datapump` export utility to export the source database. When prompted for a user name, enter `/ as sysdba`.

For example:

```
$ expdp DIRECTORY=oc_dump_dir DUMPFILE=OC_schema.dmp SCHEMAS=OC,OC_RO
LOGFILE=expdp_OC_schema.log
Export: Release 11.2.0.1.0 - Production on Mon May 23 10:14:33 2011
Copyright (c) 1982, 2009, Oracle and/or its affiliates. All rights reserved.
Username: / as sysdba
<output omitted>
Job "SYS"."SYS_EXPORT_SCHEMA.01" succesfully completed at <timestamp>
$
```

6. Review the log file and verify that there were no errors.

For example:

```
$ cat expdp_OC_schema.log
<output omitted>
```

```
Job "SYS"."SYS_EXPORT_SCHEMA.01" succesfully completed at <timestamp>
```

7. Move the dump file from the source database server to the destination database server.

For example:

```
$ scp OC_schema.dmp <destination database host name>
Password:
OC_schema.dmp      100% |*****| 18192 KB      00:01
```

8. Delete the dump file on the source database system.

For example:

```
$ rm OC_schema.dmp
```

9. As a user with database administrator privileges, log in to the destination database.

10. Create a database directory that points to the location of the dump file, then exit.

For example:

```
SQL> create or replace directory oc_dump_dir as '/var/tmp/ocdumpdir';
SQL> exit;
```

11. Use the import utility to import the database dump file into the source database.

For example:

```
$ impdp DIRECTORY=oc_dump_dir DUMPFILE=OC_schema.dmp LOGFILE=impdp_OC_
schema.log
Import: Release 11.2.0.1.0 - Production on Mon May 23 10:14:33 2011
Copyright (c) 1982, 2009, Oracle and/or its affiliates. All rights reserved.
Username: / as sysdba
<output omitted>
Job "SYS"."SYS_IMPORT_SCHEMA.01" succesfully completed at <timestamp>
```

12. Review the log file and verify that there were no errors.

For example:

```
$ cat impdp_OC_schema.log
<output omitted>
Job "SYS"."SYS_IMPORT_SCHEMA.01" succesfully completed at <timestamp>
```

13. Delete the dump file on the destination database system.

For example:

```
$ rm OC_schema.dmp
```

14. As root, log in to the Enterprise Controller system.

15. Use the `ecadm` command with the `start` subcommand and the `-w` option to start the Enterprise Controller.

For example:

```
# ./ecadm start -w
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
#
```

Verifying the Database

You can verify that the configured database is operational and accessible from the Enterprise Controller.

1. Use the `ecadm` command with the `verify-db` subcommand to verify the database.

For example:

```
./ecadm verify-db
ecadm: --- Verified database
#
```

Upgrading a Customer-Managed Database

You can upgrade the database software. To do so, you must shut down the Enterprise Controller. Before upgrading the database software, verify that the version you intend to upgrade to is supported.

1. Use the `ecadm` command with the `stop` subcommand and the `-w` option to shut down the Enterprise Controller.

For example:

```
./ecadm stop -w
ecadm: Shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
#
```

2. Upgrade the customer-managed database according to the Oracle Database 11g Enterprise Edition upgrade documentation.
3. Use the `ecadm` command with the `start` subcommand and the `-w` option to start the Enterprise Controller.

For example:

```
# ./ecadm start -w
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
#
```

Changing the Database Credentials

You can change the database password for the Oracle Enterprise Manager Ops Center user or the read-only user on an embedded or customer-managed database.

Changing the Database Credentials for the Ops Center User

1. Create a temporary file containing the new password and secure it with 600 permissions.

For example:

```
# touch /tmp/password
# chmod 600 /tmp/password
# vi /tmp/password
newpassword
```

2. Use the `ecadm` command with the `change-db-password` subcommand and the `-p <password file>` option to change the database password. When prompted, confirm the Enterprise Controller restart.

For example:

```
# ./ecadm change-db-password -p /tmp/password
The Enterprise Controller will be restarted after the database password is
changed. Continue? (y/n)
y
ecadm: --- Changed database password, restarting.
ecadm: shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
#
```

3. If you have a high availability configuration, the `ecadm` command copies the new database properties to each remote cluster node. Enter the root password for each remote cluster node.

For example:

```
ecadm: --- Changed database password, restarting.
The DB configuration file must now be copied to each remote cluster node.
You will be prompted for the root password for each node to perform the copy.
Copying to node OC-secondary
Password: password
<output omitted>
ecadm: --- Enterprise Controller successfully started HA
#
```

4. Remove the temporary file containing the new password.

For example:

```
# rm /tmp/password
```

Changing the Database Credentials for the Read-Only User

1. Create a temporary file containing the new password.

For example:

```
# vi /tmp/password
newpassword
```

2. Use the `ecadm` command with the `change-db-password` subcommand and the `-p <password file>` and `-r` options to change the database password. When prompted, confirm the Enterprise Controller restart.

For example:

```
# ecadm change-db-password -r -p /tmp/password
The Enterprise Controller will be restarted after the database password is
changed. Continue? (y/n)
y
ecadm: --- Changed database password, restarting.
ecadm: shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
```

```
#
```

3. If you have a high availability configuration, the `ecadm` command copies the new database properties to each remote cluster node. Enter the root password for each remote cluster node.

For example:

```
ecadm: --- Changed database password, restarting.
The DB configuration file must now be copied to each remote cluster node.
You will be prompted for the root password for each node to perform the copy.
Copying to node OC-secondary
Password: password
<output omitted>
ecadm: --- Enterprise Controller successfully started HA
#
```

4. Remove the temporary file containing the new password.

For example:

```
# rm /tmp/password
```

Defragmenting an Embedded Database

You can defragment an embedded database to increase free space and improve performance.

1. As root, log in to the Enterprise Controller system.
2. Use the `ecadm` command with the `stop` subcommand and the `-w` option to shut down the Enterprise Controller.

For example:

```
./ecadm stop -w
ecadm: Shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
#
```

3. Use the `ecadm` command with the `defrag-db` subcommand to defragment the embedded database.

This command makes a backup of the Enterprise Controller before defragmenting the database. By default, the temporary directory used to stage the backup file is `/var/tmp`. You can specify another temporary directory using the `-T | --tempdir <temp-dir>` option.

For example:

```
./ecadm defrag-db --tempdir /tmpdir
```

4. Use the `ecadm` command with the `start` subcommand and the `-w` option to start the Enterprise Controller.

For example:

```
# ./ecadm start -w
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
#
```

Consolidating Reports Data on a Customer-Managed Database

If you have installed or upgraded to Oracle Enterprise Manager Ops Center version 12.2.2.0.0 with a customer-managed database, reporting data may be stored in the main tablespace, which can cause Enterprise Controller downtime if the tablespace reaches its maximum size.

To determine if the reporting data is correctly stored in the OC_RM_RESOURCE_TS tablespace, you can check the `satadmsqlplus.log` file after upgrading or installing. This log file is located in the `/var/opt/sun/xvm/logs` and indicates whether report data is correctly stored in the OC_RM_RESOURCE_TS tablespace.

If the reporting data is not stored in the OC_RM_RESOURCE_TS tablespace, you can use the `ecadm` command to move this data to the OC_RM_RESOURCE_TS tablespace.

1. Run the `OCDoctor.sh` script with the `--troubleshoot` option. If it indicates that the OC_RM_RESOURCE_TS tablespace is missing, use the suggested fix to create the tablespace. For example:

```
/var/opt/sun/xvm/OCDoctor/OCDoctor.sh --troubleshoot
<output omitted>
ERROR: Tablespace OC_RM_RESOURCE_TS needs to be added to the remote DB (Bug
17737994)!
```

Tablespace creation example (to be run by DBA of remote DB):

```
CREATE TABLESPACE OC_RM_RESOURCE_TS
    DATAFILE '<path to datafile>/ocresource01.dbf'
    SIZE 100M REUSE
    AUTOEXTEND ON
    NEXT 100M
    MAXSIZE 32767M
    EXTENT MANAGEMENT LOCAL
    SEGMENT SPACE MANAGEMENT AUTO
;
```

```
ALTER USER <oc_user_name> QUOTA UNLIMITED ON OC_RM_RESOURCE_TS;
```

2. Use the `ecadm` command with the `stop` subcommand and the `-w` option to shut down the Enterprise Controller.

For example:

```
./ecadm stop -w
ecadm: Shutting down Enterprise Controller using SMF...
ecadm: Enterprise Controller services have stopped
#
```

3. Use the `ecadm` command with the `mv-rep` subcommand to move the report data.
4. Open the `/var/opt/sun/xvm/logs/satadmsqlplus.log` file and verify that no errors were reported during the move process.
5. Use the `ecadm` command with the `start` subcommand and the `-w` option to start the Enterprise Controller.

For example:

```
# ./ecadm start -w
ecadm: Starting Enterprise Controller with SMF...
ecadm: Enterprise Controller services have started
#
```

General Administration

Oracle Enterprise Manager Ops Center includes several administrative tools for viewing and fine-tuning the product's features. This chapter discusses these tools.

The following features and topics are covered in this chapter:

- [Introduction to General Administration](#)
- [Viewing and Understanding Service Statuses](#)
- [Viewing Logs](#)
- [Adding a Product Alias](#)
- [Adding or Editing Authentications](#)
- [Editing the Energy Cost](#)

Introduction to General Administration

Oracle Enterprise Manager Ops Center provides you with a variety of tools for understanding and managing your data center.

You can view services and logs, add an alias to ensure that a product is recognized, add and edit authentications for external sites, and edit the energy cost used to calculate the power cost of assets.

Some of the procedures described in this section use the `ecadm` and `proxyadm` commands. See [Appendix A, "Command Line Administration"](#) for more information about these commands.

- On Oracle Solaris systems, these commands are in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, these commands are in the `/opt/sun/xvmoc/bin/` directory.

Viewing and Understanding Service Statuses

Oracle Enterprise Manager Ops Center relies on the services listed in [Table 4–1, "Oracle Enterprise Manager Ops Center Services"](#). The status of these services is monitored and displayed in the UI. The Fault Management Resource Identifier (FMRI) for each service can be used with SMF commands.

Do not directly enable or disable these services unless directed to do so by Oracle Support. Use the `ecadm`, `proxyadm`, and `agentadm` commands to manage the services.

[Table 4–1, "Oracle Enterprise Manager Ops Center Services"](#) shows the names, FMRI identifiers, and normal statuses of the Oracle Enterprise Manager Ops Center services.

Table 4–1 Oracle Enterprise Manager Ops Center Services

Service Name	FMRI	Normal Status
Cacao	common-agent-container-1:scn-proxy	Enabled
Cacao	common-agent-container-1:oem-ec	Enabled
Enterprise Controller - Down	ec-server-splashpage:default	Disabled unless Enterprise Controller is down
Ops Center AjaxTerm Serial Console	ajaxterm:default	Enabled
SCN Infrastructure Database	db:default	Enabled
SCN Infrastructure Database	db:local	Enabled if the software is using an embedded database
SCN Infrastructure Database	db:remote	Enabled if the software is using a remote database
SCN Oracle (local) database	oracle:default	Enabled
SCN Oracle (local) database listener	oralistener:default	Enabled
SCN Satellite Console	console:default	Enabled
Update Connection Enterprise - Agent	update-agent:default	Enabled if the local Agent Controller is configured
Update Connection Enterprise - Scheduler	uce-scheduler:default	Enabled
Update Connection Enterprise - Server	uce-server:default	Enabled
dhcpd	dhcpd:default	Enabled

Viewing Service Status

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click the **Summary** tab.

The status of the Oracle Enterprise Manager Ops Center services is displayed.

Viewing Logs

You can view logs to diagnose problems or examine Oracle Enterprise Manager Ops Center activities.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.
2. Click the **Logs** tab.
3. Select a log from the drop-down list.
 - Cacao log
 - UI log
 - DB transaction log
 - DB report log
 - Proxy log
 - Update error log

- Update channel download log
- Update channel error log

The log is displayed.

4. (Optional) Click **Refresh Log File** to refresh the displayed version of the log file.

Adding a Product Alias

In some cases, an asset's type is not recognized. You can add a product alias to ensure that Oracle Enterprise Manager Ops Center recognizes an asset and that all of its features are available.

Note: Use this feature as directed by Oracle Support.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.
2. Click **Add Product Alias** in the Actions pane. The Add Product Alias page is displayed.
3. Enter the Product Alias information.
 - Product Alias: This is the existing asset name.
 - Product ID: This is the full product ID number. If a Product Label is supplied, the Product ID is optional.
 - Product Label: This is the original factory label for the asset. If a Product ID is supplied, the product Label is optional.
4. Click **Add Product Alias** to add the product alias to the Enterprise Controller.

Adding or Editing Authentications

Authentications, such as My Oracle Support (MOS) or other credentials, are used to download content such as updates from Oracle or third-party sites. MOS credentials are also used to create service requests.

You can add or edit authentications to access additional external resources.

If you have not configured Oracle Configuration Manager (OCM) with a set of MOS credentials, OCM uses the MOS credentials supplied to Oracle Enterprise Manager Ops Center to configure itself. After OCM has configured itself using a valid set of authenticated credentials, it does not use any other MOS credentials.

If OCM is already configured, no attempt is made to reconfigure it with new credentials.

Note: You must register the Enterprise Controller before adding My Oracle Support credentials.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.
2. Click **Edit Authentications** in the Actions pane.
The Edit Authentications window is displayed.

3. Add or edit one or more sets of authentications.
 - To edit an online account, click the **description**, **user name**, or **password** field and enter the new information.
 - To add a MOS user, click the **Add MOS User** icon.
 - To edit a MOS user, click the **description**, **user name**, or **password** field and enter the new information.
 - To remove a MOS user, select the user and click the **Remove MOS User** icon.
 - To set a MOS user as default, select the user and click the **Set as Default MOS User** icon.
4. Click **Apply**.

A job is launched to update the authentications.

Editing the Energy Cost

One of the Oracle Enterprise Manager Ops Center capabilities is monitoring power utilization for a server or among groups of servers or virtualization hosts.

You can also monitor the cost of power utilization by supplying the cost per currency unit. This information is displayed in the Summary or Energy tab.

1. Expand **Administration** in the Navigation pane.
2. Click **Edit Energy Cost** in the Actions pane.
3. Enter your location's cost for each kilowatt-hour.
4. Enter your business's currency unit.
5. Click **Submit**.

The energy cost is updated.

Oracle Enterprise Manager Ops Center includes the OCDoctor utility, a tool that can check systems for installation prerequisites, troubleshoot issues, and tune systems for Oracle Enterprise Manager Ops Center. This chapter discusses the use of the OCDoctor.

The following features and topics are covered in this chapter:

- [Introduction to the OCDoctor](#)
- [Downloading the OCDoctor](#)
- [Performing Preinstallation Checks](#)
- [Performing Troubleshooting and Tuning](#)
- [Updating the OCDoctor](#)
- [Determine the Number of Asset Access Points](#)

Introduction to the OCDoctor

The OCDoctor is a tool that can provide a variety of information about Oracle Enterprise Manager Ops Center and current or potential Enterprise Controller, Proxy Controller, and Agent Controller systems.

The OCDoctor is located in the `/var/opt/sun/xvm/OCDoctor` directory on the Enterprise Controller system. You can copy the OCDoctor to other systems or download it from Oracle. Once you have copied it onto a system, you can perform preinstallation checks, troubleshoot issues, and check for OCDoctor updates.

Downloading the OCDoctor

If you are operating in disconnected mode, or if you want to install the latest version of the OCDoctor on a new system, you can download the latest version from Oracle.

1. On an Internet-facing system, navigate to <http://java.net/projects/oc-doctor/downloads> and click the OCDoctor-LATEST.zip download.
2. Move the downloaded file to the target system.
3. Unzip the file.
4. If the target system is an existing Enterprise Controller, replace the contents of the `/var/opt/sun/xvm/OCDoctor` directory with the contents of the zip file.

Performing Preinstallation Checks

You can use the OCDoctor to verify that systems meet the prerequisites for an Oracle Enterprise Manager Ops Center installation, get a benchmark score, or check the system's connectivity.

1. Change to the `/var/opt/sun/xvm/OCDoctor` directory.
2. Run the `OCDoctor.sh` script with one of the following options:
 - `--ec-prereq`: Verifies that the system meets the prerequisites for an Enterprise Controller installation.
 - `--proxy-prereq`: Verifies that the system meets the prerequisites for a Proxy Controller installation.
 - `--agent-prereq`: Verifies that the system meets the prerequisites for an Agent Controller installation.
 - `--performance`: Checks the speed of the system and provides a Benchmark Time (BT) score. You can use a BT score to estimate how many assets a system can effectively manage. You should use this option when the system is idle.
 - `--check-connectivity`: Verifies that the system has network connectivity by connecting to My Oracle Support and downloading two test files.

For example:

```
# ./OCDoctor.sh --check-connectivity
Ops Center Doctor 4.36 [OC 12.2.2.808,SunOS11]
===== Checking Network Connectivity
=====
Using Ops Center Proxy server:example-proxy.company.com Port:80 (you may
overwrite it by setting https_proxy)
Please enter the My Oracle Support (MOS) Username: example.user@company.com
Password:

Test 1/4: Checking CC service reachability (without using user/password yet)
=====
Connecting to https://hs-ws1.oracle.com/ochi/servicecheck?type=cc
OK: CC status is OK

Test 2/4: Checking GUUS service (KnowledgeBase Service) reachability (without
using user/password yet)
=====
Connecting to https://hs-ws1.oracle.com/ochi/servicecheck?type=guus
OK: GUUS status is OK

Test 3/4: Downloading Knowledge Channels file from updates.oracle.com
=====
Connecting to https://updates.oracle.com/channels3/channels.xml
OK: Knowledge download was successful!

Test 4/4: Downloading patch 108437-06 from updates.oracle.com
=====
Connecting to https://updates.oracle.com/all_unsigned/108437-06.zip
OK: Patch download was successful!
```

Performing Troubleshooting and Tuning

The OCDoctor can help you troubleshoot issues and tune systems.

1. Change to the `/var/opt/sun/xvm/OCDoctor` directory.
2. Run the `OCDoctor.sh` script with one of the following options:
 - `--troubleshoot`: Troubleshoots common problems and suggests solutions. You can also use the `--fix` option to automatically fix certain issues.
 - `--collectlogs <parameters>`: Collects all logs from the current system. You can add optional parameters to pass the logs to collection scripts.
 - `--needhelp`: Provides information on gathering additional system information and filing a support case.
 - `--tuning`: Scans the current system and suggests changes to improve system performance. You can also use the `--fix` option to automatically apply some tuning improvements.
 - `--whatisblobid <id>`: Provides details about the specified blob id.
 - `--getblobid <patch id>`: Provides the blob id for a specified patch.

For example:

```
# ./OCDoctor.sh --troubleshoot
Ops Center Doctor 4.36 [OC 12.2.2.808,SunOS11] [Read only] [31-Mar-2014
10:34AM MDT]
===== Checking Enterprise Controller...
=====
OK: Total number of agents (without Solaris 11 ones): 20
OK: Number of agents with inventories: 20
OK: Enterprise Controller requirements are met
OK: Files in /var/opt/sun/xvm/images/agent/ have the right permissions
OK: Files in /var/opt/sun/xvm/osp/web/pub/pkgs/ have the right permissions
OK: both pvalue and pdefault in systemproperty are equal to false (at id 114)
OK: Found only 57 OCDB*.aud files in oracle/admin/OCDB/adump folder
OK: Found no ocdb*.aud files in oracle/admin/OCDB/adump folder
OK: No auth.cgi was found in cgi-bin
OK: User 'oracleoc' home folder points to the right location
OK: User 'allstart' home folder points to the right location
OK: Apache logs are smaller than 2 GB
OK: nlgc folder has the right permissions
OK: All agent packages are installed properly
OK: All Enterprise Controller packages are installed properly
OK: Enterprise Controller status is online
<Output omitted>
```

Updating the OCDoctor

The OCDoctor can locate and download updates if it is on an Internet-facing system. The Enterprise Controller performs this update automatically. You can also perform this update manually.

1. Change to the `/var/opt/sun/xvm/OCDoctor` directory.
2. Run the `OCDoctor.sh` script with the `--update` option. If you want to force a download of the latest online version, use the `--force` option.

For example:

```
# ./OCDoctor.sh --update
Ops Center Doctor 4.36 [OC 12.2.2.808,SunOS11]
Trying to download updates...
Using Ops Center Proxy server:example-proxy.company.com Port:80
```

```
Downloading version file using mirror: updates.oracle.com

OK: Version file was downloaded successfully
OK: Connected successfully - but no updates were found (current: 4.36, online:
4.36) .

You may force downloading the online version by running:
# ./OCDoctor.sh --update --force
```

Determine the Number of Asset Access Points

An access point is a connection between a managed asset and the Enterprise Controller through a Proxy Controller. The number of access points for the Enterprise Controller and for each Proxy Controller provides more accurate scaling information than the number of assets.

A single managed asset can have one or more access points, depending on how many Proxy Controllers are managing it. For example, if an Oracle VM Server for SPARC control domain's operating system is managed by one Proxy Controller while a hosted logical domain's operating system is managed by another Proxy Controller, the Enterprise Controller has two access points for that asset.

The OCDoctor utility includes a script, `AssetCount.sh`, that you can run on the Enterprise Controller to get the current access point count for the Enterprise Controller and each Proxy Controller, including a breakdown of the type of assets on each Proxy Controller.

When the OCDoctor utility is run with the `--troubleshoot` option, it performs an access point count. If the results of this count indicate that the Enterprise Controller or Proxy Controllers are approaching or beyond the maximum recommended number of assets, the output will include a warning.

When you run the `./OCDoctor.sh --collectlogs` command on the Enterprise Controller, the current access point count is included in the output. The current access point count can be useful when troubleshooting an issue.

The following methods can be used to view the access point count:

- [Viewing the Access Point Count for Your Environment](#)
- [Viewing the Access Point List for Each Proxy Controller](#)
- [Viewing the Access Point Types for Each Proxy Controller](#)
- [Viewing All Access Point Data](#)

Viewing the Access Point Count for Your Environment

You can view the total number of access points managed by the Enterprise Controller, as well as a categorized count of the access points managed by each Proxy Controller. Run the following command on the Enterprise Controller:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh standard
```

For example:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh standard
EC 72
Proxy Assets Zones Ldoms OVMGuests Servers Storages Switches ExadataCells MSeriesChassis MSeriesD
-----
pc4      32      5      25      0          2          0          0          0          0          0
```



```
pc1  28    0    26    0        2    0    0    0    0    0
pc0  12    2     4    0        6    0    0    0    0    0
Use option '-v' to see additional notes on the counting algorithm.
```

Viewing the Access Point List for Each Proxy Controller

You can view a list of the access points of each type that are managed by each Proxy Controller. The output first provides the total number of access points on the Enterprise Controller, then for each Proxy Controller provides the total number of access points, the number of access points of each type, and the user-friendly name for each asset.

The output for this command can be very long in a large environment.

Run the following command on the Enterprise Controller:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh machine
```

For example:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh machine
EC 72
Proxy 32 pc4
Zones 5 S1lzone101 S1lzone102 S1lzone100 S1lzone103 S1lzone104
Ldms 25 stdldom21 stdldom34 stdldom36 stdldom22 stdldom45 stdldom47 ...
OVMGuests 0
Servers 2 10.187.70.169 pc4
...
Proxy 28 pc1
Zones 0
Ldms 26 stdldom21 stdldom34 stdldom36 stdldom22 stdldom45 stdldom47 ...
OVMGuests 0
Servers 2 10.187.70.171 pc1
```

Viewing the Access Point Types for Each Proxy Controller

You can view a count of the access points for each Proxy Controller in three categories: Agent Controllers, Agentless assets, and service processors.

Run the following command on the Enterprise Controller:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh agent
```

For example:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh agent
EC 72
Proxy Agents Agentless SPs
-----
pc4  25    2    0
pc1   1    1    0
pc0   5    5    5
Use option '-v' to see additional notes on the counting algorithm.
```

Viewing All Access Point Data

You can view all access point data, including the results of the standard, machine, and agent options.

Run the following command on the Enterprise Controller:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh all
```

For example:

```
# /var/opt/sun/xvm/OCDoctor/toolbox/AssetCount.sh all
EC 72
Proxy Assets Zones Ldoms OVMGuests Servers Storages Switches ExadataCells MSeriesChassis MSeriesD
-----
pc4 32 5 25 0 2 0 0 0 0 0
pc1 28 0 26 0 2 0 0 0 0 0
pc0 12 2 4 0 6 0 0 0 0 0
```

```
Proxy Agents Agentless SPs
-----
pc4 25 2 0
pc1 1 1 0
pc0 5 5 5
```

```
Proxy 32 pc4
Zones 5 S11zone101 S11zone102 S11zone100 S11zone103 S11zone104
Ldoms 25 stdldom21 stdldom34 stdldom36 stdldom22 stdldom45 stdldom47 ...
OVMGuests 0
Servers 2 10.187.70.169 pc4
...
Proxy 28 pc1
Zones 0
Ldoms 26 stdldom21 stdldom34 stdldom36 stdldom22 stdldom45 stdldom47 ...
OVMGuests 0
Servers 2 10.187.70.171 pc1
```

Use option '-v' to see additional notes on the counting algorithm.

Auto Service Request

Oracle Enterprise Manager Ops Center can be configured to use Oracle Auto Service Request (ASR) to create service requests for assets when incidents occur.

The following features and topics are covered in this chapter:

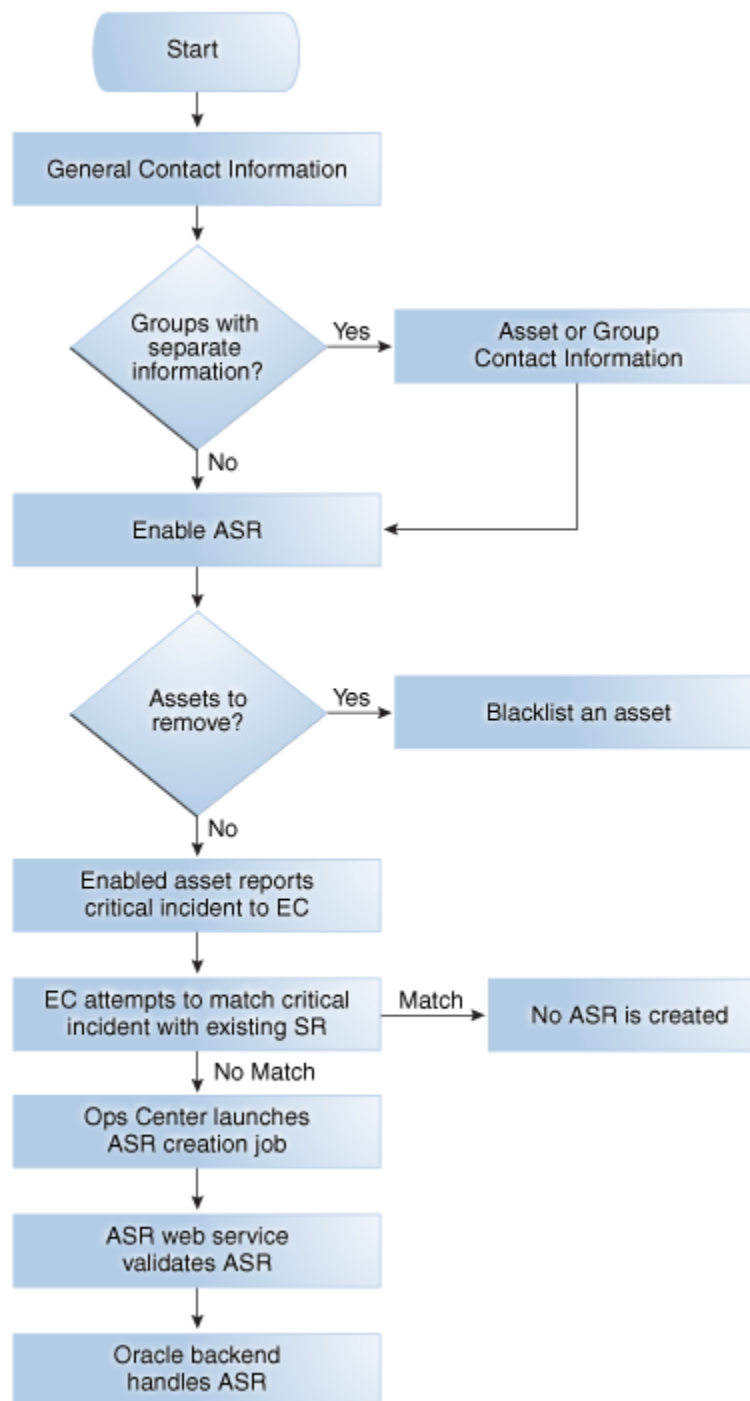
- [Introduction to ASR](#)
- [Viewing ASR Status for an Asset](#)
- [Providing Contact Information](#)
- [Enabling ASR](#)
- [Disabling ASR](#)
- [Blacklisting an Asset](#)
- [Testing ASR](#)

Introduction to ASR

Oracle Enterprise Manager Ops Center can use ASR to generate service requests based on known issues. By providing contact information for your assets and enabling ASR, you enable the creation of service requests whenever a new critical incident occurs.

Overview of ASR

Oracle Enterprise Manager Ops Center can use ASR to generate service requests based on known issues. The data from an incident in Oracle Enterprise Manager Ops Center and the asset's contact information are used to create the service request.

Figure 6–1 ASR Activation and Creation

Prerequisites

You must provide contact information for your assets and enable this feature before service requests can be generated using ASR.

An ASR can only be generated for an asset if a set of valid My Oracle Support (MOS) credentials have been provided. The asset must be present in MOS, and the credentials must be associated with a Customer Service Identifier (CSI) with rights over the asset. The CSI must be a direct CSI. Service Request Creation rights are required to create

new service requests, and Admin rights are required if the contact information for the asset must be updated. Go to <https://support.oracle.com/> and log in to verify that your assets are present in MOS.

Oracle Enterprise Manager Ops Center's ability to create an ASR is also limited by the available credentials. Oracle Enterprise Manager Ops Center can only monitor an asset for ASR telemetry using the management credentials for the asset. To ensure full coverage for your hardware, provide management credentials for all applicable protocols for each OS and hardware asset. See the Asset Management chapter of the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about adding credentials, and see http://docs.oracle.com/cd/E37710_01/nav/faultcoverage.htm for more information about the telemetry used by ASR.

How ASR Activation Works

After ASR creation is enabled, Oracle Enterprise Manager Ops Center launches a daily job to activate assets for ASR, and attempts to activate all assets when they are discovered. The asset activation job is also run whenever the Enterprise Controller is restarted. You can view the details of this job to see what assets have been activated. You can also view an asset's ASR status. If you do not want an asset to be enabled for ASR creation, you can add the serial number of that asset to a blacklist.

Note: Blade chassis can be enabled for ASR, but individual blades cannot be enabled for ASR.

When an asset is activated for ASR, Oracle Enterprise Manager Ops Center monitors the asset for faults, using either an Agent Controller if one is installed or the asset's Proxy Controller if no Agent Controller is installed. This monitoring is performed automatically, and does not create a job.

To detect faults, Oracle Enterprise Manager Ops Center uses the ILOM and FMA telemetry sources as well as HALRT faults from Exadata systems. It collects SNMP traps from hardware assets and uses SNMP to monitor switch and PDU assets. It can process SNMP V1 and V2 fault alerts, but it can only process SNMP V1 sensor alerts, and it does not check the SNMP community string. It also gathers faults from ILOM using IPMI and SSH to detect faults that occurred before the asset was activated.

Oracle Enterprise Manager Ops Center sends a daily heartbeat event to Oracle for each asset that is enabled for ASR. If this heartbeat is not received, this is reflected for the asset in MOS. The status of this asset is changed to "Active — No Heartbeat" with a date when a heartbeat was last received listed in MOS. The next time a heartbeat is received, the asset's status is changed to the standard ASR status of "Active".

Note: Some assets, such as Solaris 11 and Sun ZFS Storage Appliances, include embedded ASR support. You can choose to enable these assets for ASR directly, or to enable ASR through Oracle Enterprise Manager Ops Center. See the Storage Libraries chapter of the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information.

How ASR Creation Works

When a fault occurs on an activated asset, Oracle Enterprise Manager Ops Center first checks to see if the fault matches an existing incident. If not, a new incident is created, a job is run to create a new ASR, and an annotation is added to the incident indicating

the ASR creation attempt. The creation job sends the ASR to the ASR web service for validation. When the ASR is validated, it is sent to Oracle.

When the ASR creation is successful, another annotation is added, indicating that the ASR was successfully created and providing a URL for the ASR. Once it is created, an ASR is identical to other service requests and can be viewed and managed using the same processes and tools.

Note: If you create a manual service request for an incident that has already generated an ASR, the duplicate service request is not automatically removed.

For more information about the assets that can be activated for ASR and the incidents that can create an ASR, see the ASR documentation at <http://www.oracle.com/asr>.

Viewing ASR Status for an Asset

You can view an asset's ASR activation status. If the asset is activated for ASR, a service request is created when specific faults occur. See http://docs.oracle.com/cd/E37710_01/nav/faultcoverage.htm for more information about the faults that can trigger ASR creation. If the asset is not activated, it is either not qualified for ASR or it has not been successfully associated with one of the MOS accounts known to Oracle Enterprise Manager Ops Center.

1. Click the asset in the Assets section of the Navigation pane.
2. Click the **Service Requests** tab.

The ASR Activated State field shows the asset's ASR status.

Providing Contact Information

You can provide or edit the contact information for an asset or group of assets. You can also provide and edit the default contact information that is used for assets without asset-specific contact information. This contact information is used to create the ASR with the location of the asset.

If an asset has one set of contact information in the My Oracle Support interface and a separate set in Oracle Enterprise Manager Ops Center, the MOS set is used in the ASR. If MOS has no contact information for the asset, the contact information provided in Oracle Enterprise Manager Ops Center is used.

Providing Default Contact Information

The default contact information is used to create service requests for assets without asset-specific contact information. You must provide default contact information before enabling ASR.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.
2. Click **Edit ASR Default Contact** in the Actions pane.

The Default ASR Contact Information page is displayed.

3. Enter the contact information:

- First name

- Last name
 - Phone
 - Email
 - Country
 - Address: Two address fields are provided, but only the first is required.
 - City
 - State or Province
 - (Optional) Zip or Postal Code
 - Time Zone
4. Click **Save**.

Providing Contact Information for an Asset or Group

You can provide contact information for an asset or group. This contact information is used to create service requests for the asset or assets within the group.

1. Select an asset or group in the Assets section of the Navigation pane.
2. Click **Edit ASR Contact Information** in the Actions pane.

The ASR Contact Information page is displayed.

3. Enter the contact information:
 - First name
 - Last name
 - Phone
 - Email
 - Country
 - Address: Two address fields are provided, but only the first is required.
 - City
 - State or Province
 - (Optional) Zip or Postal Code
 - Time Zone
4. Click **Save**.

Enabling ASR

When ASR is enabled, service requests are automatically generated for your assets when a qualified incident occurs.

Note: You must provide default contact information before you enable ASR. See the [Providing Default Contact Information](#) section for more information.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.

2. Click **Enable ASR**.

A confirmation window is displayed.

3. Click **OK**.

The Auto Service Request feature is enabled.

Disabling ASR

You can disable ASR. While the feature is disabled, service requests are not automatically generated for any asset.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.

2. Click **Disable ASR**.

A confirmation window is displayed.

3. Click **OK**.

ASR is disabled.

Blacklisting an Asset

When ASR is enabled, Oracle Enterprise Manager Ops Center periodically launches a job to enable assets for ASR, and attempts to activate all assets when they are discovered. You can add the serial number of an asset to a blacklist to prevent Oracle Enterprise Manager Ops Center from enabling that asset for ASR.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.
2. Click the **Configuration** tab, then select the **Auto Service Request** subsystem.
3. In the Serial Blacklist value field, enter one or more serial numbers in a comma-separated list.
4. Click **Save**.

Testing ASR

You can create a test fault on a managed asset to verify that ASR is working correctly.

1. Log in to a managed ILOM asset using the web console.
2. Navigate to Notification in the Administration section of the UI.
3. Add or edit a test rule to include an snmp test trap, then test this new rule.
4. Log in to the Oracle Enterprise Manager Ops Center UI.
5. Click the **Incidents** section and verify that an incident for the test trap is displayed.
6. Click the **Jobs** section and verify that an ASR creation job has been created.

User and Role Management

You can add users to Oracle Enterprise Manager Ops Center from the local authentication subsystem of the Enterprise Controller's operating system or from a separate directory server. You can give each user a set of roles that grant access to the different functions of Oracle Enterprise Manager Ops Center. You can also give users privileges for their roles, which apply the roles to specific assets, networks, or other objects.

You can view the existing users and their roles and privileges from the Administration section.

The following features and topics are covered in this chapter:

- [Introduction to User and Role Management](#)
- [Adding a User](#)
- [Deleting a User](#)
- [Viewing User Role Details](#)
- [Adding a Directory Server](#)
- [Synchronizing Remote Users and Roles](#)
- [Deleting a Directory Server](#)
- [About Roles and Permissions](#)
- [Managing Roles](#)
- [Replicating a User](#)
- [About Notification Profiles](#)
- [Deleting a Notification Profile](#)
- [Viewing the Audit Log](#)

Introduction to User and Role Management

Oracle Enterprise Manager Ops Center can import any user known to the Enterprise Controller, and import sets of users from directory servers. These users can log in and launch jobs separately.

Each user can be granted roles and privileges for each role, giving them a tailored set of abilities. Roles define what actions the user can take, and privileges specify the targets to which their roles apply.

You can view the permissions granted by each role, add and remove users, and assign roles and notification profiles to users.

Whenever a user is added or deleted, or new roles are assigned to a user, an entry for the event is added to the Oracle Enterprise Manager Ops Center audit log. You can view this log to verify changes to users and roles.

Adding a User

Users with the User Admin role can add other users to Oracle Enterprise Manager Ops Center. New user information, such as the passwords for new users, are drawn from the local authentication subsystem.

1. Select **Administration** in the Navigation pane.
2. Click **Local Users**.
The Users page is displayed.
3. Click the **Add User** icon.
The Add User window is displayed.
4. Enter the user name.
5. Add one or more roles to the list of Selected Roles.
6. Click **Add User**.
The new user is created.

Deleting a User

A user with the User Admin role can delete other users, removing the user from Oracle Enterprise Manager Ops Center and erasing the user's roles and privileges.

1. Select **Administration** in the Navigation pane.
2. Click **Local Users**.
The Users page is displayed.
3. Select the user that you want to delete, then click the **Delete User** icon.
The Delete User window is displayed.
4. Click **OK**.
The user is deleted.

Viewing User Role Details

You can view the details of a specified user's roles. This includes all of the roles and privileges assigned to that user.

1. Select **Administration** in the Navigation pane.
2. Click either **Local Users** or a directory server.
The users are displayed.
3. Select a user from the list of users.
4. Click the **View User Role Details** icon.
The user's roles are displayed.
5. Click **Next**.

The privileges for each of the user's roles are displayed on separate pages.

6. View each set of privileges, then click **Next**.

The Summary page is displayed.

7. View the summary, then click **Finish**.

Adding a Directory Server

You can add directory servers to Oracle Enterprise Manager Ops Center. Users and roles are added to the product from the directory server.

To grant roles to the users in a directory server, you create groups on the directory server that correspond to the roles in Oracle Enterprise Manager Ops Center. You grant a role to a user by adding the user to the corresponding group, and remove a role from a user by removing them from the group. You cannot edit the roles of a directory server user through the Oracle Enterprise Manager Ops Center user interface. Users that are added from a directory server begin with complete privileges for each of their roles.

When you add a directory server to Oracle Enterprise Manager Ops Center, the login page uses directory server users by default. Local users can still be selected.

1. Create the following user groups on the directory server:

- ASSET_ADMIN
- CLOUD_ADMIN
- CLOUD_USER
- FAULT_ADMIN
- NETWORK_ADMIN
- OPS_CENTER_ADMIN
- PROFILE_PLAN_ADMIN
- READ
- REPORT_ADMIN
- ROLE_ADMIN
- SECURITY_ADMIN
- SERVER_DEPLOY_ADMIN
- STORAGE_ADMIN
- SUPERCLUSTER_ADMIN
- UPDATE_ADMIN
- UPDATE_SIM_ADMIN
- USER_ADMIN
- VIRT_ADMIN

2. Add users to these groups on the directory server. When the directory server is imported, the users are given the roles corresponding to their groups.
3. In Oracle Enterprise Manager Ops Center, select **Administration** in the Navigation pane.

4. Click **Directory Servers**.

5. Click the **Add Directory Server** icon.

The Remote Directory Server Connection Settings page is displayed.

6. Enter the following connection settings:

- **Name:** The name of the directory server.
- **Host:** The host name of the directory server.
- **Port:** The port number to be used to access the directory server.
- **SSL:** Check this box to use SSL to connect to the directory server.
- **Anonymous Bind:** Check this box to use anonymous binding to access the directory server.
- **Username:** The user name used to access the directory server. Username is required only if Anonymous Bind is not checked.
- **Password:** The password for the given user name. Password is required only if Anonymous Bind is not checked.
- **Authentication:** Select Use Directory Server for Authentication or Use Ops Center Local Authentication.

Click **Next**.

The Schema Settings page is displayed.

7. Enter the following schema settings:

- **Root suffix:** The root node of the directory tree.
- **Group search DN:** The container or operational unit in which to search for the role groups.
- **Group search scope:** The scope of the group search. Select Search One Level or Search Entire Subtree.
- **User search DN:** The container or operational unit in which to search for users.
- **User search scope:** The scope of the user search. Acceptable values are base, one, subtree, baseObject, singleLevel, wholeSubtree, or subordinateSubtree.
- **User search filter:** An LDAP search filter which users must meet for inclusion. This filter can include `memberUid` and `UniqueMember` LDAP schemas.
- **User name attribute:** The attribute which Oracle Enterprise Manager Ops Center should use as the user name. The specified attribute, such as `GivenName`, is treated as the user name during login and within the user interface.

Click **Next**.

The Summary page is displayed.

8. Review the summary, then click **Add Directory Server**.

Synchronizing Remote Users and Roles

You can synchronize Oracle Enterprise Manager Ops Center with one or all directory servers. This updates the list of users and roles to match the directory server's current information.

Synchronizing Remote Users and Roles With One Directory Server

You can synchronize Oracle Enterprise Manager Ops Center with a single directory server.

1. Select **Administration** in the Navigation pane.
2. Click **Directory Servers**.
The list of directory servers is displayed.
3. Select a directory server and click the **Sync Remote Users and Roles** icon.
A confirmation window is displayed.
4. Click **OK**.

Synchronizing Remote Users and Roles With All Directory Servers

You can synchronize Oracle Enterprise Manager Ops Center with all known directory servers.

1. Select **Administration** in the Navigation pane.
2. Click **Directory Servers**. The list of directory servers is displayed.
3. Click **Sync All Remote Users and Roles** in the Actions pane.
A confirmation window is displayed.
4. Click **OK**.

Deleting a Directory Server

You can remove a directory server. This action removes all users in that directory server from Oracle Enterprise Manager Ops Center.

1. Select **Administration** in the Navigation pane.
2. Click **Directory Servers**. The list of directory servers is displayed.
3. Select a directory server and click the **Delete Directory Server** icon.
A confirmation window is displayed.
4. Click **OK**.

About Roles and Permissions

Roles grant users the ability to use the different functions of Oracle Enterprise Manager Ops Center. By giving a role to a user, an Enterprise Controller Administrator controls the functions available to that user on specific assets and groups.

Each role grants a user a specific set of permissions. To perform a job, you must have the correct permissions for the target of the job.

Note: Subgroups inherit the roles assigned to the parent group.

How Roles are Mapped to Permissions

Table 7–1, "Roles and Permissions" shows the permissions granted by each role.

Table 7–1 Roles and Permissions

Role	Permissions
Asset Admin	Asset Group Management Asset Management Asset Network Management Boot Environment Management Chassis Management Chassis Usage Cluster Management Discover Assets IPMP Groups Link Aggregation Manage Assets Network Management Operating System Management Operating System Usage Power Distribution Unit Management Power Distribution Unit Usage Power Management Rack Creation Rack Deletion Rack Management Rack Usage Read Access Server Management Server Usage Service Request Storage Server Management Storage Server Usage Switch Management Switch Usage Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Cloud Admin	Asset Management
	Asset Network Management
	Cloud Management
	Cloud Usage
	Fabric Creation
	Fabric Deletion
	Fabric Management
	Fabric Usage
	IPMP Groups
	LDOM Power Management
	Link Aggregation
	Manage Assets
	Network Creation
	Network Deletion
	Network Domain Creation
	Network Domain Deletion
	Network Domain Management
	Network Domain Usage
	Network Management
	Network Usage
	Operating System Management
	Operating System Usage
	OVM Manager Management
	OVM Manager Usage
	Profile Plan Management
	Read Access
	Role Management
	Server Management
	Server Pool Management
	Server Pool Usage
	Server Provisioning
	Server Usage
	Solaris Zone Creation
	Solaris Zone Deletion
	Solaris Zone Host Management
	Solaris Zone Management
	Storage Management
	Storage Server Management
	Storage Server Usage
	Storage Usage
	Switch Management
	Switch Usage

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Cloud Admin (Continued)	Virtualization Guest Creation
	Virtualization Guest Deletion
	Virtualization Guest Management
	Virtualization Guest Usage
	Virtualization Host Management
	Virtualization Host Usage
	Write Access

Table 7-1 (Cont.) Roles and Permissions

Role	Permissions
Cloud User	Asset Management
	Asset Network Management
	Cloud Usage
	Fabric Creation
	Fabric Deletion
	Fabric Usage
	LDOM Power Management
	Manage Assets
	Network Creation
	Network Deletion
	Network Domain Management
	Network Domain Usage
	Network Management
	Network Usage
	Operating System Management
	Operating System Usage
	OVM Manager Usage
	Read Access
	Server Pool Usage
	Server Provisioning
	Server Usage
	Solaris Zone Creation
	Solaris Zone Deletion
	Solaris Zone Host Management
	Solaris Zone Management
	Storage Management
	Storage Server Usage
	Storage Usage
	Switch Usage
	Virtualization Guest Creation
	Virtualization Guest Deletion
	Virtualization Guest Management
	Virtualization Guest Usage
	Virtualization Host Management
	Virtualization Host Usage
	Write Access
Fault Admin	Fault Management
	Read Access
	Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Network Admin	Asset Management
	Asset Network Management
	Fabric Creation
	Fabric Deletion
	Fabric Management
	Fabric Usage
	IPMP Groups
	Link Aggregation
	Network Creation
	Network Deletion
	Network Domain Creation
	Network Domain Deletion
	Network Domain Management
	Network Domain Usage
	Network Management
	Network Usage
	Read Access
	Write Access
Ops Center Admin	Add Product Alias
	Discover Assets
	EC Connection Mode Management
	EC Energy Cost Management
	EC HTTP Proxy Management
	EC Local Agent Management
	EC Proxy Management
	EC Registration
	EC Storage Library Management
	EC Upgrade
	Enterprise Controller Management
	Cloud Control Management
	Job Management
	Manage Assets
	Ops Center Downloads
	OVM Manager Management
	OVM Manager Usage
	Proxy Controller Management
	Proxy Controller Upgrade
	Read Access
	Unconfigure EC
	Windows Update Management
	Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Plan/Profile Admin	Plan/Profile Management
	Read Access
	Write Access
Read	Read Access
Report Admin	Read Access
	Report Management
	Update Simulation
	Write Access
Role Management Admin	Read Access
	Role Management
	Write Access
Security Admin	Credential Management
	Read Access
	Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Supercluster Systems Admin	Read Access Manage Assets Asset Group Management Server Provisioning Fault Management Credential Management Network Management Fabric Management Storage Management Report Management Profile and Plan Management User Management Role Management Asset Management Write Access Service Requests Power Management Storage Server Management Server Management Operating System Management Cluster Management Link Aggregation Operation Execution EC Registration EC HTTP Proxy Management EC Energy Cost Management Server Pool Creation Server Pool Deletion Server Pool Management Server Pool Usage Storage Creation Storage Deletion Storage Usage Network Creation Network Deletion Network Usage Fabric Creation Fabric Deletion Fabric Usage Storage Server Usage Switch Usage Server Usage

Table 7-1 (Cont.) Roles and Permissions

Role	Permissions
Supercluster Admin (Continued)	Operating System Usage
	Directory Server Management
	PDU Usage
	PDU Management
	Network Domain Creation
	Network Domain Deletion
	Network Domain Management
	Network Domain Usage
	Asset Network Management
	Job Management
	Solaris Zone Creation
	Solaris Zone Deletion
	Solaris Zone Host Management
	Solaris Zone Management
	Software Library Management
	LDOM Power Management
Apply Deployment Plans	Operation Execution
	Read Access
	Server Provisioning
	Update Firmware
	Write Access
Storage Admin	Asset Management
	Read Access
	Storage Creation
	Storage Deletion
	Storage Management
	Storage Server Management
	Storage Server Usage
	Storage Usage
	Write Access
Update Admin	Boot Environment Management
	Read Access
	Software Library Management
	Update
	Update Simulation
	Windows Update Management
	Write Access
Update Simulation Admin	Read Access
	Update Simulation
	Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
User Management Admin	Directory Server Management Read Access User Management Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Virtualization Admin	Asset Management
	Asset Network Management
	Fabric Creation
	Fabric Deletion
	Fabric Management
	Fabric Usage
	IPMP Groups
	Link Aggregation
	LDOM Power Management
	Manage Assets
	Network Creation
	Network Deletion
	Network Domain Creation
	Network Domain Deletion
	Network Domain Management
	Network Domain Usage
	Network Management
	Network Usage
	Operating System Management
	OVM Manager Management
	OVM Manager Usage
	PDOM Domain Management
	Read Access
	Server Provisioning
	Server Management
	Server Pool Creation
	Server Pool Deletion
	Server Pool Management
	Server Pool Usage
	Solaris Zone Creation
	Solaris Zone Deletion
	Solaris Zone Host Management
	Solaris Zone Management
	Storage Creation
	Storage Deletion
	Storage Management
	Storage Server Management
	Storage Server Usage
	Storage Usage
	Virtualization Guest Creation
	Virtualization Guest Deletion
	Virtualization Guest Management

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Virtualization Admin (Continued)	Virtualization Guest Usage
	Virtualization Host Creation
	Virtualization Host Deletion
	Virtualization Host Management
	Virtualization Host Usage
	Write Access

How Permissions are Mapped to Tasks

[Table 7–2, "Permissions and Tasks"](#) shows the tasks that a user with a given permission can perform.

Table 7–2 Permissions and Tasks

Permission	Tasks
Read Access	Read Access
Discover Assets	Add Assets
	Find Assets
Manage Assets	Manage Assets
	Delete Assets
Asset Group Management	Create Group
	Edit Group
	Add Assets to Group
	Delete Group
Update	New Update OS Job
	Deploy or Update Software
	Compare System Catalog
	Create Catalog Snapshot
	View and Modify Catalog
Update Simulation	New Simulated OS Update Job
Server Provisioning	Configure and Deploy Server
	Install Server
	Configure RAID
Virtualization Guest Management	Add or delete storage
	Assign or detach network
	Start Guest
	Shut Down Guest
	Migrate Guest
	Clone Guest
	Lifecycle actions

Table 7-2 (Cont.) Permissions and Tasks

Permission	Tasks
Fault Management	Assign Incidents Add Annotation to incidents Acknowledge incidents Take Actions on Incidents Mark Incidents as Repaired Close Incidents Delete Notifications Take Actions on Notification
Credential Management	Update Management Credentials Any Actions related to changing credentials
Network Management	Edit Network Domain Edit Network Attributes Edit Network Services
Fabric Management	Fabric Management
Storage Management	Import ISO Upload image Edit Attributes
Report Management	Create reports Delete reports
Plan/Profile Management	Create, delete, and modify profiles and plans
Cloud Usage	Create/Update/Delete Instance Attach/Detach Volume to Instance Create/Delete/Update Security Group Create/Update/Delete Volume Upload/Register/Delete templates Create/RollbackTo/Delete Snapshot Shutdown All servers Link/Launch OVAB
Cloud Management	Create/Delete/Update Cloud Create/Delete/Update Cloud Domain Create Public Security Group Share Public Security Group Create VM Instance Type
Enterprise Controller Management	Manage Enterprise Controller
Proxy Controller Management	Unconfigure/Uninstall Proxy Controller Configure Agent Controller Unconfigure Agent Controller DHCP configuration Subnets External DHCP Servers

Table 7–2 (Cont.) Permissions and Tasks

Permission	Tasks
Cloud Control Management	Configure/Connect Disconnect/Unconfigure Cloud Control Console
Windows Update Management	Unconfigure SCCM Configuration
User Management	Add Users Remove Users
Role Management	Assign Roles
Asset Management	Asset Management
Write Access	Write Access
Service Request	Open Service Request
Power Management	Power On Power Off Power on with Net Boot Set Power Policy
Chassis Management	Chassis Management
Storage Server Management	Storage Server Management
Switch Management	Launch Switch UI
Server Management	Reset Servers Reset Service Processors Refresh Locator Light On/Off Snapshot Bios Configuration Update Bios Configuration
Operating System Management	Reboot Upgrade Agent Controller
Cluster Management	Cluster Management
Link Aggregation	Aggregate Links
IPMP Groups	IPMP Groups
Update Firmware	Update Firmware
Proxy Controller Upgrade	Upgrade Proxy Controller
Operation Execution	Execute Operation
Unconfigure EC	Unconfigure Enterprise Controller
Add Product Alias	Add Product Alias
EC Upgrade	Upgrade Enterprise Controller
EC Storage Library Management	Set Enterprise Controller Storage Library
EC Local Agent Management	Configure Local Agent Unconfigure Local Agent

Table 7–2 (Cont.) Permissions and Tasks

Permission	Tasks
EC Proxy Management	Proxy Deployment Wizard
EC Connection Mode Management	Set up Connection Mode
EC Registration	Register Enterprise Controller
EC HTTP Proxy Management	Change HTTP Proxy
EC Energy Cost Management	Edit Energy Cost
Ops Center Downloads	Ops Center Downloads
Boot Environment Management	Activate Boot Env and Reboot Create New Boot Env. Synchronize Boot Env.
Server Pool Creation	Create Server Pool
Server Pool Deletion	Delete Server Pool
Server Pool Management	Rebalance Resource Edit Server Pool Attribute Attach Network to Server Pool Associate Library to Server Pool Add/Remove Virtual Host
Server Pool Usage	Create OVM virtual Servers Create zone servers Create Logical Domains
Virtualization Host Creation	Create Virtualization Host
Virtualization Host Deletion	Delete Virtualization Host
Virtualization Host Management	Add/Remove Virtual Host to/from Server Pool Edit Tags Edit Attributes Reboot Change Routing Configuration Change NFS4 Domain Change Naming Service Change Remote Logging Configuration
Virtualization Host Usage	Create Logical Domains Create zones Create OVM virtual servers
Virtualization Guest Creation	Create Logical Domains Create zones Create OVM virtual servers
Virtualization Guest Deletion	Delete Logic Domain Delete Zones Delete OVM Virtual Servers

Table 7–2 (Cont.) Permissions and Tasks

Permission	Tasks
Virtualization Guest Usage	Start Guest Shutdown Guest Migrate Guest Clone Guest
Solaris Zone Creation	Create Solaris Zone
Solaris Zone Deletion	Delete Solaris Zone
Solaris Zone Host Management	Solaris Zone Host Management
Solaris Zone Management	Solaris Zone Management
Storage Creation	Create Library
Storage Deletion	Delete Library
Storage Usage	Associate Library
Network Creation	Create Network Domain Create Network (manage network)
Network Deletion	Delete Network Domain Delete Network
Network Usage	Assign Network Connect Guests
Fabric Creation	Create Fabric
Fabric Deletion	Delete Fabric
Fabric Usage	Fabric Management
Chassis Usage	Chassis Usage
Storage Server Usage	Storage Server Usage
Switch Usage	Switch Usage
Server Usage	Launch LOM Controller Edit Tags
Operating System Usage	Edit Tags Edit Attributes
Rack Creation	Create Rack
Directory Server Management	Directory Server Management
Power Distribution Unit Usage	Power Distribution Unit Usage
Power Distribution Unit Management	Power Distribution Unit Management
Rack Creation	Rack Creation
Rack Deletion	Rack Deletion
Rack Management	Rack Management
Rack Usage	Rack Usage
OVM Manager Usage	OVM Manager Usage

Table 7–2 (Cont.) Permissions and Tasks

Permission	Tasks
OVM Manager Management	OVM Manager Management
Network Domain Creation	Network Domain Creation
Network Domain Deletion	Network Domain Deletion
Network Domain Management	Network Domain Management
Network Domain Usage	Network Domain Usage
Asset Network Management	Asset Network Management
Job Management	Job Management

Managing Roles

Users with the Role Admin role can grant users different roles and privileges.

1. Select **Administration** in the Navigation pane.

2. Click the **Roles** tab.

The Roles page is displayed.

3. Select a user from the list of users.

4. Click the **Manage User Roles** icon.

5. Add or remove one or more roles from the selected roles list.

By default, users are given full privileges for each of their assigned roles. To specify privileges, deselect the Use the default Role associations box.

Click **Next**.

6. If you chose to specify privileges, the privileges for each type of target are displayed on separate pages. Select the roles to apply to each target, then click **Next**.

7. The Summary page is displayed. Review the roles and privileges assigned to the user, then click **Finish**.

Replicating a User

You can copy a user's roles and privileges to other target users. The target users' current roles and privileges are overwritten.

Note: You can replicate a user from a directory server, but only the user's privileges are replicated. The target user must begin with the same roles as the source user.

1. Select **Administration** in the Navigation pane.

2. Click either **Local Users** or a directory server.

The users are displayed.

3. Select the source user from the list of users.

4. Click the **Replicate User Roles** icon.
The Replicate User Roles page is displayed.
5. Add one or more users to the list of target users.
6. Click **Replicate Roles**.

About Notification Profiles

Notification Profiles determine how notifications are sent to a user and what levels of notifications are sent. By configuring separate notification profiles, different users can receive specific levels of notifications through the UI, through email, or through a pager.

Eight levels of notification can be sent:

- **None:** No notifications are sent to the destination.
- **Incident Severity >= Critical:** Incidents of critical severity are sent to the destination.
- **Incident Severity >= Warning:** Incidents of critical or warning severity are sent to the destination.
- **Incident Severity >= Info:** Incidents of any severity are sent to the destination.
- **Incident updates and all severities:** Incidents of any severity and incident updates such as status changes and new annotations are sent to the destination.
- **Notification Priority >= High:** High severity notifications are sent to the destination. This level can only be sent to the user interface.
- **Notification Priority >= Medium:** Medium and high severity notifications are sent to the destination. This level can only be sent to the user interface.
- **Notification Priority >= Low:** Low, medium, and high severity notifications are sent to the destination. This level can only be sent to the user interface.

Different levels of notifications can be sent for specific Server Pools, or asset groups.

If a user has no notification profile, all notifications of medium or high severity for all assets are sent to the UI, and no notifications are sent to other destinations.

Configuring a Notification Profile

You can configure a new notification profile for a user or edit an existing profile.

1. Select **Administration** in the Navigation pane.
2. Select **Local Users** in the Navigation pane.
The Users tab is displayed.
3. Select the user for whom you want to configure notifications.
4. Click the **Configure Notification Profile** icon.
The Configure Notification Profile Wizard is displayed.
If a Notification Profile has already been configured for the user, the existing profile is displayed.
5. Select either **Subscribe to All Messages** or **Subscribe to Custom List of Messages**.
 - If you select **Subscribe to All Messages**, you receive notifications for all assets.

Use the User Interface drop-down list to select the severity of messages to be received through the UI.

Use the Email drop-down list to select the severity of messages to be received through email.

Use the Pager drop-down list to select the severity of messages to be received through a pager.

- If you select **Subscribe to Custom List of Messages**, the **Configure Group Notifications** page and **Configure Server Pool Notifications** pages are displayed. You receive the specified priority of notifications for each Group and Server Pool.

For each Group, select the severity of messages to be received through the UI, email, and pager.

For each Server Pool, select the severity of messages to be received through the UI, email, and pager.

6. If you chose to receive notifications by email, enter the email information:

- **Email Address:** The destination email address.
- **Mail Host:** The mailhost to use in sending the email. Enter localhost or the name or IP address of the Enterprise Controller to send emails directly.
- **Port:** The port to use in sending the email.
- **Mail User Name:** Enter a user name if it is required by the mail host.
- **Mail Password:** Enter a password if it is required by the mail host.
- **Connection Security:** Select STARTTLS or SSL/TLS for the connection security.
- **From Email Address:** Enter the email address from which email notifications are sent.

7. If you chose to receive notifications by pager, enter a pager address, then click **Next**.

The Summary page is displayed.

8. Click **Update Notification Profile**.

The new notification profile is applied.

Deleting a Notification Profile

Notification Profiles determine what events generate notifications for a user and how those notifications are sent to the user. If a user's notification profile is deleted, Oracle Enterprise Manager Ops Center only sends notifications of medium or high severity to the UI, and does not send notifications by email or pager.

1. Select **Administration** in the Navigation pane.
2. Select **Local Users** in the Navigation pane.
The Users tab is displayed.
3. Select the user whose Notification Profile you want to delete.
4. Click the **Delete Notification Profile** icon.

The Delete User Notification Profile confirmation window is displayed.

5. Click **Delete**.

The User's Notification Profile is deleted.

Viewing the Audit Log

Whenever a user is added or deleted, or new roles are assigned to a user, an entry for the event is added to the Oracle Enterprise Manager Ops Center audit log. The log also contains the details of the connection. You can view this log to verify and track changes to users and roles.

You must have root permissions on the Enterprise Controller system to view the audit log. This log cannot be edited.

See the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about the audit log.

1. Log in to the Enterprise Controller system as an administrative user.
2. Change to the directory containing the log files. The log files are in the following directory:
 - On Oracle Solaris: `/var/cacao/instances/oem-ec/logs/audit-logs.*`
 - On Linux: `/var/opt/sun/cacao2/instances/oem-ec/logs/audit-logs.*`
3. View the most recent log. Log entries are stored in the format `<date/time> <action> <connection info> <additional info>`.

Backup and Recovery

Oracle Enterprise Manager Ops Center has capabilities that can be used to recover data and resume functions if the Enterprise Controller system fails.

The following features and topics are covered in this chapter:

- [Introduction to Backup and Recovery](#)
- [Backing Up and Restoring an Enterprise Controller](#)
- [Backing Up and Restoring a Proxy Controller](#)

Introduction to Backup and Recovery

Oracle Enterprise Manager Ops Center has several tools that can be used for disaster recovery. These tools let you preserve Oracle Enterprise Manager Ops Center data and functionality if the Enterprise Controller or Proxy Controller systems fail.

The `ecadm backup` and `ecadm restore` commands back up and restore the Enterprise Controller. They also back up and restore the colocated Proxy Controller unless otherwise specified. The `proxyadm backup` and `proxyadm restore` commands back up and restore remote Proxy Controllers.

The `ecadm backup` command creates a tar file that contains all of the Oracle Enterprise Manager Ops Center information stored by the Enterprise Controller, including asset data, administration data, job history, and the database password, but not including software and storage library contents. The `proxyadm backup` command creates a tar file that contains all of the Oracle Enterprise Manager Ops Center information stored by the Proxy Controller, including asset data. You can specify the name and location of the backup file and the log file for each command.

Run the `ecadm backup` and `proxyadm backup` commands regularly and save the backup files on a separate system.

If the Enterprise Controller system fails, you can use the `ecadm restore` command and the backup file to restore the Enterprise Controller to its previous state on the original system or on a new system. The new Enterprise Controller system must have the same operating system and architecture, and must have the same version of Oracle Enterprise Manager Ops Center installed as was used when the backup was made. The `ecadm restore` command accepts the name of the backup file as input, and restores the Enterprise Controller to the state it had at the time of the backup. If the new Enterprise Controller system has a new IP address, you must manually update the Proxy Controllers to use the new IP address.

If a remote Proxy Controller system fails, you can use the `proxyadm restore` command and the backup file to restore the Proxy Controller. The `proxyadm restore` command

accepts the name of the backup file as input, and restores the Proxy Controller to the state it had at the time of the backup.

Some of the procedures described in this section use the `ecadm` and `proxyadm` commands. See [Appendix A, "Command Line Administration"](#) for more information about these commands.

- On Oracle Solaris systems, these commands are in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, these commands are in the `/opt/sun/xvmoc/bin/` directory.

Backing Up and Restoring an Enterprise Controller

You can use the `ecadm` command to back up and restore an Enterprise Controller.

Backing Up an Enterprise Controller

You can create a backup for the Enterprise Controller using the `ecadm` command with the `backup` subcommand.

By default, the server data is saved in a backup file in the `/var/tmp` directory with a file name that includes a date and time stamp. You can define the file name and location during the backup, as shown in the example below.

If you are using an embedded database, the backup file includes the product schema from the embedded database. This database schema includes all logical structures and data related to Oracle Enterprise Manager Ops Center. If you are using a customer-managed database, you can back up the database schema using the `--remotedb` option, or you can use the existing backup and recover processes implemented by your database administrator.

1. From the command line, log in to the Enterprise Controller system.
2. Use the `ecadm` command with the `backup` subcommand to back up the Enterprise Controller.

The following options may be used with the `ecadm` command:

- **-o | --output <backup file>**: Specify the file in which the backup archive is generated. Do not specify a path inside the `/opt/*xvm*` directories. The default output file is `/var/tmp/sat-backup-<date>-<time>.tar`.
- **-c | --configdir <dir>**: Specify an alternate backup configuration directory.
- **-l | --logfile <logfile>**: Save output from command in `<logfile>`. Log files are stored in the `/var/opt/sun/xvm/logs/` directory.
- **-d | --description <description string>**: Embed the `<description string>` as the description of the backup archive.
- **-r | --remotedb**: If the Enterprise Controller uses a customer-managed database, export the database schema to a `.dmp` file in the Oracle Enterprise Manager Ops Center dump directory on the database server. This directory is `/var/tmp/ocdumpdir` in the examples used in the installation documentation, but any directory can be specified as the dump directory during installation and configuration. The `.dmp` file lets the restore operation restore the database schema. This option only backs up the Oracle Enterprise Manager Ops Center database schema; other schemas and data are not included.
- **-t | --tag <tag>**: Embed `<tag>` as a single-word tag in the backup archive.

- **-T|--tempdir <dir>**: Specify the temporary staging directory location.
- **-v|--verbose**: Increase the verbosity level. This option may be repeated.

For example:

```
ecadm backup -o /var/backup/EC-17December.tar
ecadm: using logFile = /var/opt/sun/xvm/logs/sat-backup-2012-12-17-16:21:12.log
ecadm: *** PreBackup Phase
ecadm: *** Backup Phase
ecadm: *** PostBackup Phase
ecadm: *** Backup complete
ecadm: *** Output in /var/backup/EC-12December.tar
ecadm: *** Log in /var/opt/sun/xvm/logs/sat-backup-2012-12-17-16:21:12.log
```

3. Copy the backup file to a separate system.

Restoring an Enterprise Controller

You can use a backup file to restore the state of the Enterprise Controller to the state it had at the time of the backup.

This procedure restores the data from the backup file, which is the archive created by the `ecadm backup` operation.

If you are using an embedded database, the restore process restores the product schema from the embedded database. If you are using a customer-managed database, you can use the `--remotedb` option to restore the product schema on the customer-managed database, or leave this option off to make no changes to the database.

1. Prepare the Enterprise Controller system.

- If you are restoring the backup on a new system, then the new system must have the same architecture and operating system as the old system. It is recommended that the operating system versions be identical, including updates and SRUs. The new system's host name and Enterprise Controller software version must also match those of the backed up system.
- If you are restoring the backup on the same system, but the software has become corrupt or an upgrade failed, uninstall the Enterprise Controller software.

Run the `install` script with the `-e` and `-k` options. The `-e` option uninstalls the Enterprise Controller and co-located Proxy Controller, and the `-k` option preserves the Oracle Configuration Manager software. For example:

```
# cd /var/tmp/OC/xvmoc_full_bundle
# install -e -k
```

- If you are restoring the backup on the same system, and the software is functioning normally, unconfigure the Enterprise Controller.
2. Install the Enterprise Controller if it has not been installed, but do not configure the Enterprise Controller, as the `ecadm restore` command restores your configuration settings.
 - Oracle Solaris OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*.
 - Linux OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*.

Note: If you are using a customer-managed database which is still functioning, the Enterprise Controller installation procedure indicates several steps that you must skip and an additional option that you must use to avoid overwriting your existing database schema.

3. Upgrade the Enterprise Controller to the same version that was running when the backup was made, if it is not already running that version. Perform this upgrade from the command line.
4. Run the `ecadm` command with the `restore` subcommand and the `-i <backup directory location and file name>` option.

The following options may be used with the `ecadm` command:

- **-i | --input <backup file>:** (Required) Specify the location of the backup file.
- **-c | --configdir <dir>:** Specify an alternate restore configuration directory.
- **-l | --logfile <logfile>:** Save output from command in <logfile>. Log files are stored in the `/var/opt/sun/xvm/logs/` directory.
- **-r | --remotedb:** If the Enterprise Controller uses a customer-managed database, this option restores the product schema on that database. If you are restoring on a new database system, copy the `.dmp` file that corresponds with your backup file from the Oracle Enterprise Manager Ops Center dump directory to the new database system and verify that it is owned by the oracle user on the new system.
- **-e | --echa:** If the Enterprise Controller is configured in HA mode, this option indicates that the colocated Proxy Controller should not be restored.
- **-T | --tempdir <dir>:** Specify the temporary staging directory location.
- **-v | --verbose:** Increase verbosity level (may be repeated)

For example:

```
ecadm restore -i /var/backup/EC-17December.tar
ecadm: using logFile =
/var/opt/sun/xvm/logs/sat-restore-2012-12-17-21:37:22.log
ecadm: *** PreRestore Phase
ecadm: *** Restore Phase
ecadm: *** PostRestore Phase
ecadm: *** Log in /var/opt/sun/xvm/logs/sat-restore-2012-12-17-21:37:22.log
```

5. For an Enterprise Controller with a co-located Proxy Controller, check the Proxy Controller's status using the `proxyadm` command with the `status` subcommand. If the Proxy Controller is stopped, restart it using the `proxyadm` command with the `start` subcommand and the `-w` option.

```
# proxyadm status
offline
# proxyadm start -w
proxyadm: Starting Proxy Controller with SMF...
proxyadm: Proxy Controller services have started
#
```

6. If you restored the Enterprise Controller on a new system, reconfigure each remote Proxy Controller to use the new Enterprise Controller.
 - a. As root, log in to the Proxy Controller.

- b. Unconfigure the Proxy Controller using the `proxyadm` command with the `unconfigure` subcommand and the `-k` option. For example:


```
# proxyadm unconfigure -k
```
- c. Reconfigure the Proxy Controller using the `proxyadm` command with the `configure` subcommand and the `-s` <Enterprise Controller hostname>, `-u` <Enterprise Controller admin user name>, and `-p` <Enterprise Controller password file name> options. For example:


```
# proxyadm configure -s <new hostname> -u root -p <passwordfilename>
```
- d. Restart the Proxy Controller using the `proxyadm` command with the `start` subcommand and the `-w` option. For example:


```
# proxyadm start -w
```

Note: After restoring the Enterprise Controller, the asset details might take several minutes to display completely in the user interface.

Example: Restoring an Enterprise Controller With an Embedded Database

In this example, the `ecadm restore` command includes options to set the restore in verbose mode (`-v`), and to create a restore log (`-l`) for debugging purposes. The input (`-i`) option specifies the backup file location.

```
# /opt/SUNWxvmoc/bin/ecadm restore -v -i /var/tmp/OC/server1/EC-17December.tar -l logfile-restore-15January.log
```

Example: Restoring an Enterprise Controller With a Customer-Managed Database

In this example, the `ecadm restore` command includes the (`-r`) option to restore the database schema on a customer-managed database. The input (`-i`) option specifies the backup file location.

```
# /opt/SUNWxvmoc/bin/ecadm restore -i /var/tmp/OC/server1/EC-17December.tar -r
```

Example: Restoring an Enterprise Controller With a Customer-Managed Database Without Restoring the Database Schema

In this example, the `ecadm restore` command includes options to set the restore in verbose mode (`-v`), and to create a restore log (`-l`) for debugging purposes. The input (`-i`) option specifies the backup file location. The (`-r`) option is not included.

```
# /opt/SUNWxvmoc/bin/ecadm restore -v -i /var/tmp/OC/server1/EC-17December.tar -l logfile-restore-15January.log
```

Backing Up and Restoring a Proxy Controller

You can use the `proxyadm` command to back up and restore a remote Proxy Controller.

The Proxy Controller backup file includes asset data, but does not include the contents of the `/var/opt/sun/xvm/images/os` directory. You must back up images stored in this directory separately.

Backing Up a Proxy Controller

You can create a backup for a remote Proxy Controller using the `proxyadm` command with the `backup` subcommand. If you are using a co-located Proxy Controller, it is backed up by the `ecadm backup` operation, and no additional backup is needed.

By default, the server data is saved in a backup file in the `/var/tmp` directory with a file name that includes a date and time stamp. You can define the file name and location during the backup, as shown in the example below.

1. From the command line, log in to the Proxy Controller system.
2. Use the `proxyadm` command with the `backup` subcommand to back up the Proxy Controller.

The following options may be used with the `proxyadm` command:

- **-o | --output <backup file>**: Specify the file in which the backup archive is generated. Do not specify a path inside the `/opt/*xvm*` directories. The default output file is `/var/tmp/proxy-backup-<date>-<time>.tar`.
- **-c | --configdir <dir>**: Specify an alternate backup configuration directory.
- **-l | --logfile <logfile>**: Save output from command in <logfile>. Log files are stored in the `/var/opt/sun/xvm/logs/` directory.
- **-d | --description <description string>**: Embed the <description string> as the description of the backup archive.
- **-t | --tag <tag>**: Embed <tag> as a single-word tag in the backup archive.
- **-T | --tempdir <dir>**: Specify the temporary staging directory location.
- **-v | --verbose**: Increase the verbosity level. This option may be repeated.

For example:

```
proxyadm backup -o /var/backup/PC-B_Sept14.tar
```

3. Copy the backup file to a separate system.

Restoring a Proxy Controller

You can use a backup file to restore the state of a Proxy Controller to the state it had at the time of the backup.

This procedure restores the data from the backup file, which is the archive created by the `proxyadm backup` operation.

1. Install the Proxy Controller if it has not been installed.
 - Oracle Solaris OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*.
 - Linux OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*.
2. Upgrade the Proxy Controller to the same version that was running when the backup was made, if it is not already running that version. Perform this upgrade from the command line.
3. Run the `proxyadm` command with the `restore` subcommand and the `-i <backup directory location and file name>` option.

The following options may be used with the `proxyadm` command:

- **-i | --input <backup file>:** (Required) Specify the location of the backup file.
- **-c | --configdir <dir>:** Specify an alternate restore configuration directory.
- **-l | --logfile <logfile>:** Save output from command in <logfile>. Log files are stored in the `/var/opt/sun/xvm/logs/` directory.
- **-T | --tempdir <dir>:** Specify the temporary staging directory location.
- **-v | --verbose:** Increase verbosity level (may be repeated)

For example:

```
proxyadm restore -i /var/backup/PC-B_Sept14.tar
```

4. Stop the Proxy Controller by running the `proxyadm` command with the `stop` subcommand and the `-w` option.

For example:

```
proxyadm stop -w
```

5. Start the Proxy Controller by running the `proxyadm` command with the `start` subcommand and the `-w` option.

For example:

```
proxyadm start -w
```

High Availability

Oracle Enterprise Manager Ops Center has several capabilities that can be used to recover data and resume functions if the Enterprise Controller system or a Proxy Controller system fail.

If you set up a High Availability configuration during the installation and configuration process, you can fail over to the standby Enterprise Controller if the active Enterprise Controller fails.

The following features and topics are covered in this chapter:

- [Introduction to High Availability](#)
- [Enabling and Using Enterprise Controller High Availability](#)
- [Enabling and Using Proxy Controller High Availability](#)

Introduction to High Availability

Oracle Enterprise Manager Ops Center has several tools that can be used for disaster recovery. These tools let you preserve Oracle Enterprise Manager Ops Center data and functionality if the Enterprise Controller or Proxy Controller systems fail.

Some of the procedures described in this section use the `ecadm` command. See [Appendix A, "Command Line Administration"](#) for more information about this command.

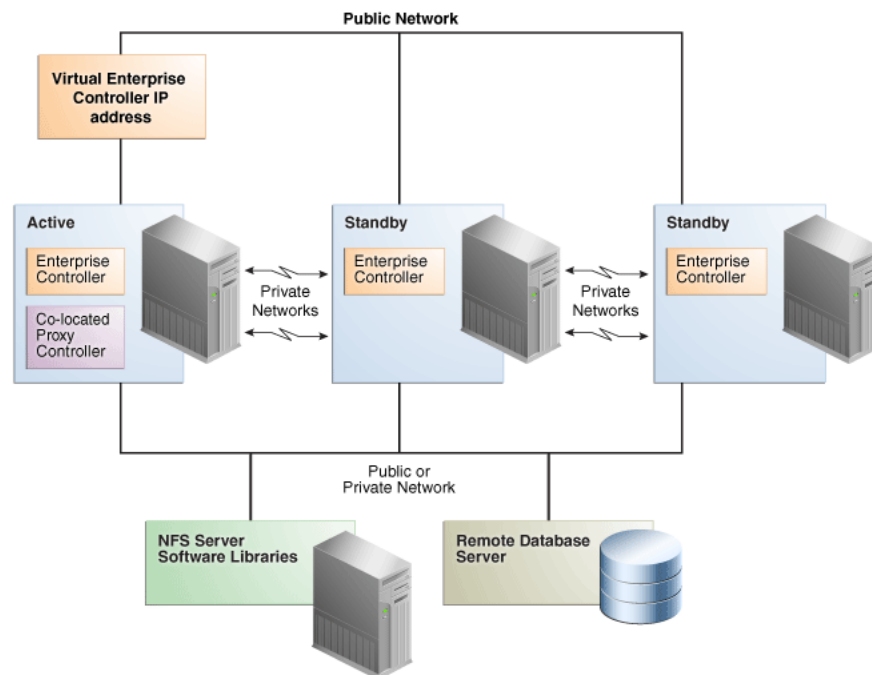
- On Oracle Solaris systems, this command is in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, this command is in the `/opt/sun/xvmoc/bin/` directory.

Enterprise Controller High Availability

High Availability is a setup involving multiple Enterprise Controllers using Oracle Clusterware and a remote database. The active Enterprise Controller is used for all Oracle Enterprise Manager Ops Center operations. The standby Enterprise Controllers are configured as backups. The user interface uses a virtual IP address (VIP), which always connects to the active Enterprise Controller.

If the active Enterprise Controller must be taken offline, you can make another Enterprise Controller active. One of the standby Enterprise Controllers is also activated if the active Enterprise Controller fails.

[Figure 9–1, "Enterprise Controller High Availability Configuration"](#) shows an example Enterprise Controller High Availability configuration.

Figure 9–1 Enterprise Controller High Availability Configuration

Note: If you have not yet installed Oracle Enterprise Manager Ops Center, the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System* and *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems* explain how to install with Enterprise Controller High Availability.

The following are requirements for a High Availability environment:

- Use two or more systems of the same model and configured identically:
 - Processor class
 - Operating system
 - Oracle Enterprise Manager Ops Center software version, including updates
 - Network interfaces that are cabled identically to the same subnets
- Add an asset tag to identify the active Enterprise Controller and to distinguish it from the standby Enterprise Controller using the Edit Asset action.
- Maintain the standby Enterprise Controller's system in the same way as the active Enterprise Controller. The active and standby Enterprise Controllers must use the same version of Oracle Enterprise Manager Ops Center software. If you cannot use the user interface to verify the installed software versions at the time that you need to transfer functions to the standby system, view the content of the `/nlgc-setup/.version.properties` file. The `product.version` property lists the specific revision level of the installed software. For example:

```
cat /nlgc-setup/.version.properties
#Note: This file is created at build time.
#Sat Nov 03 23:48:37 MDT 2012
jar.sign=true
date=2012/11/03 23\;48
```

```

build.variation=xvmopscenter
oc.build.type=dev-ga
product.version=12.2.0.2457
product.installLocation=/var/opt/sun/xvm/EnterpriseController_installer_
12.2.0.2457
#

```

Verify that the product.version property lists the same version on the active and standby Enterprise Controllers before you perform a relocate procedure.

- Configure one shared private network. Gigabit speed is recommended.
- Configure at least one shared public network. Gigabit speed is recommended.
- Make the following public network addresses available:
 - **<node#>-vip** - One address of this format should be available for each node.
 - **cluster SCAN address**
- An EC HA environment must use a customer-managed database on a system other than the Enterprise Controller systems.
- The Enterprise Controller libraries must be NFS shares that are accessible by every Enterprise Controller system.
- Configure a shared storage solution. This can be:
 - A shared NFS filesystem configured for root access by each node.
 - Shared SAN storage with at least one FibreChannel LUN connected to each server with identical /dev/dsk and /dev/rdisk names.

The following are limitations of a High Availability environment:

- User accounts and data that are not associated with Oracle Enterprise Manager Ops Center are not part of the relocate process. Only Oracle Enterprise Manager Ops Center data is moved between the active and standby Enterprise Controllers.
- UI sessions are lost on relocate.
- The EC HA configuration applies only to the Enterprise Controller.

Proxy Controller High Availability

A specific Proxy Controller manages each asset. If a Proxy Controller fails or is uninstalled, you are prompted to migrate assets to another Proxy Controller if one is available. Alternatively, you can enable automatic failover, which automatically migrates assets to another Proxy Controller if their current Proxy Controller becomes unreachable. In either case, you can manually move assets to a new Proxy Controller at any time.

To migrate an asset to a new Proxy Controller, the destination Proxy Controller must either be connected to the networks of the assets being moved, or be associated with those networks and have them enabled. The destination Proxy Controller must also be online and reachable.

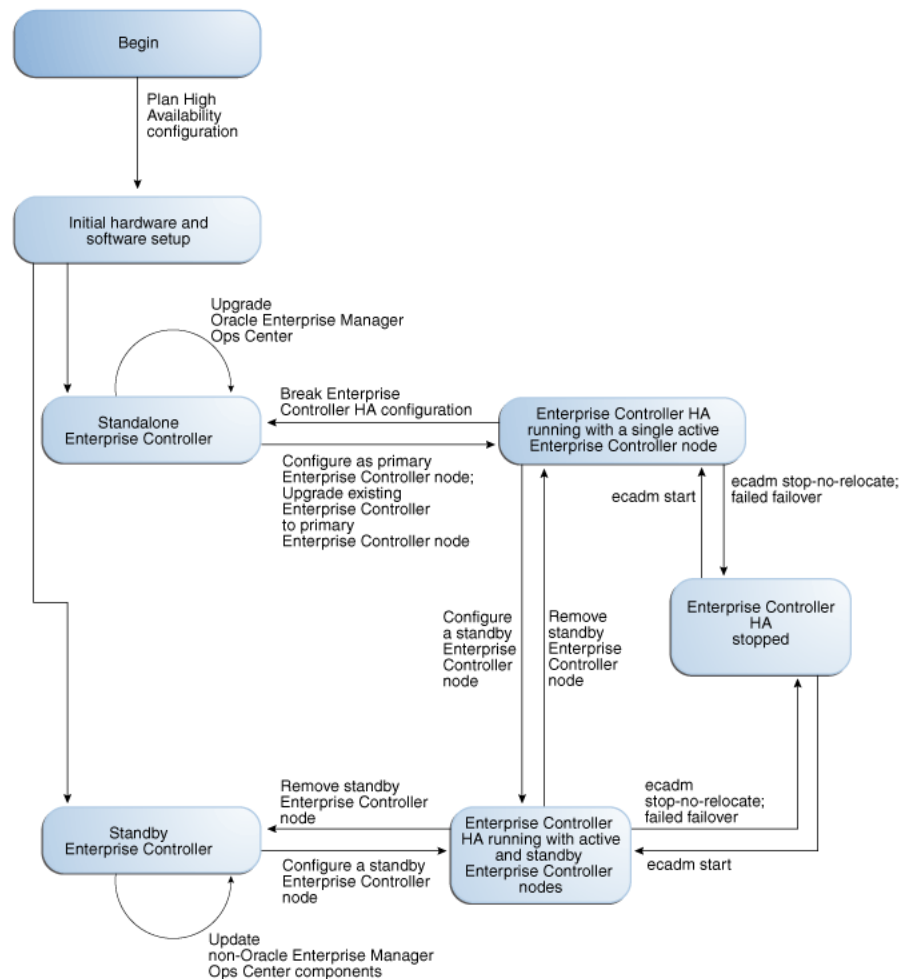
Enabling and Using Enterprise Controller High Availability

You can use Oracle Clusterware and Oracle Real Application Cluster software to create a High Availability configuration. A High Availability configuration includes one active Enterprise Controller node and one or more standby Enterprise Controller nodes, all using an external database. If the active Enterprise Controller node fails, a

standby node is made active, and a notification is sent to notify the user that the relocate has occurred.

Figure 9–2, "Enterprise Controller High Availability States" shows the possible states of an Enterprise Controller High Availability configuration and the steps needed to move between them.

Figure 9–2 Enterprise Controller High Availability States



Converting a Single Enterprise Controller to High Availability

If you are using a single configured Enterprise Controller, you can switch to a high availability configuration.

This procedure assumes that you have already installed and configured a single Enterprise Controller. If you have not installed and configured an Enterprise Controller, see the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System* or the *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems* for information on installing with High Availability.

Preparing for High Availability with Oracle Clusterware

Installing and configuring Oracle Clusterware is the first step in setting up High Availability in your environment.

1. Install Oracle Clusterware in your environment using the *Grid Infrastructure Installation Guide for Oracle Solaris Systems* or the *Grid Infrastructure Installation Guide for Linux Systems*.
2. If you are using a local database, switch to a remote database. See [Chapter 3, "Database Management"](#) for more information.

Making the Current Enterprise Controller the Primary Node

Once your environment is prepared, configure the current Enterprise Controller as the primary node.

1. Stop the Enterprise Controller using the `ecadm` command and the `stop` subcommand.
2. Use the `ecadm` command with the `ha-configure-primary` subcommand to configure the system as the active Enterprise Controller.

If the clusterware `crsctl` command is not in the `/u01` directory, use the `--crsctl_basepath <location>` option to specify its location.

For example:

```
# ./ecadm ha-configure-primary
INFO: HAECClusterwareAdapter/doConfigurePrimary() Stopping Ops Center ...
INFO: HAECClusterwareAdapter/doConfigurePrimary() Ops Center stopped
INFO: HAECClusterwareAdapter/createActionScript() created Resource Action
Script='/var/opt/sun/xvm/ha/EnterpriseController'
INFO: HAECClusterwareAdapter/doConfigurePrimary() created Clusterware Action
Script='/var/opt/sun/xvm/ha/EnterpriseController'
INFO: HAECClusterwareAdapter/doConfigurePrimary() created Clusterware
Resource='EnterpriseController'
INFO: HAECClusterwareAdapter/doHABStart() starting
resource='EnterpriseController' on node='primary-system'
INFO: HAECClusterwareAdapter/doHABStart()statusSB='CRS-2672: Attempting to start
'EnterpriseController' on 'primary-system'
CRS-2676: Start of 'EnterpriseController' on 'primary-system' succeeded'
INFO: HAECClusterwareAdapter/doHABStart() started
resource='EnterpriseController' on node='primary-system'
INFO: HAECClusterwareAdapter/doConfigurePrimary() Ops Center started on
node='primary-system'
ecadm:    --- Enterprise Controller successfully configured HA primary node
#
```

Installing a Standby Node

Once you have configured one Enterprise Controller as the active node, you can install and configure standby nodes.

1. If you are installing on Oracle Solaris 11, and if the system requires an HTTP proxy to reach the Internet, set the `http_proxy` and `https_proxy` environment variables. These values are only used during the installation. Use the following format:
 - `http_proxy=http://<proxy IP address>:<port number>` or `http://<username:password>@<proxy IP address>:<port number>` - This variable specifies the proxy server to use for HTTP.
 - `https_proxy=https://<proxy IP address>:<port number>` or `https://<username:password>@<proxy IP address>:<port number>` - This variable specifies the proxy server to use for HTTPS.

For example:

```
export http_proxy=http://10.79.204.11:8080
export https_proxy=https://10.79.204.12:8080
```

2. If you are installing on Oracle Solaris 11, check the user type for the root user. If root is a role, configure root as a normal user. For example:

```
# grep root /etc/user_attr
root:::type=role;auths=solaris.*,solaris.grant;profiles=...
# sudo rolemod -K type=normal root
```

3. Create a temporary directory on your system, then copy or move the appropriate Oracle Enterprise Manager Ops Center archive for your system from delivery media to the temporary directory that you created. For example:

```
# mkdir /var/tmp/OC
# cp enterprise-controller.Solaris.i386.12.2.0.2457.tar.gz /var/tmp/OC
```

The installation archive consumes about 3.5 GBytes of disk space.

4. Change to the directory where the installation archive is located on your system.

```
# cd /var/tmp/OC
#
```

5. Expand the installation archive, then list the contents of the expanded directory.

- If your installation archive has the .zip extension, use the unzip command to uncompress the archive. For example:

```
# unzip enterprise-controller.Solaris.i386.12.2.0.2457.zip
# ls
enterprise-controller.Solaris.i386.12.2.0.2457.zip
xvmoc_full_bundle
#
```

- If your installation archive has the .tar.zip extension, use the unzip and tar commands to uncompress and un-tar the archive, then list the contents of the temporary directory. The following command example retains the original compressed archive file. The data extracted from the archive consumes about 1 GB of additional space. For example:

```
# unzip enterprise-controller.Solaris.i386.12.2.0.2457.tar.zip | tar xf -
# ls
enterprise-controller.Solaris.i386.12.2.0.2457.tar.zip
xvmoc_full_bundle
#
```

6. Create a database properties file on the Enterprise Controller system. The database properties file must contain the location of the customer-managed database and a user name and password that can access the database.

The database information can be found in the `tnsnames.ora` file.

For example:

```
# vi /var/tmp/RemoteDBProps.txt
mgmtdb.appuser=TESTSCHEMA
mgmtdb.password=TESTSCHEMA_PWD
mgmtdb.roappuser=TESTSCHEMA_RO
mgmtdb.ropassword=TESTSCHEMA_RO_PWD
mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<database service name>
```

The `mgmtdb.dburl` property can be entered in any of these formats:

```
mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<database service
name>
mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>:<SID>
mgmtdb.dburl=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=<host
>) (PORT=<port>)) (CONNECT_DATA=(SERVICE_NAME=<service>)))
```

7. Change directory to `xvmoc_full_bundle`, and run the install script with the `--remoteDBprops` <path to database properties file> and `--standbyEC` options. For example:

```
# cd xvmoc_full_bundle
# ./install --remoteDBprops=/var/tmp/remoteDBProps.txt --standbyEC
```

8. The Oracle Configuration Manager installation text is displayed. Enter the My Oracle Support user name or email address that you want to associate with Oracle Enterprise Manager Ops Center.

Provide your email address to be informed of security issues, install and initiate Oracle Configuration Manager. Easier for you if you use your My Oracle Support Email address/User Name.

Visit <http://www.oracle.com/support/policies.html> for details.

Email address/User Name:

9. If you want security updates to appear on your My Oracle Support page, enter your My Oracle Support password.

Provide your My Oracle Support password to receive security updates via your My Oracle Support account.

Password (optional):

The screen clears, then the install script displays a list of installation tasks that automatically updates as the installation proceeds. For example:

```
Ops Center Enterprise Controller Installer
(version 12.2.0.2457 on SunOS)
```

1. Check for installation prerequisites.	[Not Completed]
2. Configure file systems.	[Not Completed]
3. Install prerequisite packages.	[Not Completed]
4. Install Agent components.	[Not Completed]
5. Create Deployable Proxy Bundles.	[Not Completed]
6. Install application packages.	[Not Completed]
7. Run postinstall tasks.	[Not Completed]
8. Install Expect.	[Not Completed]
9. Install IPMI tool.	[Not Completed]
10. Set database credentials.	[Not Completed]
11. Install and Configure Oracle Database.	[Not Completed]
12. Seed Ops Center Database Schema	[Not Completed]
13. Install Service container components.	[Not Completed]
14. Install Core Channel components.	[Not Completed]
15. Install Proxy Core components.	[Not Completed]
16. Set Proxy database credentials.	[Not Completed]
17. Install Enterprise Controller components.	[Not Completed]
18. Install Update Connection - Enterprise.	[Not Completed]
19. Install Ops Center BUI components.	[Not Completed]
20. Install OS provisioning components.	[Not Completed]
21. Initialize and start services.	[Not Completed]
Executing current step: Check for installation prerequisites...	

10. Review and correct any problems when the install script checks for installation prerequisites that are not met. For example, this install script detected insufficient disk space:

```
Warning for Step: Check for installation prerequisites.
The following is a portion of the installer
log which may indicate the cause of the warning.
If this does not indicate the cause of the
warning, you will need to view the full log
file. More information on how to do that is
available below.
You may choose to ignore this warning by selecting to continue.
* * * * *

Ignoring job: 01checkRPMs.pl
Ignoring job: 03removeEmptyDirs.pl

Executing job: jobs/00checkPrereqs.pl --install

WARNING: Installation prerequisites not met:
Disk: / 72G needed, 24G available.
* * * * *

Please fix the problem and then try this step again.
For a full log of the failed install see the file: /var/tmp/installer.log.9361.

t. Try this step again (correct the failure before proceeding)
c. Continue (ignore the warning)
x. Exit
Enter selection: (t/c/x)
```

You can enter `t` to try again, `c` to continue and ignore the warning, or `x` to exit the install script. You should exit the install script, correct the problem, and then run the install script again, which resumes from where it stopped. Choose to continue and ignore the warning only if you accept the impact of the error condition on your installation. Entering `t` typically produces the same error, unless you are able to correct the problem before trying the step again. If the install script finds that all prerequisites have been satisfied, or if you choose to continue despite the warning, the install script continues and installs all Enterprise Controller and Proxy Controller components.

When complete, the install script displays a confirmation that all components have been installed. The `/var/tmp/installer.log.latest` file contains the installation log.

11. Create a password file containing the root user name and password for the active Enterprise Controller. For example:

```
# touch /tmp/creds.props
# chmod 400 /tmp/creds.props
# vi /tmp/creds.props
# cat /tmp/creds.props
username:root
password:XXXXX
```

12. Use the `ecadm` command with the `ha-configure-standby` and `-p <password file>` subcommands to configure the node as a standby node.

If the clusterware `crsctl` command is not in the `/u01` directory, use the `--crsctl_basepath <location>` option to specify its location.

For example:

```
# ecadm ha-configure-standby -p /tmp/creds.props
INFO: HAECClusterwareAdapter/doConfigureStandby() Stopping Ops Center ...
INFO: HAECClusterwareAdapter/doConfigureStandby() Ops Center stopped
INFO: remoteFileCopy() copied '/etc/passwd' from
remoteHostname='primary-system' to local file='/tmp/activeNodepw'
<output omitted>
ecadm:    --- Enterprise Controller successfully configured HA standby node
```

13. Use the `ecadm` command with the `ha-status -d` option to check the status of the standby Enterprise Controller.

For example:

```
# ecadm ha-status -d
INFO: HAECClusterwareAdapter/doHASStatus() Status:
# HAEC Cluster Info: Thu Sep 29 15:49:09 MDT 2011
haec.cluster.active.node=primary
haec.cluster.nodes=standby, primary
haec.ec.public.nics=ngel
haec.ec.status=ONLINE
<output omitted>
haec.cluster.script=/var/opt/sun/xvm/ha/EnterpriseController
haec.cluster.crsctl=/u01/app/11.2.0/grid/bin/crsctl
# End of Cluster Info
ecadm:    --- Enterprise Controller ha-status command succeeded
Status stored in file: /var/opt/sun/xvm/ha/HAECStatus
#
```

Converting a High Availability Configuration to a Single Enterprise Controller

You can convert your High Availability configuration to a single Enterprise Controller.

1. As root, log on to each standby Enterprise Controller node.
2. On each standby Enterprise Controller node, use the `ecadm` command with the `ha-unconfigure-standby` subcommand to remove the node from the High Availability configuration.

The node is removed from the cluster.

3. As root, log on to the active Enterprise Controller node.
4. Use the `ecadm` command with the `ha-stop-no-relocate` subcommand to stop the active node without bringing up a new node.

The active Enterprise Controller node is stopped.

5. Use the `ecadm` command with the `ha-unconfigure-primary` subcommand to unconfigure the Enterprise Controller as part of a High Availability configuration.

The active Enterprise Controller node is unconfigured as the active node.

6. Use the `ecadm` command with the `start` subcommand to start the active node.

The Enterprise Controller is restarted.

Performing a Manual Relocate

You can manually relocate from the current Enterprise Controller to a standby Enterprise Controller.

1. As root, log in to the active Enterprise Controller node.
2. Use the `ecadm` command with the `ha-relocate` subcommand to switch to a different node. If multiple standby nodes are available, use the `--node <standby node>` option to switch to the specified standby node.

Another node is activated and the current node is switched to standby mode.

Managing HA Network Resources

Oracle Clusterware provides support for one network address known as the Single Client Access Name (SCAN). However, in some deployments, systems must communicate with the Enterprise Controller on a network separate from the SCAN network.

You can add and manage network resources for high availability using the Clusterware `crsctl` command.

For more information about these commands, and information about deleting, starting, stopping, or checking the status of network resources, see the *Oracle Clusterware Administration and Deployment Guide 11g Release 2*.

Adding a Network Resource

You can add a network resource using the `crsctl` command.

To add a network resource, run the `crsctl add resource` command with the following format:

```
/u01/app/11.2.0/grid/bin/crsctl add resource <resource name> -type
application -attr ACTION_SCRIPT=/u01/app/11.2.0/grid/bin/usrvip, USR_ORA_
NETMASK=<netmask>,USR_ORA_VIP=<vip IP address>,USR_ORA_START_
TIMEOUT=0,USR_ORA_STOP_TIMEOUT=0,USR_ORA_STOP_MODE=immediate,USR_ORA_
IF=<network interface>,USR_ORA_OPI=false,USR_ORA_CHECK_TIMEOUT=0,USR_ORA_
DISCONNECT=false,USR_ORA_PRECONNECT=none,HOSTING_MEMBERS=<node1>:<node2>
```

The following options are included in this format:

- `<resource name>`: Specifies the resource name.
- `-type application`
- `USR_ORA_IF=<network interface>`: Specifies the network interface (NIC) for the network resource.
- `USR_ORA_VIP= <ipaddress>`: Specifies the IP address for the network resource.
- `USR_ORA_NETMASK=<netmask>`: Specifies the netmask for the network resource.
- `USR_ORA_IF=<network interface>`: Specifies the network interface (NIC) for the network resource.
- `HOSTING_MEMBERS=<node1>:<node2>`: Specifies the cluster nodes hosting the Enterprise Controller.
- `ACTION_SCRIPT=/u01/app/11.2.0/grid/bin/usrvip`
- `PLACEMENT=favored`

Modifying a Network Resource

You can modify an existing network resource using the `crsctl` command.

To add a network resource, run the `crsctl modify resource` command with the following format:

```
./crsctl modify resource <resource name> -attr <attribute>=<new value>,  
<attribute>=<new value>,...
```

The following attributes can be modified:

- USR_ORA_IF=<network interface>: Specifies the network interface (NIC) for the network resource.
- USR_ORA_VIP= <ipaddress>: Specifies the IP address for the network resource.
- USR_ORA_NETMASK=<netmask>: Specifies the netmask for the network resource.
- USR_ORA_IF=<network interface>: Specifies the network interface (NIC) for the network resource.
- HOSTING_MEMBERS=<node1>:<node2>: Specifies the cluster nodes hosting the Enterprise Controller.
- ACTION_SCRIPT=/u01/app/11.2.0/grid/bin/usrvip
- PLACEMENT=favored

Removing a Standby Enterprise Controller Node

You can remove a standby Enterprise Controller node from the cluster.

1. As root, log on to the standby Enterprise Controller node.
2. Use the `ecadm` command with the `ha-unconfigure-standby` subcommand to remove the node from the High Availability configuration.

The node is removed from the cluster. You can uninstall the Enterprise Controller on the node using the normal Enterprise Controller uninstall procedure.

Checking the Status of the Enterprise Controller Cluster

You can check the status of the cluster from any Enterprise Controller node.

1. As root, log on to an Enterprise Controller node.
2. Use the `ecadm` command with the `ha-status` subcommand and the `-d` option to check the status of the cluster.

The node's status is displayed.

Shutting Down the Enterprise Controller Temporarily Without Relocating

You can stop the active node without making a different node active. The user interface and the command-line interface are unusable while all Enterprise Controller nodes are shut down.

1. As root, log on to the active Enterprise Controller node.
2. Use the `ecadm` command with the `ha-stop-no-relocate` subcommand to stop the active node without bringing up a new node.

The active node is stopped.

3. Use the `ecadm` command with the `ha-start` subcommand to start the active node.

The active node is restarted.

Accessing the Cluster Management UI

You can view the cluster configuration from the user interface.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click **Manage Cluster Configuration** in the Actions pane.

The Cluster Management UI is displayed.

Enabling and Using Proxy Controller High Availability

A specific Proxy Controller manages each asset. If a Proxy Controller fails or is uninstalled, you are notified and given the option to migrate the failed Proxy Controller's assets to another Proxy Controller. Alternatively, you can enable automatic failover, which automatically migrates assets to another Proxy Controller if their current Proxy Controller fails. You can also move an asset from one functional Proxy Controller to another.

To migrate an asset to a new Proxy Controller, the destination Proxy Controller must either be connected to the networks of the assets being moved, or be associated with those networks and have them enabled. The destination Proxy Controller must also be online and reachable.

Enabling Automatic Failover

You can enable automatic failover, which automatically migrates assets to another Proxy Controller if their current Proxy Controller becomes unreachable. The Alert indicating that the Proxy Controller is unreachable triggers the automatic failover.

Before you enable automatic failover, close all existing unreachability incidents on remote Proxy Controllers.

Oracle Enterprise Manager Ops Center cannot migrate assets to a Proxy Controller if it has any alerts indicating that it is unreachable.

Note: Automatic Failover only applies to remote Proxy Controllers. Assets cannot be automatically relocated from a co-located Proxy Controller.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click the **Configuration** tab.
3. Select **Proxy Manager** in the Subsystem drop-down list.
4. Change the value of the AUTO_FAILOVER property to true.
5. Click the **Save Properties** icon.

Automatic Failover is enabled.

Disabling Automatic Failover

You can disable automatic failover to resume manual failover or to prevent failover during a scheduled Proxy Controller outage. Automatic failover is disabled by default.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click the **Configuration** tab.

3. Select **Proxy Manager** in the Subsystem drop-down list.
4. Change the value of the `AUTO_FAILOVER` property to false.
5. Click the **Save Properties** icon.

Automatic Failover is disabled.

Setting the Relative Power for Proxy Controllers

When Oracle Enterprise Manager Ops Center migrates an asset, it targets the available Proxy Controller with the lowest load. You can edit a Proxy Controller's relative power to make it a more or less common target for automatic migration.

The load for each Proxy Controller is determined by the following formula:

$$\text{Load} = (\text{managedResourceCount} + (\text{managedAgentCount} * \text{RELATIVE_CASCADE_WEIGHT})) / \text{PC.RELATIVE_POWER}$$

In this formula, the following variables are used:

- `managedResourceCount` – The number of assets managed by the Proxy Controller.
- `managedAgentCount` – The number of Agent Controllers managed by the Proxy Controller.
- `RELATIVE_CASCADE_WEIGHT` – A relative weight of `managedAgentCount` across all Proxy Controllers.
- `PC.RELATIVE_POWER` – A Proxy Controller-specific variable that specifies the relative power of the Proxy Controller.

You can edit the `PC.RELATIVE_POWER` for a Proxy Controller to make it a more or less common target for automatic migration. Proxy Controllers with a higher Relative Power than other Proxy Controllers are more likely to be targets for automatic migration. You can also edit the `RELATIVE_CASCADE_WEIGHT` to increase or decrease the importance of Agent Controllers in the load calculation; a higher value for this variable increases the importance of Agent Controllers in the load calculation.

1. Click the Enterprise Controller in the Administration section of the Navigation pane.
2. Click the **Configuration** tab.
3. Select **Proxy Manager** in the Subsystem drop-down list.

The Proxy Manager variables are displayed. Two variables are relevant:

- `RELATIVE_CASCADE_WEIGHT` – A relative weight of `managedAgentCount` across all Proxy Controllers. The default value is five.
 - `<PROXY_CONTROLLER>.RELATIVE_POWER` – Each Proxy Controller has a Relative Power variable. The default value is one.
4. (Optional) Edit the value of the `RELATIVE_CASCADE_WEIGHT` property.
 5. Edit the value of the `<PROXY_CONTROLLER>.RELATIVE_POWER` property for the target Proxy Controllers.

Note: You cannot set the `PC.RELATIVE_POWER` value to zero. If it is set to zero or to a non-numeric value, it will be reset to the default of one when a migration job is launched or when automatic failover is enabled.

If you want a Proxy Controller to be temporarily disabled as a target for automatic migration, place the Proxy Controller in maintenance mode as described in the *Infrastructure* chapter.

6. Click the **Save Properties** icon.

Recovering After an Automatic Failover

An automatic failover can require some cleanup actions. Depending on the circumstances of the failover, access points for failed or old Proxy Controllers can remain on some assets. These access points do not cause any known issues, but can cause confusion for users.

If an automatic failover occurs and the failed Proxy Controller is permanently unavailable, unconfigure and delete the Proxy Controller. See [Removing a Proxy Controller from the User Interface](#) for more information.

If an automatic failover occurs and the failed Proxy Controller is restarted, manually migrate the assets to the desired Proxy Controllers. Then view the access points for each asset. If an asset has an access point for an incorrect Proxy Controller, delete that access point. See the [Asset Management](#) chapter of the *Feature Reference Guide* for more information about deleting access points.

Migrating Assets Between Proxy Controllers

You can migrate an asset from one functional Proxy Controller to another to balance job load or if you intend to uninstall a Proxy Controller.

1. Select the source Proxy Controller in the Administration section of the Navigation pane.
2. Click the **Managed Assets** tab.
3. Select one or more assets to move, then click the **Migrate Assets** icon.

If another Proxy Controller is available that can manage the assets, the Asset Migration Wizard is displayed.

If no other Proxy Controller is available that can manage the assets, an error message is displayed.

4. Within the Asset Migration Wizard, the selected assets are displayed in groups which can be migrated together. Select one or more groups, then select the destination Proxy Controller from the list of Proxy Controllers, or select **Auto Balance across Proxies** to automatically select a destination Proxy Controller.
5. Click **Migrate**.

A job is launched to migrate the selected assets to the destination Proxy Controller. The migration status is displayed in the job and in the Managed Assets tab.

Migrating Assets from a Failed Proxy Controller

If a Proxy Controller fails, Oracle Enterprise Manager Ops Center sends an alert giving you the option of migrating assets from the failed Proxy Controller to another Proxy Controller.

If you expect the Proxy Controller to come back online, leave the assets under its management. However, if you expect the Proxy Controller not to come back online, you can migrate them to another available Proxy Controller. This action also removes the Proxy Controller.

For a Proxy Controller to serve as a destination for an asset migration, the asset must be connected to a network that can be accessed by the Proxy Controller. If no other Proxy Controller can reach an asset, it cannot be migrated.

1. Open the alert indicating that a Proxy Controller has failed.
2. Click **Migrate Assets**.

If another Proxy Controller is available that can manage the assets, the Asset Migration Wizard is displayed.

If no other Proxy Controller is available that can manage the assets, an error message is displayed.

3. Within the Asset Migration Wizard, the selected assets are displayed in groups which can be migrated together. Select one or more groups, then select the destination Proxy Controller from the list of Proxy Controllers, or select **Auto Balance across Proxies** to automatically select a destination Proxy Controller.
4. Click **Migrate**.

A job is launched to migrate the selected assets to the destination Proxy Controller. The migration status is displayed in the job and in the Managed Assets tab.

You can upgrade to the latest version of Oracle Enterprise Manager Ops Center 12c if you are currently using Oracle Enterprise Manager Ops Center 12c.

Introduction to Upgrading

You can upgrade to the latest version of Oracle Enterprise Manager Ops Center from Oracle Enterprise Manager Ops Center 12c.

Some of the procedures described in this section use the `ecadm`, `proxyadm`, and `agentadm` commands. See [Appendix A, "Command Line Administration"](#) for more information about these commands.

- On Oracle Solaris systems, these commands are in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, these commands are in the `/opt/sun/xvmoc/bin/` directory.

Versions Supported for Upgrade

This section details the supported upgrade paths. Before planning your upgrade, read this section carefully, as you may need to perform multiple upgrades to reach the latest version.

Upgrading From Version 12.2

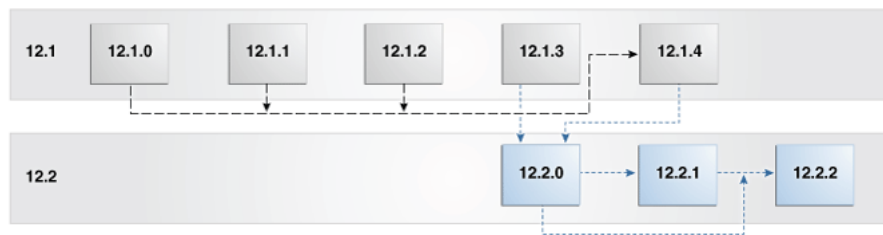
If you are currently using version 12.2.0 or 12.2.1, you can upgrade directly to any later version.

Figure 10–1 Supported Upgrade Paths From Version 12.2



Upgrading From Version 12.1

If you are currently using Oracle Enterprise Manager Ops Center version 12.1, you can upgrade to version 12.1.3 or 12.1.4, then upgrade to version 12.2.0, and finally upgrade to the latest version.

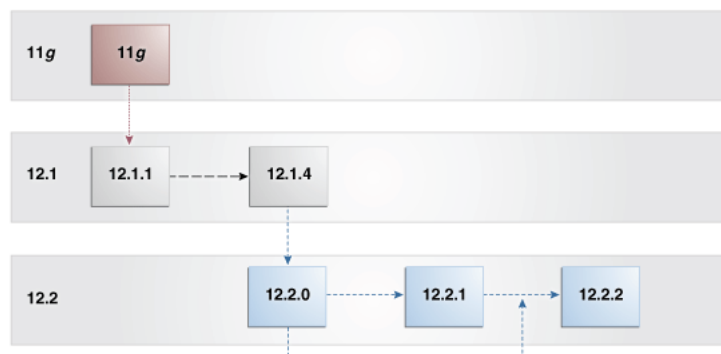
Figure 10–2 Supported Upgrade Paths From Version 12.1

You must upgrade in this order:

1. If you are using version 12.1.0, 12.1.1, or 12.1.2, upgrade to version 12.1.4.0.0 as described in the *Version 12.1 Administration Guide*.
2. Upgrade to version 12.2.0.0.0 as described in this guide.
3. Upgrade to version 12.2.1.0.0 or version 12.2.2.0.0 as described in this guide.

Upgrading From Version 11g

If you are currently using Oracle Enterprise Manager Ops Center 11g, you can upgrade to version 12.1.1, then upgrade to version 12.1.4, then upgrade to version 12.2.0, and finally upgrade to the latest version.

Figure 10–3 Supported Upgrade Paths From Version 11g

You must upgrade in this order:

1. Upgrade to version 12.1.1.0.0 as described in the *Version 12.1 Administration Guide*.
2. Upgrade to version 12.1.4.0.0 as described in the *Version 12.1 Administration Guide*.
3. Upgrade to version 12.2.0.0.0 as described in this guide.
4. Upgrade to version 12.2.1.0.0 or version 12.2.2.0.0 as described in this guide.

Planning The Upgrade

Upgrading to a newer version of Oracle Enterprise Manager Ops Center can change the system requirements and affect existing settings and data. Take the following steps to plan your upgrade:

- Review the *Oracle Enterprise Manager Ops Center Release Notes* for pre-installation requirements and known issues.

- Verify that your system meets the system requirements outlined in the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System* or *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*, since some system requirements have changed.

You can use the OCDoctor to check system requirements. See

<http://java.net/projects/oc-doctor> for more information about the OCDoctor.

- If you made changes to the `uce.rc` file, the upgrade erases your changes. Copy your changes to the `.uce.rc` file before beginning the upgrade.
- If you replaced the self-signed web server certificate for the Enterprise Controller, the upgrade erases your web server configuration changes, and might erase the certificate. Copy the certificate to a safe location before beginning the upgrade. After the upgrade, reapply your configuration changes and copy the certificate to its original location.

Note: Due to improvements to vServer management, Oracle VM Server for SPARC vServer templates from version 12.1.4.0.0 or earlier will not function in version 12.2.0.0.0 and must be recreated. In addition, a user with the Cloud Administrator role must configure at least one vNet as a boot network before creating any new vServers. See the Virtual Datacenters chapter of the *Feature Reference Guide* for more information.

Note: If your Enterprise Controller is installed on Oracle Solaris 11, your Oracle Solaris 11 repository must contain the specific version of Oracle Solaris 11 installed on the Enterprise Controller before you begin the upgrade.

Database Requirements

Oracle Enterprise Manager Ops Center version 12c can use either an embedded database on the Enterprise Controller system or a customer-managed database. You cannot change the existing database configuration during the upgrade.

The embedded database is configured and managed by Oracle Enterprise Manager Ops Center. The embedded database requires 10 GB of space, plus 240 MB per managed asset, 400 MB per UCE channel, and 20% of the space currently taken up by the `/var/opt/sun/xvm/db/management` and `var/opt/sun/xvm/db/report` directories.

You must install and configure a compatible database to use a customer-managed database. Using a customer-managed database requires no additional space beyond that required by the Enterprise Controller.

Upgrading Your Environment

The *Oracle Enterprise Manager Ops Center Upgrade Guide* includes upgrade procedures for a variety of environments. Several factors will determine the procedure that is most appropriate for your environment. [Table 10-1, "Upgrade Procedures by Environment and Upgrade Choices"](#) shows the relevant chapter for you based on your environment and your preferences for the upgrade. Each chapter is a complete upgrade procedure.

Environments with a single Enterprise Controller use a separate procedure from environments with Enterprise Controller High Availability.

You can perform upgrades through the user interface or from the command line.

Table 10–1 Upgrade Procedures by Environment and Upgrade Choices

Enterprise Controller High Availability?	User Interface or Command Line?	Chapter
Yes	User Interface	Chapter 2, Upgrading an HA Environment Using the User Interface
Yes	Command Line	Chapter 3, Upgrading an HA Environment Using the Command Line
No	User Interface	Chapter 4, Upgrading a Single EC Environment Using the User Interface
No	Command Line	Chapter 5, Upgrading a Single EC Environment Using the Command Line

Uninstalling and Unconfiguring

These procedures describe unconfiguring and uninstalling the Agent Controller, Proxy Controller, and Enterprise Controller components of Oracle Enterprise Manager Ops Center.

Check with Oracle Support for any additional scripts that might be available to ensure a clean removal of Enterprise Controller or Proxy Controller software.

The following features and topics are covered in this chapter:

- [Introduction to Uninstalling and Unconfiguring](#)
- [Uninstalling and Unconfiguring Agent Controllers](#)
- [Uninstalling and Unconfiguring a Proxy Controller](#)
- [Uninstalling and Unconfiguring the Enterprise Controller](#)

Introduction to Uninstalling and Unconfiguring

This section explains how to uninstall and unconfigure the Oracle Enterprise Manager Ops Center infrastructure.

Some of the procedures described in this section use the `ecadm`, `proxyadm`, and `agentadm` commands. See [Appendix A, "Command Line Administration"](#) for more information about these commands.

- On Oracle Solaris systems, these commands are in the `/opt/SUNWxvmoc/bin/` directory.
- On Linux systems, these commands are in the `/opt/sun/xvmoc/bin/` directory.

Uninstalling and Unconfiguring Agent Controllers

You can uninstall and unconfigure Agent Controllers to remove them from Oracle Enterprise Manager Ops Center. This also removes the assets managed by the Agent Controllers from Oracle Enterprise Manager Ops Center.

Uninstalling and Unconfiguring Agent Controllers from the User Interface

You can uninstall and unconfigure Agent Controllers from the user interface.

Note: If you unconfigure and reconfigure an Agent Controller on an LDOM Control Domain, many LDOM management functions cease to function.

1. Select **Assets** from the Navigation pane.
2. In the All Assets pane, click the **Managed Assets** tab.
The list of currently managed assets are displayed in the Managed Assets section.
3. From the Managed Assets list, select the managed OS instance from which you want to remove the Agent Controller.
4. Click the **Delete Assets** icon (X icon placed above the list header).
The Management Credentials page of the Unmanage Assets Wizard is displayed.
5. Provide a set of credentials to access the Agent Controller, then click **Next**.
 - **New:** Click New to create a new set of credentials.
Enter a name and the credential information, then click Ok.
 - **Select:** Click Select to select an existing set of credentials.
Select a set of credentials from the list, then click Ok.The Summary page is displayed.
6. Click **Finish**.
A job is launched to uninstall and unconfigure the Agent Controllers.

Uninstalling and Unconfiguring Agent Controllers from the Command Line

You can uninstall and unconfigure Agent Controllers from the command line.

Caution: Do not uninstall co-located Agent Controllers from an Enterprise Controller or Proxy Controller system. Uninstalling a co-located Agent Controller can corrupt Enterprise Controller or Proxy Controller services.

1. From the command line, log in to the Agent Controller system.
2. Use the `agentadm` command with the `stop` subcommand to stop the Agent Controller.

```
# ./agentadm stop
```
3. Use the `agentadm` command with the `unconfigure` subcommand to unconfigure the Agent Controller. If the Agent Controller is installed on an Oracle VM Server for SPARC, confirmation text is displayed.

```
# ./agentadm unconfigure
Unconfiguring an Agent Controller in a Control Domain will delete the current
configuration.
This action cannot be undone.

Do you really want to continue (y/N) ?
```

If the confirmation text is displayed, enter `y` to continue.

The Agent Controller is now unconfigured from the Enterprise Controller.
4. Use the `/var/scn/install/uninstall` command to uninstall the Agent Controller.

Uninstalling and Unconfiguring a Proxy Controller

Unconfiguring and uninstalling a Proxy Controller breaks its connection with the Enterprise Controller and removes the Proxy Controller software. All Assets discovered or managed by the Proxy Controller are also removed. The Agent Controllers installed on systems managed by the Proxy Controller are not removed.

Three methods are available for unconfiguring and uninstalling a Proxy Controller. The first two options are performed through the user interface.

- Unconfigure and Uninstall the Proxy Controller from the user interface. This option connects to the Proxy Controller through SSH, then commands it to unconfigure and uninstall itself. You can only take this action if the Proxy Controller is reachable.
- Remove the Proxy Controller from Oracle Enterprise Manager Ops Center. This option removes the Proxy Controller from the Oracle Enterprise Manager Ops Center infrastructure, but does not uninstall the Proxy Controller. You can remove a Proxy Controller even if it is unreachable. You can uninstall the Proxy Controller from the command line once it has been removed.
- Unconfigure the Proxy Controller from the command line. The Proxy Controller software must then be uninstalled from the command line.

Unconfiguring and Uninstalling a Proxy Controller from the User Interface

You can unconfigure and uninstall Proxy Controllers from the user interface.

1. Click a Proxy Controller in the Administration section of the Navigation pane.
2. Click **Unconfig/uninstall Proxy** in the Actions pane.

The Unconfigure/Uninstall Proxy Controller window is displayed.

3. If the Proxy Controller is currently managing assets, click **Migrate Assets** to migrate the assets to another Proxy Controller. Select another Proxy Controller and click **Migrate**.
4. Select **Send Job to Remote Proxy**.
5. Enter the privileged user name and password for the Proxy Controller. If root login is not permitted on the Proxy Controller system, enter a non-root user name and password followed by the root user name and password.
6. Click **Unconfigure/Unregister**. The Proxy Controller is removed from Oracle Enterprise Manager Ops Center.

Removing a Proxy Controller from the User Interface

You can remove an unreachable Proxy Controller from the infrastructure using the user interface. This action prevents the Proxy Controller from being used by Oracle Enterprise Manager Ops Center, but it does not uninstall the Proxy Controller.

1. Click a Proxy Controller in the Administration section of the Navigation pane.
2. Click **Unconfig/uninstall Proxy** in the Actions pane.

The Unconfigure/Uninstall Proxy Controller window is displayed.

3. Select **Force the Removal of the Proxy Controller from Oracle Enterprise Manager Ops Center**.
4. Click **Unconfigure/Unregister**.

Unconfiguring a Proxy Controller from the Command Line

Unconfiguring a Proxy Controller breaks its connection with the Enterprise Controller.

1. From the command line, log in to the Proxy Controller.
2. Use the `proxyadm` command with the `stop` subcommand and the `-w` option to stop the Proxy Controller.

For example:

```
# ./proxyadm stop -w
proxyadm: Shutting down Proxy Controller using SMF...
proxyadm: Proxy Controller services have stopped
```

3. Use the `proxyadm` command with the `unconfigure` subcommand to unconfigure the Proxy Controller.

The following options may be used:

- `-s` | `--satellite`: Unregisters the Proxy Controller from the Enterprise Controller.
- `-k` | `--keep`: Do not clear the local Proxy Controller database.

The example below uses the `-s` option to unregister the Proxy Controller from the Enterprise Controller.

```
# ./proxyadm unconfigure -s
```

The Proxy Controller is now unconfigured from the Enterprise Controller.

Uninstalling a Proxy Controller from the Command Line

Uninstalling a Proxy Controller removes the Proxy Controller software and all Oracle Enterprise Manager Ops Center data. All Assets discovered or managed by the Proxy Controller are removed as well. The Agent Controllers installed on systems managed by the Proxy Controller are not removed.

You can uninstall a Proxy Controller from the command line. This may be necessary if the Proxy Controller is not responding to remote commands.

Note: The co-located Proxy Controller that is installed with the Enterprise Controller cannot be uninstalled without uninstalling the Enterprise Controller.

1. Use the `proxyadm` command with the `stop` subcommand and the `-w` option to stop the Proxy Controller services.

The following options may be used:

- `-l` | `--logfile <log file>`: Saves the output from the command in `<logfile>`.
- `-v` | `--verbose`: Increase verbosity level (may be repeated).

For example:

```
# ./proxyadm stop -w
```

2. Use the `/nlgc-setup/installer/install` command with the `-e` option to uninstall the Proxy Controller software components from your system. For example:

```
# cd /nlgc-setup/installer
```



```
# ./install -e
Invoking uninstall
```

The install script displays a list of uninstallation tasks that automatically updates as the uninstallation proceeds. For example:

```
Ops Center Proxy Controller Uninstall
(version 12.2.2.610 on SunOS)

1. Restore file system configuration. [Not Uninstalled]
2. Uninstall Expect. [Not Uninstalled]
3. Uninstall IPMI tool. [Not Uninstalled]
4. Uninstall Agent components. [Not Uninstalled]
5. Uninstall application packages. [Not Uninstalled]
6. Uninstall Core Channel components. [Not Uninstalled]
7. Uninstall Proxy Core components. [Not Uninstalled]
8. Uninstall UCE Http proxy. [Not Uninstalled]
9. Uninstall OS provisioning components. [Not Uninstalled]
10. Stop and delete services. [Uninstalled]
(1 of 10 Uninstalled)

Executing current step: Uninstall OS provisioning components...

When complete, the install script indicates that the Proxy Controller has been
uninstalled.
```

Uninstalling and Unconfiguring the Enterprise Controller

Unconfiguring an Enterprise Controller removes user, authentication, and configuration data and unregisters the Enterprise Controller from Oracle. Data about Proxy Controllers and managed systems is retained. If you unconfigure your Enterprise Controller, you must reconfigure it before using Oracle Enterprise Manager Ops Center.

Uninstalling the Enterprise Controller removes the Enterprise Controller software and all Oracle Enterprise Manager Ops Center data.

Unconfiguring the Enterprise Controller

You can unconfigure an Enterprise Controller to reconfigure it or as a precursor to uninstalling.

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.
2. Click **Unconfigure** in the Actions pane.
A confirmation page is displayed.
3. Click **Unconfigure**.
The Enterprise Controller is unconfigured.

Uninstalling the Enterprise Controller

You can uninstall the Enterprise Controller. This removes the Enterprise Controller software and all Oracle Enterprise Manager Ops Center data.

Note: Uninstalling the Enterprise Controller does not uninstall a customer-managed database or remove the Oracle Enterprise Manager Ops Center schema.

1. If the Enterprise Controller is part of an HA configuration and is currently the active node, use the `ecadm ha-relocate` command to make another node active if another node is available.
2. If the Enterprise Controller is part of an HA configuration and another node is the primary, use the `ecadm ha-unconfigure-standby` command to remove the current node from the HA configuration.
3. Use the `ecadm` command with the `stop` subcommand and the `-w` option to stop the Enterprise Controller services.

For example:

```
# ./ecadm stop -w
ecadm: Shutting down satellite using SMF...
#
```

4. Use the `/nlgc-setup/installer/install` command with the `-e` option to uninstall the Enterprise Controller software components from your system.

For example:

```
# cd /nlgc-setup/installer/
# ./install -e
Invoking uninstall
```

The install script displays a list of uninstallation tasks that automatically updates as the uninstallation proceeds. For example:

```
Ops Center Enterprise Controller Uninstall
(version 12.2.2.610 on SunOS)

1. Restore file system configuration. [Not Uninstalled]
2. Uninstall empty directories. [Not Uninstalled]
3. Uninstall prerequisite configuration. [Not Uninstalled]
4. Uninstall Agent components. [Not Uninstalled]
5. Remove Deployable Proxy Bundles. [Not Uninstalled]
6. Uninstall application packages. [Not Uninstalled]
7. Run preremove tasks. [Not Uninstalled]
8. Uninstall Expect. [Not Uninstalled]
9. Uninstall IPMI tool. [Not Uninstalled]
10. Remove database credentials. [Not Uninstalled]
11. Uninstall Oracle database. [Not Uninstalled]
12. Remove OC Database Schema [Not Uninstalled]
13. Uninstall Service container components. [Not Uninstalled]
14. Uninstall Core Channel components. [Not Uninstalled]
15. Uninstall Proxy Core components. [Not Uninstalled]
16. Remove Proxy database credentials. [Not Uninstalled]
17. Uninstall Enterprise Controller components. [Not Uninstalled]
18. Uninstall Update Connection - Enterprise. [Not Uninstalled]
19. Uninstall Ops Center BUI components. [Not Uninstalled]
20. Uninstall OS provisioning components. [Not Uninstalled]
21. Stop and delete services. [Not Uninstalled]
Executing current step: Stop and delete services...
```

When complete, the install script indicates that the Enterprise Controller has been uninstalled.

Command Line Administration

This chapter explains how to manage the Oracle Enterprise Manager Ops Center Enterprise Controller, Proxy Controller, and Agent Controller from the command line.

The following information is included:

- [Configuring the Enterprise Controller: ecadm](#)
- [Configuring the Proxy Controller: proxyadm](#)
- [Configuring the Agent Controller: agentadm](#)

Configuring the Enterprise Controller: ecadm

The `ecadm` command helps to configure, unconfigure, and perform administrative tasks on the Oracle Enterprise Manager Ops Center Enterprise Controller.

Synopsis

Oracle Solaris OS

```
/opt/SUNWxvmoc/bin/ecadm -V  
/opt/SUNWxvmoc/bin/ecadm [ -h | --help ]  
/opt/SUNWxvmoc/bin/ecadm subcommand [ options ]
```

Linux OS

```
/opt/sun/xvmoc/bin/ecadm -V  
/opt/sun/xvmoc/bin/ecadm [ -h | --help ]  
/opt/sun/xvmoc/bin/ecadm subcommand [ options ]
```

Options

The following common options are supported:

- h | --help: Displays the usage synopsis for `ecadm`.
- V | --version: Displays the version of Oracle Enterprise Manager Ops Center.

Subcommands

The subcommands of `ecadm` are as follows:

start

Starts the Enterprise Controller services running on the host.

stop

Stops the Enterprise Controller services running on the host.

status

Displays the status of the Enterprise Controller services. Displays either online or offline to the standard output and sets the exit status to reflect the Enterprise Controller service state.

configure

Performs configuration tasks for the Enterprise Controller services. Registers the Enterprise Controller with My Oracle Support.

unconfigure

Performs the inverse operation of configuring the Enterprise Controller. Deregisters the Enterprise Controller.

backup

Creates a backup archive of the state data of the Enterprise Controller. This command does not back up any installed software.

restore

Restores the state data of an Enterprise Controller from a backup archive. If a new system is being used, the system must have the same host name as the original Enterprise Controller. After the successful completion of this command, the Enterprise Controller is in the same operational state that existed at the time of the backup.

If the registration of the Enterprise Controller to My Oracle Support is invalidated with the `ecadm unconfigure` command, any backup archives created during the time the Enterprise Controller was registered become unusable. The Enterprise Controller is no longer able to communicate with My Oracle Support, and the asset data shared between the Enterprise Controller and the hosted servers lose their synchronization.

verify-db

Verifies that the database used for the Enterprise Controller data persistence is available, reachable, and the schemas are set up with the proper permissions.

change-db-password

Changes the Enterprise Controller password for the application or read only database schema that is used by Oracle Enterprise Manager Ops Center database password for the local or remote database. The Enterprise Controller services are restarted after using this command.

defrag-db

Defragments the embedded database to increase free space and improve performance.

maintenance

Changes the state of the database to maintenance state.

migrate

Moves Enterprise Controller data persistence from a local database to a customer-managed database, then removes the local database and the local database server binaries from the Enterprise Controller. The database must be installed in the destination location before beginning this procedure. The Enterprise Controller is shutdown and is restarted on successful completion.

sqlplus

Opens a sqlplus console to the underlying database.

ha-status

Checks the status of the Oracle Clusterware Enterprise Controller resource.

ha-configure-primary

Configures the system as the primary Enterprise Controller in an Oracle Clusterware framework.

ha-configure-standby

Configures the system as a standby Enterprise Controller in an Oracle Clusterware framework.

ha-modify-resource

Modifies the Enterprise Controller Clusterware resource attributes. To modify the Clusterware resource attributes, edit the `/var/opt/sun/xvm/ha/EnterpriseController_HA_clusterware.properties` file with the appropriate changes, and run this command to take effect.

ha-relocate

Switches from the currently active Enterprise Controller node to a different node.

ha-start

Starts the Enterprise Controller Clusterware resource on one of the Clusterware nodes. Starting the Enterprise Controller Clusterware resource causes the Enterprise Controller services to start.

ha-stop-no-relocate

Stops the Enterprise Controller Clusterware resource. Stopping the Enterprise Controller resource causes the currently active node hosting the Enterprise Controller services to be stopped.

ha-unconfigure-primary

Removes the last node hosting the Enterprise Controller in an Oracle Clusterware framework.

ha-unconfigure-standby

Removes a Enterprise Controller node from the Oracle Clusterware framework.

Subcommand options

Common options for all subcommands:

- h | --help: Displays the usage synopsis for the subcommand.
- v | --verbose: Displays verbose error and informational messages.
- l | --logfile <logfile>: Captures any output from ecadm in the <logfile>.

start

Enter `ecadm start [-h | --help] [-v | --verbose] [-c | --cluster] [-t | --temporary] [-w | --wait] [-l | --logfile <logfile>]`.

-c | --cluster: Cluster environment.

-w | --wait: ecadm does not exit until all services have been started.

-t | --temporary: The state change is made temporary until next reboot.

stop

Enter `ecadm stop [-h | --help] [-v | --verbose] [-c | --cluster] [-t | --temporary] [-w | --wait] [-l | --logfile <logfile>]`.

-c|--cluster: Cluster environment.

-w|--wait: ecadm does not exit until all services have been stopped.

-t|--temporary: The state change is made temporary until next reboot.

status

Enter `ecadm status [-h | --help]`.

configure

Enter `ecadm configure [-h | --help] [-f | --config <config-file>] [-p | --proxy] [-P | --noproxy] [-v | --verbose] [-l | --logfile <logfile>]`.

-f|--config <config-file>: Uses the contents of <config-file> to register the Proxy Controller with My Oracle Support.

-p|--proxy: By default, enables the local Proxy Controller after the Enterprise Controller is configured.

-P|--noproxy: The local control proxy is not enabled.

Note: Ensure that the file permission for the configuration file properties is set to 400 because it contains the Online Account user name and password. The configuration file must not be accessible to unauthorized users.

unconfigure

Enter `ecadm unconfigure [-h | --help] [-v | --verbose] [-l | --logfile <logfile>]`.

backup

Enter `ecadm backup [-o | --output <backup-file>] [-t | --tag <tag>] [-d | --description <description>] [-r | --remotedb] [-c | --configdir <config-dir>] [-T | --tempdir <temp-dir>] [-h | --help] [-v | --verbose] [-l | --logfile <logfile>]`.

-o|--output <backup-file>: Stores the backup archive in tar format in <backup-file>. Do not specify the path inside the xvm install directories (/opt/*xvm*). Default: /var/tmp/sat-backup-<date>-<time>.tar

-t|--tag <tag>: Stores the string <tag> as a property of the backup archive which is displayed by restore operation when referencing the <backup-file>.

-d|--description <description>: Stores the string <description> as a descriptive property of the backup archive (the description is informational and it is displayed during restore operation).

-r|--remotedb: If Enterprise Controller uses a remote database, export the schema to a file on the database server. This option must be specified if the Enterprise Controller uses a remote database, otherwise data is not exported from the database.

-c|--configdir <config-dir>: <config-dir> is an alternative collection of backup modules when performing the backup. ecadm backup is modular in design and executes a set of backup tasks in the configuration directory. This option provides a means to use an alternate set of modules to produce a backup archive in a specialized way.

-T | --tempdir <temp-dir>: Uses <temp-dir> instead of the temporary directory in /var/tmp for intermediate storage needs during the backup. This temporary directory is required to hold a large quantity of data during the backup operation.

restore

Enter `ecadm restore -i | --input <backup-file> [-c | --configdir <config-dir>] [-r | --remotedb] [-d | --tempdir <temp-dir>] [-h | --help] [-v | --verbose] [-l | --logfile <logfile>] .`

-i | --input <backup-file>: Restores state data from <backup-file> which is the archive created by the `ecadm backup` operation. This parameter is required.

-r | --remotedb: If EC uses a remote database, export the schema to a file on the database server. This option must be specified if the Enterprise Controller uses a remote database, otherwise data is not exported from the database.

-c | --configdir <config-dir>: <config-dir> is an alternative collection of restore modules when performing the backup. `ecadm restore` is modular in design and executes a set of restore tasks in the configuration directory. This option provides a means to use an alternate set of modules to restore a backup archive in a specialized way.

-d | --tempdir <temp-dir>: Uses <temp-dir> instead of the temporary directory in /var/tmp for intermediate storage needs during the restore. This temporary directory is required to hold a large quantity of data during the restore operation.

verify-db

Enter `ecadm verify-db [-v | --verbose] .`

change-db-password

Enter `ecadm change-db-password -p | --passwordfile <password-file> [-v | --verbose] .`

-p | --password-file <password-file>: Specifies the file containing the new password.

-r | --as_read_only_user: Specifies if the operation is done for a read only user. If this option is used, the password for the read only user is specified in the <password file>, and the read only user is the target of the change.

defrag-db

Enter `ecadm defrag-db [-T | --tempdir <temporary directory>] .`

-T | --tempdir <temporary directory>: Specifies a different temporary directory to use for the defragmentation.

maintenance

Enter `ecadm maintenance [-h | --help] [-v | --verbose] [-c | --cluster] [-r | --reason <reason-file>] [-t | --temporary] [-w | --wait] [-l | --logfile <logfile>] .`

-c | --cluster: Cluster environment.

-r | --reason <reason-file>: Record reason for shutdown from message in <reason-file>.

-w | --wait: `ecadm` does not exit until all services have been stopped.

-t | --temporary: The state change is made temporary until next reboot.

migrate

Enter `ecadm migrate -r | --remoteDBprops <credentials-file> [-h | --help] [-v | --verbose] [-l | --logfile <logfile>]`.

`-r | --remoteDBprops <credentials-file>`: Specify the file containing credentials and url for the target database.

sqlplus

Enter `ecadm sqlplus [-h | --help] [-r | --as_read_only_user] [-c | --command] [-f | --filedbprop <db.properties file>] [-p | --propfile <dbpw.properties file>] [-d | --directory <directory to run in>]`.

`-r | --as_read_only_user`: Logs into the database as the read only user.

`-c | --command`: Reads the input stream commands that are passed to sqlplus.

`-f | --filedbprop <db.properties file>`: Contains the properties to get the schema name and database URL to set the database properties. The default location of `db.properties` file is `/var/opt/sun/xvm/db.properties`

`-p | --propfile <dbpw.properties file>`: Contains the passwords for the schema names in `db.properties`. The `dbpw.properties` file is found by default in `/var/opt/sun/xvm/dbpw.properties`

`-d | --directory <directory to run in>`: Uses the directory passed in as the working directory for the sqlplus session.

ha-status

Enter `ecadm ha-status [-h | --help] [-v | --verbose] [-d | --display] [-l | --logfile <logfile>]`.

`-d | --as_read_only_user`: Displays full High Availability status info.

ha-configure-primary

Enter `ecadm ha-configure-primary [-h | --help] [-v | --verbose] [-l | --logfile <logfile>]`.

ha-configure-standby

Enter `ecadm ha-configure-standby [-h | --help] [-p | --credentialsfilename <credentials-file>] [-v | --verbose] [-l | --logfile <logfile>]`.

`-p | --credentialsfilename<credentials-file>`: Specifies the file containing the user name and password for privileged access. The first line of the file must contain the user name in this format: `username=<user>`. The second line of the file must contain the password in this format: `password=<password>`.

ha-modify-resource

Enter `ecadm ha-modify-resource [-h | --help] [-p | --credentialsfilename <credentials-file>] [-v | --verbose] [-l | --logfile <logfile>]`.

`-p | --credentialsfilename <credentials-file>`: Specifies the file containing the user name and password for privileged access. The first line of the file must contain the user name in this format: `username=<user>`. The second line of the file must contain the password in this format: `password=<password>`.

ha-relocate

Enter `ecadm ha-relocate [-h | --help] [-n | --node <standby node>] [-v | --verbose] [-l | --logfile <logfile>]`.

`-n | --node <standby node>`: Relocates to node in `<standby node>`.

ha-start

Enter `ecadm ha-start [-h | --help] [-n | --node <standby node>] [-v | --verbose] [-l | --logfile <logfile>]`.

`-n | --node <standby node>`: Relocates to node in <standby node>.

ha-stop-no-relocate

Enter `ecadm ha-stop-no-relocate [-h | --help] [-v | --verbose] [-l | --logfile <logfile>]`.

ha-unconfigure-primary

Enter `ecadm ha-unconfigure-primary [-h | --help] [-v | --verbose] [-l | --logfile <logfile>]`.

ha-unconfigure-standby

Enter `ecadm ha-unconfigure-standby [-h | --help] [-n | --node <standby node>] [-v | --verbose] [-l | --logfile <logfile>]`.

`-n | --node <standby node>`: Unconfigures the standby node when run from another cluster node. Use this option when the standby node is down.

Exit status

The exit status displays the status of the Enterprise Controller services. The status currently displays either offline or online to the standard output. The exit status displays one of the following codes:

0: Online

2: Offline (only for status subcommand)

1: Error occurred during processing

Configuring the Proxy Controller: proxyadm

The `proxyadm` command helps to start, stop, configure and unconfigure the Oracle Enterprise Manager Ops Center Proxy Controller services.

Synopsis**Oracle Solaris OS**

```
/opt/SUNWxvmoc/bin/proxyadm -V
/opt/SUNWxvmoc/bin/proxyadm [ -h | --help ]
/opt/SUNWxvmoc/bin/proxyadm subcommand [ options ]
```

Linux OS

```
/opt/sun/xvmoc/bin/proxyadm -V
/opt/sun/xvmoc/bin/proxyadm [ -h | --help ]
/opt/sun/xvmoc/bin/proxyadm subcommand [ options ]
```

Options

The `proxyadm` command supports the following options:

`-h | --help`: Displays the usage synopsis for `proxyadm`.

`-v`: Displays the version of Oracle Enterprise Manager Ops Center.

Subcommands

The `proxyadm` command includes the following subcommands:

start

Starts the Proxy Controller services running on the host.

stop

Stops the Proxy Controller services running on the host.

status

Displays the online or offline status of the Proxy Controller services to the standard output, and sets the exit status to reflect the Proxy Controller service state.

configure

Performs configuration tasks for the Proxy Controller services.

You can set the following classes of configuration information:

- Registering the Proxy Controller with the Enterprise Controller.
- Configuring the type of DHCP server that the Proxy Controller runs and the parameters for that DHCP server.

unconfigure

Performs the inverse operation of configuring the Proxy Controller. Deregisters and unconfigures the connection between the Proxy Controller and the Enterprise Controller it is associated with.

Subcommand options

The following common options are supported for all the subcommands:

`-h` | `--help`: Displays the usage synopsis for that subcommand.

`-v` | `--verbose`: Displays verbose error and informational messages.

start

Enter `proxyadm start [-h | --help] [-v | --verbose] [-w | --wait] [-t | --temporary] [-l | --logfile <logfile>]`.

`-w` | `--wait`: `proxyadm` does not exit until all the services are started.

`-l` | `--logfile <logfile>`: Captures any output from `proxyadm` in the logfile.

`-t` | `--temporary`: The state change is made temporary until next reboot.

stop

Enter `proxyadm stop [-h | --help] [-v | --verbose] [-w | --wait] [-t | --temporary] [-l | --logfile <logfile>]`.

`-w` | `--wait`: `proxyadm` does not exit until all the services are stopped.

`-l` | `--logfile <logfile>`: Captures any output from `proxyadm` in the logfile.

`-t` | `--temporary`: The state change is made temporary until next reboot.

status

Enter `proxyadm status [-h | --help]`.

configure

Enter `proxyadm configure [-h | --help] [-v | --verbose] [-a | --proxy-ip] [-u | --user <user name>] [-p | --passwordfile] [-t |`

```
--tokenfile <password-file> ] [ -x | --proxy <host name>[:<port>] ] [ -U |
--proxy-user <proxy user name> ] [ -P | --proxy-passwordfile
<password-file> ] [ -a | --proxy-ip ].
```

-s | --satellite <Enterprise Controller>: Specifies the Enterprise Controller with which to register the Proxy Controller. Requires the -u and -p options.

-u | --user <user name>: Specifies the Enterprise Controller administrator user name.

-p | --passwordfile <passwordfile>: Specifies a filename containing the password for the Enterprise Controller administrator.

(Optional) -t | --tokenfile <autoregistration_tokenfile>: Specifies an autoregistration token stored in a file. This is used as an alternative for Enterprise Controller administrator user name and password.

(Optional) -x | --proxy <host name>[:<port>]: If an HTTPS proxy is required to reach the Enterprise Controller, specify the <host name> for that proxy. Specifying the IP port is optional. The default proxy port is 8080.

(Optional) -U | --proxy-user <proxy user name>: Use this option if a proxy requires a user name for authentication.

(Optional) -P | --proxy-passwordfile <password-file>: Uses the password in <password-file> for proxy authentication.

(Optional) -a | --proxy-ip: Explicitly enter the IP address of the control proxy.

Note: The password file must be secured to prevent unauthorized users from examining the file. The file permission must be set to 400.

unconfigure

```
Enter proxyadm unconfigure [ -h | --help ] [ -k | --keep ].
```

-k | --keep: Keeps the local Proxy Controller database.

Exit status

The exit status displays the status of the proxy services. The states currently display either offline or online on the standard output. The exit status displays one of the following codes:

0: Online

2: Offline (only for status subcommand)

1: Error occurred during processing

Configuring the Agent Controller: agentadm

The agentadm command helps to manage the Oracle Enterprise Manager Ops Center agents such as registering the Agent Controller to the proxy and unconfiguring the agents.

Synopsis

Oracle Solaris OS

```
/opt/SUNWxvmoc/bin/agentadm  
/opt/SUNWxvmoc/bin/agentadm [ -h | --help ]  
/opt/SUNWxvmoc/bin/agentadm subcommand [ options ]
```

Linux OS

```
/opt/sun/xvmoc/bin/agentadm -V  
/opt/sun/xvmoc/bin/agentadm [ -h | --help ]  
/opt/sun/xvmoc/bin/agentadm subcommand [ options ]
```

Usage

```
agentadm [-V | --version ] [ -K | --property-keys <file>] [ -q | --quiet ]  
[ -v | --verbose ] [ -f | --force ] [ -n | --norefresh ] [ -o |  
--output-file ] [ -h | --help]  
agentadm subcommand [ options ]
```

Options

The following common options are supported:

- K | --property-keys <file>: The properties filename for the subcommands.
- V | --version: Displays the version number of the Agent Controller software.
- h | --help: Displays the usage synopsis for all configuration steps supported by agentadm.
- v | --verbose: Display verbose error and informational messages. Use multiple occurrences of this option to increase the verbosity level.
- q | --quiet: Does not display anything and returns only the return code.
- f | --force: Ignores non critical errors during steps operations.
- n | --norefresh: Does not overwrite the existing operation.
- o | --output-file: Sends the output to the specified logfile.

Subcommands

The subcommands of agentadm are as follows:

start

Starts the Agent Controller services running on the host.

stop

Stops the Agent Controller services running on the host.

configure

Performs configuration tasks for the Agent Controller services.

unconfigure

Performs the inverse operation of configuring the Agent Controller.

usage

Equivalent to [-h | --help]

Subcommand options

start

Enter `agentadm start`.

stop

Enter `agentadm stop`.

configure

The configuration step consists of:

- `sc-console` registration of the agent to proxy.
- `scn-agent` cacao instance creation.
- `uce-agent` cacao instance creation.
- Registration of the agent's products to the proxy.

The registration of the agent to the proxy is as follows: `agentadm configure [-u | --user <user name>] [-p | --passwordfile<password-file>] [-a | --agent-ip <IP address>] [-t | --token <tokenfilename>] [-x | --proxy <URI>] [-I | --non-interactive] [-k | --keep-connection]`

`-u | --user <user name>`: The Online Account user name.

`-p | --passwordfile <passwordfile>`: Filename with the Online Account credentials.

`-a | --agent-ip <IP address>`: Specify the IP address to be used during registration.

`-t | --token <tokenfilename>`: Filename containing auto registration token.

`-x | --proxy <URI>`: URI of the proxy to be registered.

`-I | --non-interactive`: Launch `sc-console` in non-interactive mode (without `-i`). Default is interactive mode.

`-k | --keep-connection`: Do not re-register to proxy if the connection exists.

unconfigure

Enter `agentadm unconfigure`

Index

A

- accessing the cluster management UI, 9-11
- adding a directory server, 7-3
- adding a product alias, 4-3
- adding authentications, 4-3
- adding users, 7-2
- Agent Controllers
 - agentadm command, A-9
 - local Agent Controllers, 2-9
 - configuring on the Enterprise Controller, 2-9
 - configuring on the Proxy Controller, 2-10
 - unconfiguring on the Enterprise Controller, 2-9
 - unconfiguring on the Proxy Controller, 2-10
 - migrating between Proxy Controllers, 9-14
 - uninstalling, 11-1
 - viewing, 2-2
- agentadm command, A-9
- Assets
 - determining the number of, 5-4
- associating networks with a Proxy Controller, 2-15
- authentications
 - adding, 4-3
 - editing, 4-3
- Auto Service Requests
 - blacklisting an asset, 6-6
 - disabling, 6-6
 - enabling, 6-5
 - providing contact information, 6-4
 - providing contact information for an asset or group, 6-5
 - providing default contact information, 6-4
 - viewing an asset's ASR status, 6-4

B

- backup and restore
 - backing up an Enterprise Controller, 8-2
 - restoring an Enterprise Controller, 8-3
- blacklisting an asset for Auto Service Requests, 6-6

C

- changing the customer-managed database
 - location, 3-5

- changing the database credentials, 3-7
- changing the HTTP Proxy, 2-26
- checking the Enterprise Controller Cluster status, 9-11
- checking the Enterprise Controller status, 2-12
- checking the Proxy Controller status, 2-13
- command line administration, A-1
- configuring a notification profile, 7-22
- configuring a Proxy Controller to use a strong cipher suite configuration, 2-16
- configuring DHCP, 2-17
- configuring external DHCP servers, 2-20
- configuring Oracle Configuration Manager, 2-10
- configuring subnets, 2-19
- configuring the Enterprise Controller for WAN Boot, 2-23
- Connected Mode, 2-4
- connection modes, 2-4
 - switching to Connected Mode, 2-4
 - switching to Disconnected Mode, 2-4
- converting a single Enterprise Controller to high availability, 9-4
- converting to a single Enterprise Controller, 9-9

D

- database
 - changing credentials, 3-7
 - changing the customer-managed database location, 3-5
 - Installing and configuring a customer-managed database, 3-2
 - migrating to a customer-managed database, 3-4
 - upgrading a customer-managed database, 3-7
 - verifying, 3-7
- deleting a directory server, 7-5
- deleting a notification profile, 7-23
- deleting users, 7-2
- DHCP configuration, 2-17
- directory servers
 - adding, 7-3
 - deleting, 7-5
- disabling Auto Service Requests, 6-6
- disabling networks for a Proxy Controller, 2-15
- Disconnected Mode, 2-4
- downloading the OCDDoctor, 5-1

E

- ecadm command, A-1
- editing authentications, 4-3
- editing the energy cost, 4-4
- enabling Auto Service Requests, 6-5
- enabling networks for a Proxy Controller, 2-15
- energy cost
 - editing, 4-4
- Enterprise Controller
 - backing up, 8-2
 - checking the status, 2-12
 - ecadm command, A-1
 - high availability, 9-3
 - registering, 2-11
 - restoring, 8-3
 - starting, 2-12
 - stopping, 2-13
 - uninstalling, 11-5
 - viewing configuration, 2-3
 - WAN boot configuration, 2-23
- external DHCP server configuration, 2-20

H

- harvester script, 2-4
 - copying content to the Enterprise Controller, 2-8
 - downloading, 2-5
 - identifying a harvester system, 2-5
 - using, 2-5
- high availability, 9-3
 - accessing the cluster management UI, 9-11
 - checking the cluster status, 9-11
 - converting to a single Enterprise Controller, 9-9
 - converting to high availability, 9-4
 - managing network resources, 9-10
 - manually relocating, 9-9
 - removing a standby Enterprise Controller, 9-11
 - shutting down an Enterprise Controller without relocating, 9-11
- HTTP Proxy
 - changing, 2-26

I

- installing and configuring a customer-managed database, 3-2

L

- logs, 4-2

M

- managing HA network resources, 9-10
- managing Proxy Controller networks, 2-15
- managing roles, 7-21
- manually relocating the Enterprise Controller, 9-9
- migrating to a customer-managed database, 3-4

N

- networks
 - associating with a Proxy Controller, 2-15
 - enable or disable, 2-15
- notification profiles
 - configuring, 7-22
 - deleting, 7-23

O

- OCDDoctor, 5-4
 - downloading, 5-1
 - preinstallation checks, 5-2
 - running a self-diagnosis, 2-11
 - troubleshooting and tuning, 5-2
 - updating, 5-3
- Oracle Configuration Manager
 - configuring, 2-10

P

- performing preinstallation checks, 5-2
- performing troubleshooting and tuning, 5-2
- permissions
 - granted by roles, 7-5
 - required for tasks, 7-16
- preinstallation checks, 5-2
- product aliases, 4-3
- providing ASR contact information, 6-4
- Proxy Controllers
 - associate networks, 2-15
 - automatic failover, 9-12
 - checking the status, 2-13
 - configuring to use a strong cipher suite
 - configuration, 2-16
 - DHCP configuration, 2-17
 - enable or disable networks, 2-15
 - high availability, 9-12
 - maintenance mode, 2-14
 - manage networks, 2-15
 - proxyadm command, A-7
 - putting in maintenance mode, 2-14
 - removing from maintenance mode, 2-15
 - starting, 2-14
 - stopping, 2-14
 - subnet configuration, 2-19
 - uninstalling, 11-3
 - viewing, 2-2
- proxyadm command, A-7
- putting a Proxy Controller in maintenance mode, 2-14

R

- registering the Enterprise Controller, 2-11
- relocating the Enterprise Controller, 9-9
- removing a Proxy Controller from maintenance mode, 2-15
- removing a standby Enterprise Controller, 9-11
- replicating a user, 7-21

roles

- copying to a new user, 7-21
- managing, 7-21
- permissions granted by roles, 7-5
- tasks available based on permissions, 7-16

running a self-diagnosis, 2-11

S

self-diagnosis, 2-11

service status, 4-1

shutting down an Enterprise Controller without
relocating, 9-11

starting a Proxy Controller, 2-14

starting the Enterprise Controller, 2-12

stopping a Proxy Controller, 2-14

stopping the Enterprise Controller, 2-13

strong cipher suite configuration, 2-16

subnet configuration, 2-19

synchronizing remote users and roles, 7-4

T

troubleshooting with the OCDoctor, 5-2

tuning with the OCDoctor, 5-2

U

uninstalling

- Agent Controllers, 11-1

- Enterprise Controllers, 11-5

- Proxy Controllers, 11-3

updating the OCDoctor, 5-3

upgrading

- planning the upgrade, 10-2

upgrading a customer-managed database, 3-7

users

- adding, 7-2

- configuring notification profiles, 7-22

- deleting, 7-2

- deleting notification profiles, 7-23

- managing user roles, 7-21

- replicating, 7-21

- viewing role details, 7-2

using connection modes, 2-4

V

verifying the database, 3-7

viewing Agent Controllers, 2-2

viewing ASR status for an asset, 6-4

viewing logs, 4-2

viewing Proxy Controllers, 2-2

viewing service status, 4-1

viewing the Enterprise Controller configuration, 2-3

viewing user role details, 7-2

W

WAN boot configuration, 2-23

