

Oracle® Enterprise Manager Ops Center

Administration

12c Release 3 (12.3.2.0.0)

E59969-03

June 2016

Oracle Enterprise Manager Ops Center Administration, 12c Release 3 (12.3.2.0.0)

E59969-03

Copyright © 2007, 2016, Oracle and/or its affiliates. All rights reserved.

Primary Author: Krithika Gangadhar

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	xi
Audience	xi
Related Documents.....	xi
Conventions.....	xi
1 Get Started with Administration	
2 Manage the Infrastructure	
Introduction to Infrastructure.....	2-2
Roles for Infrastructure.....	2-2
Actions for Infrastructure.....	2-3
Location of Infrastructure Information in the User Interface.....	2-4
Viewing Infrastructure.....	2-5
Viewing Agent Controllers.....	2-5
Viewing Proxy Controllers.....	2-6
Viewing the Enterprise Controller Configuration.....	2-6
About Connection Modes.....	2-7
Switching to Disconnected Mode.....	2-7
Switching to Connected Mode.....	2-8
About Using the Harvester.....	2-8
Identify a Harvester System.....	2-8
Downloading the Harvester Bundle.....	2-9
Using the Harvester Script.....	2-9
Copying Content to the Enterprise Controller in Disconnected Mode.....	2-12
About Configuring Local Agent Controllers.....	2-14
Configuring the Local Agent Controller on the Enterprise Controller.....	2-14
Unconfiguring the Local Agent Controller on the Enterprise Controller.....	2-14
Configuring a Local Agent Controller on a Proxy Controller.....	2-15
Unconfiguring a Local Agent Controller on a Proxy Controller.....	2-15
Configuring Oracle Configuration Manager.....	2-15
Registering the Enterprise Controller.....	2-16
Running a Self Diagnosis.....	2-17

Viewing and Changing the EC, PC, and AC Status	2-17
Checking the Status of the Enterprise Controller	2-18
Starting the Enterprise Controller	2-18
Stopping the Enterprise Controller	2-19
Checking the Status of a Proxy Controller	2-19
Starting a Proxy Controller	2-19
Stopping a Proxy Controller	2-20
Putting a Proxy Controller in Maintenance Mode	2-20
Removing a Proxy Controller from Maintenance Mode	2-21
Checking the Status of an Agent Controller	2-21
About Managing Proxy Controller Networks	2-21
Associating Networks With a Proxy Controller	2-22
Enabling or Disabling Networks for a Proxy Controller	2-22
Changing the IP Address of an Enterprise Controller	2-22
Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration	2-23
About Configuring DHCP and Subnets for OS Provisioning	2-24
About DHCP	2-24
Configuring DHCP	2-25
About Subnets	2-26
Configuring Subnets	2-26
About External DHCP Servers	2-27
Configuring External DHCP Servers	2-28
About Configuring the Enterprise Controller for WAN Boot	2-30
Checking the WAN Boot Status	2-30
Changing the Default Port for Oracle Solaris 11 WAN Boot	2-30
Enabling or Disabling WAN Boot	2-31
Editing Oracle Solaris 11 Credentials	2-31
Retaining Migration Scripts in Server Pools	2-32
Generating a Default Set of OS Provisioning Profiles and Plans	2-32
Displaying Related Assets In Groups	2-33
Changing the HTTP Proxy	2-33
Using Diagnostics Mode	2-33
Viewing Blacklisted Assets	2-34
Rebalancing Assets	2-34
Related Resources for Infrastructure	2-36

3 Manage the Configuration

Introduction to Configuration Management	3-2
Roles for Configuration Management	3-2
Actions for Configuration Management	3-3
Location of Configuration Management Information in the User Interface	3-3
About Auto Service Request Configuration	3-4
About BUI Configuration	3-4

About Console Access Configuration.....	3-5
About Discovery Configuration	3-5
About Domain Model Navigator Configuration	3-5
About EC Manager Configuration.....	3-6
About Job Manager Configuration	3-6
About OCDocctor Configuration.....	3-6
About OS Provisioning Configuration.....	3-7
About Proxy Manager Configuration.....	3-8
About Report Service Configuration	3-8
About Server Pools Configuration.....	3-9
About Virtualization Configuration	3-9
Related Resources for Configuration Management.....	3-10
4 Manage the Database	
Introduction to Database Management.....	4-1
Roles for Database Management.....	4-2
Actions for Database Management.....	4-2
Location of Database Management Information in the User Interface.....	4-3
Installing and Configuring a Customer-Managed Database	4-3
Installing and Configuring Oracle 12CDB Customer-Managed Database	4-5
Migrating to a Customer-Managed Database	4-7
Changing the Customer-Managed Database Location	4-8
Verifying the Database.....	4-10
Upgrading a Customer-Managed Database	4-10
Changing the Database Credentials.....	4-10
Changing the Database Credentials for the Ops Center User	4-11
Changing the Database Credentials for the Read-Only User	4-12
Defragmenting an Embedded Database	4-13
Consolidating Reports Data on a Customer-Managed Database.....	4-14
Related Resources for Database Management	4-15
5 Perform General Administration	
Introduction to General Administration	5-1
Roles for General Administration	5-2
Actions for General Administration	5-2
Location of General Administration Information in the User Interface.....	5-2
Viewing and Understanding Service Statuses.....	5-3
Viewing Service Status	5-4
Viewing Logs.....	5-4
Adding a Product Alias	5-5
Adding or Editing Authentications	5-5
Editing the Energy Cost.....	5-6
Related Resources for General Administration.....	5-7

6	Manage the OCDoctor	
	Introduction to the OCDoctor	6-1
	Roles for OCDoctor	6-1
	Actions for OCDoctor.....	6-2
	Location of OCDoctor Information in the User Interface	6-2
	Downloading the OCDoctor	6-2
	Performing Preinstallation Checks.....	6-3
	Performing Troubleshooting and Tuning.....	6-4
	Updating the OCDoctor.....	6-4
	Cleanup Through OCDoctor.....	6-5
	About Determining the Number of Asset Access Points.....	6-6
	Viewing the Access Point Count for Your Environment.....	6-6
	Viewing the Access Point List for Each Proxy Controller	6-7
	Access Point Types for Each Proxy Controller	6-7
	Viewing All Access Point Data.....	6-7
	Related Resources for OCDoctor	6-8
7	Manage Auto Service Request	
	Introduction to ASR.....	7-1
	Overview of ASR	7-1
	Prerequisites	7-2
	How ASR Activation Works	7-3
	How ASR Creation Works	7-4
	Roles for ASR.....	7-4
	Actions for ASR.....	7-4
	Location of ASR Information in the User Interface	7-5
	Viewing ASR Status for an Asset	7-5
	Providing Contact Information.....	7-5
	Providing Default Contact Information.....	7-6
	Providing Contact Information for an Asset or Group.....	7-6
	Enabling ASR.....	7-7
	Disabling ASR	7-7
	Blacklisting an Asset.....	7-8
	Testing ASR	7-8
	Moving Assets from Standalone ASR to Oracle Enterprise Manager Ops Center ASR	7-8
	Related Resources for Auto Service Request	7-9
8	Manage the Users and Roles	
	Introduction to User and Role Management	8-2
	Roles for User and Role Management	8-2
	Actions for User and Role Management	8-2
	Location of User and Role Management Information in the User Interface	8-3

Adding a User	8-3
Deleting a User	8-4
Viewing User Role Details.....	8-4
Adding a Directory Server	8-4
About Synchronizing Remote Users and Roles	8-6
Synchronizing Remote Users and Roles With One Directory Server	8-7
Synchronizing Remote Users and Roles With All Directory Servers	8-7
Deleting a Directory Server	8-7
About Roles and Permissions	8-8
How Roles are Mapped to Permissions	8-8
How Permissions are Mapped to Tasks.....	8-18
Managing Roles.....	8-23
Replicating a User	8-24
About Notification Profiles	8-24
Configuring a Notification Profile	8-25
Deleting a Notification Profile.....	8-26
Viewing the Audit Log	8-27
Related Resources for User and Role Management.....	8-27
9 Perform Backup and Recovery	
Introduction to Backup and Recovery	9-1
Roles for Backup and Recovery	9-2
Actions for Backup and Recovery	9-2
Location of Backup and Recovery Information in the User Interface.....	9-3
Backing Up and Restoring an Enterprise Controller.....	9-3
Backing Up an Enterprise Controller	9-3
Restoring an Enterprise Controller	9-5
Backing Up and Restoring a Proxy Controller	9-7
Backing Up a Proxy Controller.....	9-8
Restoring a Proxy Controller	9-8
Related Resources for Backup and Recovery	9-9
10 Manage High Availability	
Introduction to High Availability	10-1
About Enterprise Controller High Availability	10-1
About Proxy Controller High Availability	10-3
Roles for High Availability.....	10-4
Actions for High Availability.....	10-4
Location of High Availability Information in the User Interface	10-5
About Enabling and Using Enterprise Controller High Availability	10-5
Converting a Single Enterprise Controller to High Availability	10-6
Converting a High Availability Configuration to a Single Enterprise Controller.....	10-11
Performing a Manual Relocate.....	10-12

Managing HA Network Resources.....	10-12
Removing a Standby Enterprise Controller Node.....	10-14
Checking the Status of the Enterprise Controller Cluster	10-14
Shutting Down the Enterprise Controller Temporarily Without Relocating.....	10-15
Accessing the Cluster Management UI.....	10-15
Enabling and Using Proxy Controller High Availability	10-15
Enabling Automatic Failover.....	10-15
Disabling Automatic Failover.....	10-16
Setting the Relative Power for Proxy Controllers.....	10-16
Recovering After an Automatic Failover	10-17
Migrating Assets Between Proxy Controllers	10-18
Migrating Assets from a Failed Proxy Controller	10-18
Removing Access Points.....	10-19
Related Resources for High Availability	10-19

11 Perform Upgrades

Introduction to Upgrade.....	11-1
Roles for Upgrade.....	11-1
Actions for Upgrade	11-2
Location of Upgrade Information in the User Interface.....	11-2
Versions Supported for Upgrade	11-2
Upgrading From Version 12.3	11-3
Upgrading From Version 12.2	11-3
Upgrading From Version 12.1	11-3
Upgrading From Version 11g.....	11-4
Planning the Upgrade	11-5
Database Requirements	11-6
Upgrading Your Environment.....	11-7
Related Resources for Upgrade	11-7

12 Uninstall and Unconfigure the Software

Introduction to Uninstall and Unconfigure	12-1
Roles for Uninstall and Unconfigure	12-1
Actions for Uninstall and Unconfigure	12-2
Location of Uninstall and Unconfigure Information in the User Interface.....	12-2
Uninstalling and Unconfiguring Agent Controllers.....	12-2
Uninstalling and Unconfiguring Agent Controllers from the User Interface	12-3
Uninstalling and Unconfiguring Agent Controllers from the Command Line	12-3
Uninstalling and Unconfiguring a Proxy Controller.....	12-4
Unconfiguring and Uninstalling a Proxy Controller from the User Interface	12-5
Removing a Proxy Controller from the User Interface.....	12-5
Unconfiguring a Proxy Controller from the Command Line	12-5
Uninstalling a Proxy Controller from the Command Line	12-6

Uninstalling and Unconfiguring the Enterprise Controller	12-7
Unconfiguring the Enterprise Controller.....	12-7
Uninstalling the Enterprise Controller.....	12-7
Related Resources for Uninstall and Unconfigure.....	12-9

A Command Line Administration

About Configuring the Enterprise Controller: ecadm.....	A-1
Synopsis for ecadm	A-1
Options for ecadm.....	A-2
Subcommands for ecadm.....	A-2
Subcommand Options for ecadm	A-4
Exit Status for ecadm	A-7
About Configuring the Proxy Controller: proxyadm.....	A-8
Synopsis	A-8
Options for proxyadm	A-8
Subcommands for proxyadm	A-8
Subcommand Options for proxyadm.....	A-9
Exit Status for proxyadm.....	A-11
About Configuring the Agent Controller: agentadm.....	A-11
Synopsis for agentadm	A-12
Usage.....	A-12
Options for agentadm.....	A-12
Subcommands for agentadm.....	A-12
Subcommand Options for agentadm	A-13

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.

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*
- *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*
- *Oracle Enterprise Manager Ops Center Installation for Oracle Solaris Operating System*
- *Oracle Enterprise Manager Ops Center Configuration Reference*
- *Oracle Enterprise Manager Ops Center Operations Reference*
- *Oracle Enterprise Manager Ops Center Virtualize Reference*
- *Oracle Enterprise Manager Ops Center Operations for Oracle SuperCluster Reference*
- *Oracle Enterprise Manager Ops Center Command Line Interface*
- *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*

For more information, see the other documents in the Oracle Enterprise Manager Ops Center 12c Release 3 documentation set, located at this site: http://docs.oracle.com/cd/E59957_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.

Get Started with Administration

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.

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

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 administrating 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:

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

-
- [Manage 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.
 - [Perform Upgrades](#): Explains how to upgrade to the latest available version of Oracle Enterprise Manager Ops Center.
 - [Uninstall and Unconfigure the Software](#): Explains how to uninstall and unconfigure Oracle Enterprise Manager Ops Center.

Manage the 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.

This chapter includes the following sections:

- [Introduction to Infrastructure](#)
- [Roles for Infrastructure](#)
- [Actions for Infrastructure](#)
- [Location of Infrastructure Information in the User Interface](#)
- [Viewing Infrastructure](#)
- [About Connection Modes](#)
- [About Using the Harvester](#)
- [About Configuring Local Agent Controllers](#)
- [Configuring Oracle Configuration Manager](#)
- [Registering the Enterprise Controller](#)
- [Running a Self Diagnosis](#)
- [Viewing and Changing the EC, PC, and AC Status](#)
- [About Managing Proxy Controller Networks](#)
- [Changing the IP Address of an Enterprise Controller](#)
- [Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration](#)
- [About Configuring DHCP and Subnets for OS Provisioning](#)
- [About 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](#)
- [Using Diagnostics Mode](#)

- [Viewing Blacklisted Assets](#)
- [Rebalancing Assets](#)
- [Related Resources for Infrastructure](#)

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 [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.

Roles for Infrastructure

You require specific roles to perform infrastructure tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 2-1 Infrastructure Tasks and Roles

Task	Role
View infrastructure	Ops Center Admin
Use connection mode or disconnection mode	Ops Center Admin
Configure and Unconfigure Local Agent Controllers	Ops Center Admin
Register the Enterprise Controller	Ops Center Admin
Run a self diagnosis	Ops Center Admin
Check the controller status	Ops Center Admin
Associate, enable, or disable networks for Proxy Controllers	Ops Center Admin
Configure DHCP, External DHCP servers, and subnets	Ops Center Admin

Table 2-1 (Cont.) Infrastructure Tasks and Roles

Task	Role
Enable or disable WAN Boot	Ops Center Admin
Edit Oracle Solaris 11 credentials	Ops Center Admin
Change the HTTP Proxy	Ops Center Admin

Actions for Infrastructure

You can perform various infrastructure operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- View infrastructure
- Switch to disconnected mode
- Switch to connected mode
- Download the harvester bundle
- Copy content to the Enterprise Controller in disconnected mode
- Configure a Local Agent Controller on an Enterprise Controller or a Proxy Controller
- Unconfigure a Local Agent Controller on an Enterprise Controller or a Proxy Controller
- Configure Oracle Configuration Manager
- Register the Enterprise Controller
- Run a Self Diagnosis
- Check the Status of a Enterprise Controller, Proxy Controller, or Agent Controller
- Start an Enterprise Controller or a Proxy Controller
- Stop an Enterprise Controller or a Proxy Controller
- Put a Proxy Controller in Maintenance Mode
- Remove a Proxy Controller from Maintenance Mode
- Associate Networks With a Proxy Controller
- Enable or Disable Networks for a Proxy Controller
- Configure Proxy Controllers to Use a Strong Cipher Suite Configuration
- Configure DHCP and Subnets
- Configure External DHCP Servers
- Check the WAN Boot Status

- Change the Default Port for Oracle Solaris 11 WAN Boot
- Enable or Disable WAN Boot
- Edit Oracle Solaris 11 Credentials
- Retain Migration Scripts in Server Pools
- Generate a Default Set of OS Provisioning Profiles and Plans
- Display Related Assets In Groups
- Change the HTTP Proxy

Location of Infrastructure Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find infrastructure information in different locations.

Table 2-2 Location of Infrastructure Information in the UI

To See	Location
View Agent Controllers	Expand Assets in the Navigation pane and select a group of managed operating systems.
View Proxy Controllers	Expand Administration in the Navigation pane and select a Proxy Controller. Select Configuration in the center pane.
View Enterprise Controller configuration	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane.
Connection Mode	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Setup Connection Mode in the Actions pane.
Local Agent Controller	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Configure Local Agent/ Unconfigure Local Agent in the Actions pane.
Local Agent Controller on a Proxy Controller	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Configure Agent on Proxy/ Unconfigure Agent on Proxy in the Actions pane.
Register Enterprise Controller	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Register Enterprise Controller in the Actions pane.
Run Self Diagnosis	Expand Administration in the Navigation pane and select an asset. Select Self Diagnosis in the Actions pane.
Proxy Controller Networks	Expand Administration in the Navigation pane and select a Proxy Controller.
Configure DHCP	Expand Administration in the Navigation pane and select a Proxy Controller. Select DHCP Config in the Actions pane.
Configure Subnets	Expand Administration in the Navigation pane and select a Proxy Controller. Select Subnets in the Actions pane.

Table 2-2 (Cont.) Location of Infrastructure Information in the UI

To See	Location
Configure External DHCP Servers	Expand Administration in the Navigation pane and select a Proxy Controller. Select External DHCP Servers in the Actions pane.
Enterprise Controller for WAN boot	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration tabs and choose OS Provisioning from the subsystems menu.
Edit Oracle Solaris 11 Credentials	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Credentials.
Migration Scripts in Server Pools	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Server Pools from the subsystem menu in the Configuration tab.
OS Provisioning Profiles and Plans	Expand Administration in the Navigation pane and select a Enterprise Controller. Select OS Provisioning from the subsystem menu in the Configuration tab.
Assets In Groups	Expand Administration in the Navigation pane and select a Enterprise Controller. Select BUI from the subsystem menu in the Configuration tab.
Change HTTP Proxy	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Change HTTP Proxy in the Actions pane.

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.

The Agent Controller information includes:

- 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.

The Proxy Controllers information includes:

- 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.

About Connection Modes

Oracle Enterprise Manager Ops Center can operate in either Connected Mode 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.

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.

About 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.

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.

Identify a Harvester System

You must select a system from which to run the harvester script.

The selected 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 an internet-facing system, download the harvester script. See [Related Resources for Infrastructure](#) for the link to download the script.
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.

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.

Note:

Due to security reasons, avoid storing your password in clear text inside a file when working with the harvester in disconnected mode. If you choose to use a text file, use it with caution and set its permissions to 400, store it in a safe directory allowing only safe user(s) to use it.

Starting with harvester version 2.16, the harvester script checks the password file permissions and provides a warning if the permissions are other than 400. You can continue and let the script change the permissions to 400 or quit and take necessary actions such as changing the password and the permissions before the next run.

- `--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, you need to upload the content in bulk.

Copying a Knowledge Base Bundle

You can upload 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

You can upload a new knowledge base bundle to the Enterprise Controller and upload the patch content.

Follow this procedure to upload a new knowledge base bundle to the Enterprise Controller and to upload the 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.
7. 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
#
```

8. 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
#
```

Copying a Knowledge Base Bundle and Incremental Patches

You can upload a new knowledge base bundle to the Enterprise Controller and upload a 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.
7. 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
#
```

8. 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
#
```

About 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.

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.

Note:

On Oracle Solaris 10, the local Agent Controller uses Java 6 version. If a later version of Java 6 is already installed on the system, then the local Agent Controller uses the already installed greater version. Starting from 12.3.2, if Java 7 version is installed on the system, then the local Agent Controller uses the Java 7 version instead of the Java 6 version.

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.

Follow these steps to configure the Local Agent Controller on the Enterprise Controller.

1. Click the **Enterprise Controller** in the **Administration** section of the Navigation pane.
2. Click **Configure Local Agent** in the Actions pane.

A confirmation window is displayed.

3. Select the existing SNMPV3 credentials or create new SNMPV3 credentials.
 - To use the existing SNMPV3 credentials, click **Select**.
 - To create new SNMPV3 credentials, click **New**.
4. 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.

Follow these steps to unconfigure the Local Agent Controller on the Enterprise Controller.

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.

Follow these steps to configure a Local Agent Controller on a Proxy Controller.

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. Select the existing SNMPV3 credentials or create new SNMPV3 credentials.
 - To use the existing SNMPV3 credentials, click **Select**.
 - To create new SNMPV3 credentials, click **New**.
4. 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.

Follow these steps to unconfigure a Local Agent Controller on a Proxy Controller.

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.

Follow these steps to register the Enterprise Controller.

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 OCDoctor'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 EC, PC, and AC 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" successfully 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.

To check the status of a Proxy Controller, perform the following steps:

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.

Follow this procedure to put a Proxy Controller in maintenance mode.

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.

Follow this procedure to remove a Proxy Controller from maintenance mode.

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.

Checking the Status of an Agent Controller

You can check the status of an Agent Controller using the `agentadm` command.

To check the status of the Agent Controller, perform the following steps:

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

For example:

```
# ./agentadm status  
online
```

The status of the Agent Controller is displayed.

About 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.

To associate networks with a Proxy Controller, perform the following steps:

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.

Changing the IP Address of an Enterprise Controller

You can change the Enterprise Controller IP address and then update the Proxy Controllers with the new Enterprise Controller IP address using the `proxyadm` command.

To change the IP address of the Enterprise Controller, stop the Enterprise Controller, change the IP address, and then restart the Enterprise Controller.

Once the Enterprise Controller IP address is changed, you must update the Proxy Controllers with the new Enterprise Controller IP address using the `proxyadm` command.

Note: Do not modify the host name of the Enterprise Controller, Proxy Controller, and Agent Controller system.

To update the Proxy Controller with the new Enterprise Controller IP address:

1. Stop the Proxy Controller using the `proxyadm` command with the `stop` subcommand and the `-w` option. For example:


```
# proxyadm stop -w
```
2. To change the IP address on an Oracle Solaris 10 configuration, see <http://docs.oracle.com/cd/E19253-01/816-4554/gbwx/index.html>, and to change the IP address on an Oracle Solaris 11 configuration, see https://docs.oracle.com/cd/E23824_01/html/821-1458/gjwiq.html.
3. On the Proxy Controller, update the `/var/opt/sun/xvm/persistence/scn-proxy/connection.properties` URL property to point to the new IP address of the Enterprise Controller. Update this URL property through the command line interface using the `proxyadm` command with the `update` subcommand and the `-s` option:


```
proxyadm update -s|--satellite-ip <ip>
```
4. Restart the Proxy Controller using the `proxyadm` command with the `start` subcommand and the `-w` option. For example:


```
# proxyadm start -w
```

Changing the IP address for the Proxy Controllers is not supported. However, you can create a new Proxy Controller and move the assets to the new Proxy Controller.

Note:

You can change the IP address for an Agent Controller.

Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration

You can configure 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 Oracle Technology Network Java SE Downloads page. See [Related Resources for Infrastructure](#) for the link to Java SE Downloads page.
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.

About 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 [About 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.

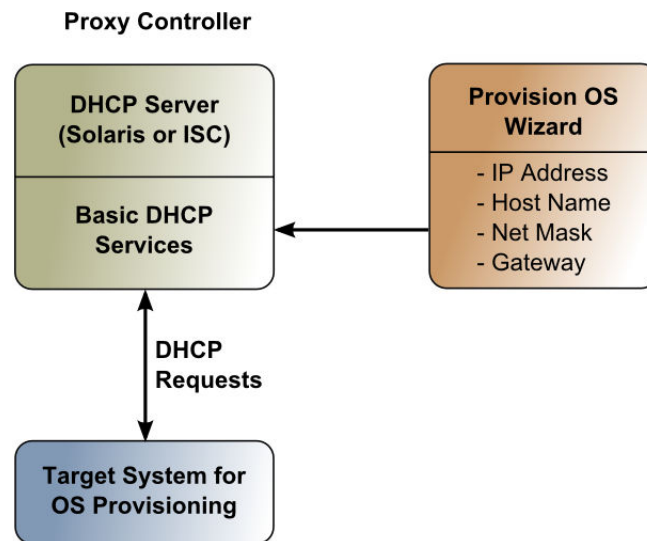
The DHCP Config action requires that you specify the Ethernet interface through which the Proxy Controller should provide DHCP services, for example `bge0`. You can establish DHCP services on all the Ethernet interfaces in the Proxy Controller. The Proxy Controller's Ethernet interface that you specify 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 shows the basic DHCP configuration.

Figure 2-1 Basic DHCP Configuration



Configuring DHCP

You can configure DHCP using Oracle Enterprise Manager Ops Center.

To configure DHCP, perform the following steps:

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.

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

You can configure subnets using Oracle Enterprise Manager Ops Center.

To configure subnets, perform the following steps:

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.

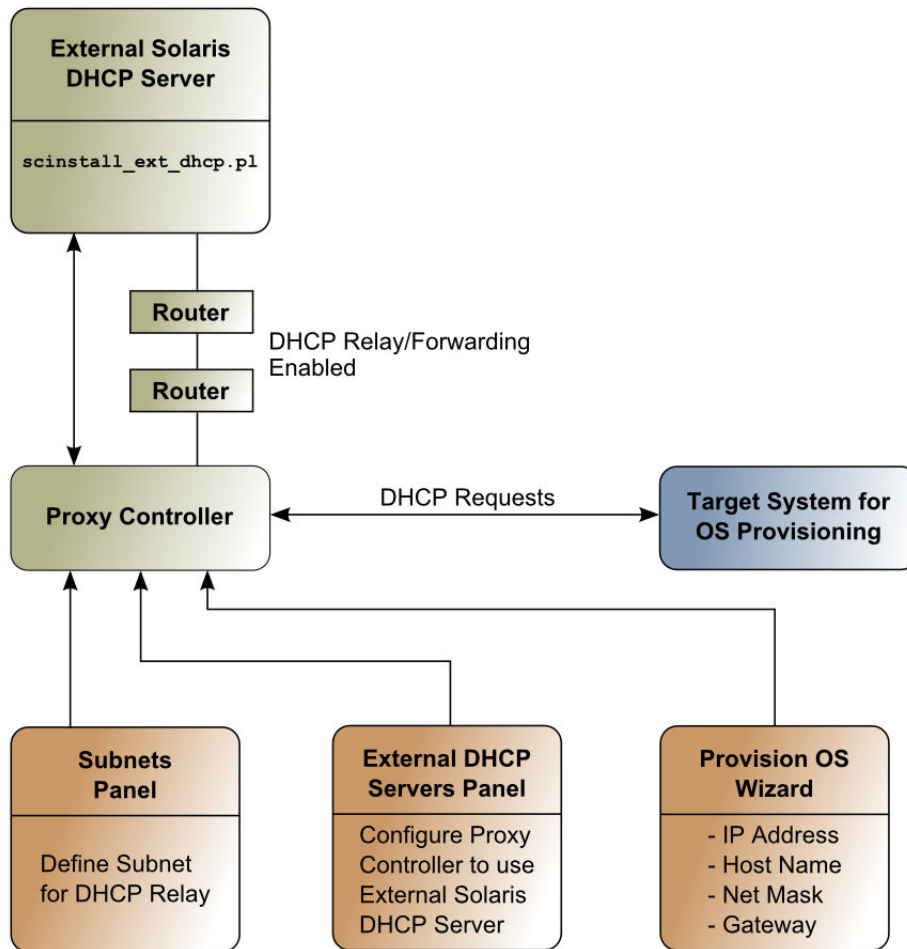
About External DHCP Servers

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](#) 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

You can configure external DHCP servers using Oracle Enterprise Manager Ops Center.

To configure external DHCP servers, perform the following steps:

1. Use `wget` to get the `scinstall_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.

About 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.

To check the WAN Boot status, perform the following steps:

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

You can enable or disable WAN Boot.

To enable or disable WAN Boot, perform the following steps:

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`.

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.

To retain migration scripts in server pools, perform the following steps:

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.

To change the HTTP Proxy, perform the following steps:

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.

Using Diagnostics Mode

You can enable the diagnostics mode to collect diagnostics data for all jobs that are run.

When the diagnostics mode is enabled, the diagnostics data for each job is collected under the `/var/opt/sun/xvm/logs/diagnostics/<jobID.RunID>` directory.

Note: Enabling the diagnostic mode degrades the performance of Oracle Enterprise Manager Ops Center.

To enable the diagnostic mode:

1. Expand the **Administration** section in the Navigation pane, then click **Enterprise Controller**.
2. Click the **Configuration** tab.
3. Select **OCDocctor** from the Subsystem menu.
4. Change the value of the `DiagnosticsOn` property to `true` to collect diagnostics data for all jobs that are run.
5. Change the value of the `DiagnosticsOnForFailedJobs` property to `true` to collect diagnostics data only if a job fails.

Note: After the diagnostics data is collected, the diagnostics mode should be disabled by modifying the value of system property to `false`.

Viewing Blacklisted Assets

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 as described in [Blacklisting an Asset](#). You can view the list of assets added to the blacklist.

To view the blacklisted assets:

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

The asset names that are in the blacklist mode are displayed in the center pane.

3. (Optional) To remove the assets from the blacklist mode, select the asset name in the center pane and click **Clear blacklist**.
4. (Optional) To update the credentials of the assets in blacklist mode, select the asset name in the center pane and click **Update credentials**.

Rebalancing Assets

You can rebalance assets of a Proxy Controller.

When a Proxy Controller fails, you need to rebalance the assets of the failed Proxy Controller by migrating them to other Proxy Controllers. You can also rebalance the assets of a Proxy Controller when it experiences a high load by migrating the assets to other Proxy Controllers.

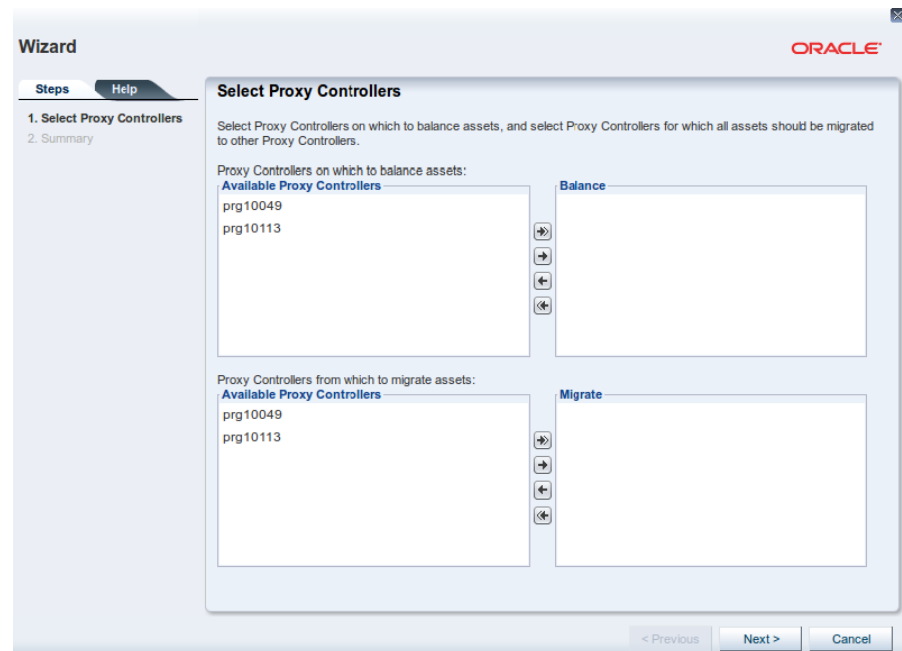
When an asset rebalance job is initiated, it calculates the necessary migrations required and starts the migration tasks.

To rebalance assets:

1. Expand the Administration section of the Navigation pane, then select **Enterprise Controller**.
2. Click **Rebalance Assets** in the Actions pane.

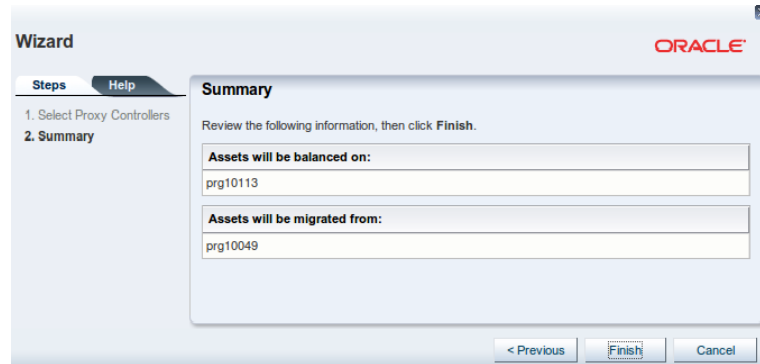
The Select Proxy Controller wizard appears which displays the available Proxy Controllers on which to balance assets and Proxy Controllers from which to migrate assets.

Figure 2-3 Select Proxy Controllers Wizard



3. For Proxy Controllers on which to balance assets, select and move the specific Proxy Controller listed in the Available Proxy Controllers field to the Balance field.
4. For Proxy Controllers from which to migrate assets, select and move the specific Proxy Controller listed in the Available Proxy Controllers field to the Migrate field.
5. Click **Next**.

The Summary wizard with the Proxy Controller selected for assets to be balanced on and Proxy Controller selected for assets to be migrated from is displayed.

Figure 2-4 Summary Wizard

6. Click **Finish**.

Related Resources for Infrastructure

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For more information about using Disconnected mode, see *Oracle Enterprise Manager Ops Center Use Disconnected Mode*
- For information on using the harvester script to upload the content in bulk, see *Oracle Enterprise Manager Ops Center Configuration Reference*
- To download the harvester script, go to https://updates.oracle.com/OCDoctor/harvester_bundle-latest.zip
- For information on the advantages of managing assets using Agent Controller, see *Oracle Enterprise Manager Ops Center Operations Reference*
- For Oracle Technology Network Java SE Downloads page, go to <http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>
- For more information on WAN boot connection, see *Oracle Enterprise Manager Ops Center Operations Reference*
- To provide a new key and certificate for Oracle Solaris 11, go to <https://pkg-register.oracle.com>
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Manage the Configuration

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

This chapter includes the following sections:

Topics

- [Introduction to Configuration Management](#)
- [Roles for Configuration Management](#)
- [Actions for Configuration Management](#)
- [Location of Configuration Management Information in the User Interface](#)
- [About Auto Service Request Configuration](#)
- [About BUI Configuration](#)
- [About Console Access Configuration](#)
- [About Discovery Configuration](#)
- [About Domain Model Navigator Configuration](#)
- [About EC Manager Configuration](#)
- [About Job Manager Configuration](#)
- [About OCDoctor Configuration](#)
- [About OS Provisioning Configuration](#)
- [About Proxy Manager Configuration](#)
- [About Report Service Configuration](#)
- [About Server Pools Configuration](#)
- [About Virtualization Configuration](#)
- [Related Resources for Configuration Management](#)

Introduction to Configuration Management

The Oracle Enterprise Manager Ops Center can be used to configure different subsystems.

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.

- Auto Service Request
- BUI
- Console Access Configuration
- Discovery
- Domain Model Navigator
- EC Manager
- Job Manager
- OC Doctor
- OS Provisioning
- Proxy Manager
- Report Service
- Server Pools
- Virtualization

Roles for Configuration Management

List of required roles for configuration management tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 3-1 Configuration Management Tasks and Roles

Task	Role
Modify any of the subsystem configuration	Ops Center Admin

Actions for Configuration Management

You can perform the operations below using the Configuration tab in Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can configure the Auto Service Request, BUI, Console Access Configuration, Discovery, Domain Model Navigator, EC Manager, Job Manager, OCDoctor, OS Provisioning, Proxy Manager, Report Service, Server Pools, Virtualization subsystem properties for an Enterprise Controller.

Location of Configuration Management Information in the User Interface

This table lists where to find different information for configuration management in the UI.

Table 3-2 Location of Configuration Management Information in the UI

To See	Location
View Auto Service Request subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Auto Service Request from the Subsystem drop-down
View BUI subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select BUI from the Subsystem drop-down
View Console Access Configuration subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Console Access Configuration from the Subsystem drop-down.
View Discovery subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Discovery from the Subsystem drop-down.
View Domain Model Navigator subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Domain Model Navigator from the Subsystem drop-down.
View EC Manager subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select EC Manager from the Subsystem drop-down.
View Job Manager subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Job Manager from the Subsystem drop-down.
View OCDoctor subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select OCDoctor from the Subsystem drop-down.
View OS Provisioning subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select OS Provisioning from the Subsystem drop-down.
View Proxy Manager subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Proxy Manager from the Subsystem drop-down.

Table 3-2 (Cont.) Location of Configuration Management Information in the UI

To See	Location
View Report Service subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Report Service from the Subsystem drop-down.
View Server Pools subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Server Pools from the Subsystem drop-down.
View Virtualization subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select Virtualization from the Subsystem drop-down.

About Auto Service Request Configuration

The Auto Service Request subsystem manages the ASR settings for adding assets to the blacklist mode.

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.

The following system property is displayed for Auto Service Request subsystem:

serial.blacklist: Subsystem property to add an asset to the blacklist mode. Enter the serial number of the asset to be added in the blacklist mode in the value field.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the Auto Service Request subsystem property value.

About BUI Configuration

The BUI subsystem manages the group settings for displaying the 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.

The following system property is displayed for BUI subsystem:

com.oracle.sysman.showSubTreeInGroups: Subsystem property to display the related assets in groups. Set the value to `true` to display the related assets in groups and set the value to `false` if you do not want to display the related assets in groups.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the BUI subsystem property value.

About Console Access Configuration

To enable a connection to a service processor or virtual machine, you must define the user account that Oracle Enterprise Manager Ops Center uses to open an SSH tunnel on the Enterprise Controller or to create a serial connection.

You need to create an account for each type of asset which uses SSH to connect to a serial console. Before you create an account for the assets, you must define the **ConsoleSSHCredname** system property.

The following system property is displayed for Console Access Configuration subsystem:

ConsoleSSHCredname: Subsystem property to define the Console Access Configuration subsystem property for console access. Set the value of this property with the name of the new user account.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the Console Access Configuration subsystem property value.

About Discovery Configuration

Several configuration properties are available in Oracle Enterprise Manager Ops Center for discovery configuration.

The following system properties are displayed for Discovery subsystem:

- **service-tags-discovery-enabled:** Subsystem property to enable or disable Find Assets action to discover assets using service tags. Set the value of this property to `true` to enable discovery by service tags and set the value to `false` to disable discovery by service tags.
- **ssh.alom.timeout:** Starting in Release 12.3.1, the discovery of assets with the ALOM service processor is disabled by default. If your site has an asset with this type of service processor, enable discovery by changing the value of this property from 0 to the number of seconds to allow for discovery.

Note: Do not modify the property settings unless directed by Oracle.

See the [Related Resources for Configuration Management](#) for information on editing the Discovery subsystem property value.

About Domain Model Navigator Configuration

Oracle Enterprise Manager Ops Center provides a Domain Model Navigator to allow Oracle support personnel to gather detailed information about the state of the system.

You can enable or disable the Domain Model Navigator subsystem by changing the value of `allowToRun` system property.

The following property is displayed for Domain Model Navigator subsystem:

allowToRun: Subsystem property to enable or disable the Domain Model Navigator. Set the value to `true` to enable the Domain Model Navigator and `false` to disable the Domain Model Navigator.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the Domain Model Navigator subsystem property value.

About EC Manager Configuration

You can edit the system properties to control the timestamp in audit logs and to select the type of email notifications to send in Oracle Enterprise Manager Ops Center.

The following system properties are displayed for EC Manager subsystem:

- **audit.dateformat:** Subsystem property to specify the format of date and time for audit logs. Edit the value of this property with a specification that is supported by Java's SimpleDateFormat class.
- **alert.mail.format:** Subsystem property to send email notifications either in HTML or plain text format. Set the value of this property to TEXT_FORMAT to receive email notifications in the form of plain text or set to HTML_FORMAT to receive email notifications in HTML format. By default, the value of this property is set to HTML_FORMAT. If you provide an invalid value, then the default format is considered.

Note: Do not modify the **audit.dateformat** property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the EC Manager subsystem property value.

About Job Manager Configuration

You can change the configuration of jobs in Oracle Enterprise Manager Ops Center.

The Job Manager subsystem manages the way jobs are run.

The following property is displayed for a Job Manager subsystem:

taskTimeOut: Subsystem property to increase or decrease the task performance of all jobs. Set a higher value to increase the performance of all jobs and set to a lower value to decrease the performance of all jobs.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the Job Manager subsystem property value.

About OCDoctor Configuration

You can change the configuration of OCDoctor in Oracle Enterprise Manager Ops Center.

The OCDoctor subsystem property value can be modified to set the upload path for OCDoctor and to enable diagnostics mode to collect the diagnostics data for all jobs that are run.

The following system properties are displayed for OCDoctor:

- **UPLOAD_PATH:** Subsystem property to define the OCDoctor upload path. Set the value of this property with the upload path.
- **DiagnosticsOn:** Subsystem property to collect diagnostics data for all jobs that are run. Set the value to `true` to collect the diagnostics data for all jobs.
- **DiagnosticsOnForFailedJobs:** Subsystem property to collect diagnostics data only if a job fails. Set the value to `true` to collect the diagnostics data when a job fails.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the OCDoctor subsystem property value.

About OS Provisioning Configuration

You can change the configuration of OS Provisioning in Oracle Enterprise Manager Ops Center.

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 using OS Provisioning subsystem.

You can also enable or disable WAN boot using the OS Provisioning subsystem. 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.

The following system properties are displayed for OS Provisioning subsystem:

- **createS11Profiles:** Subsystem property to enable automatic generation of OS Provisioning profiles and plans. Set the value to `true` to enable the automatic generation of profiles and plans and set the value to `false` to disable the automatic generation of profiles and plans.
- **usesS11WANBoot:** Subsystem property to enable WAN boot for Oracle Solaris 11. Set the value to `true` to enable WAN boot and set the value to `false` to disable WAN boot.
- **usesS10WANBoot:** Subsystem property to enable WAN boot for Oracle Solaris 10. Set the value to `true` to enable WAN boot and set the value to `false` to disable WAN boot.
- **useSRUVersion:** Subsystem property to set the same SRU version that you selected when creating a profile to be used for provisioning your operating system. Set the value to `true` to set the same SRU version.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the OS Provisioning subsystem property value.

About Proxy Manager Configuration

You can change the configuration of the Proxy Manager subsystem in Oracle Enterprise Manager Ops Center to enable the automatic migration of assets to another Proxy Controller when the current Proxy Controller fails and also to modify the Proxy Controller's relative power and relative cascade weight.

The Proxy Manager subsystem manages the interactions between the parts of the infrastructure.

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.

When Oracle Enterprise Manager Ops Center migrates an asset, it targets the available Proxy Controller with the lowest load. Using the Proxy Manager subsystem, you can edit a Proxy Controller's relative power to make it a more or less common target for automatic migration and also edit the `RELATIVE_CASCADE_WEIGHT` to increase or decrease the importance of Agent Controllers in the load calculation.

The following system properties are displayed for a Proxy Manager subsystem:

- **AUTO_FAILOVER**: Subsystem property to enable or disable the automatic migration of assets to another Proxy Controller when the current Proxy Controller fails. Set the value to `true` to enable the automatic migration of assets and set the value to `false` to disable the automatic migration of assets.
- **RELATIVE_CASCADE_WEIGHT**: Subsystem property to increase or decrease the importance of Agent Controllers in the load calculation. Set to a higher value to increase the importance of Agent Controllers in the load calculation.
- **<PROXY CONTROLLER>.RELATIVE_POWER**: Subsystem property to modify the Proxy Controller's relative power. Set to a higher value for the Proxy Controller to be a more likely target for automatic migration.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the Proxy Manager subsystem property value.

About Report Service Configuration

You can change the configuration of Report Service subsystem in Oracle Enterprise Manager Ops Center.

The report service writes to the database every 1000 samples and retains the information for a defined amount of time. The default retention periods are Daily samples, 1 hour samples, 12 hour samples, and 24 hour samples. You can tune the report service to write to the database of samples.

You can configure the retention periods to change the number of days that data is retained or you can disable the roll up of data using the Report Service subsystem properties.

The following system properties are displayed for Report Service subsystem:

- **sample-retention-days:** Subsystem property to display the number of days that data is retained. Edit the number in the value field to set the number of days to a desired value.
- **repsvc.saves-bt-commits:** Subsystem property to increase or decrease the sample size. Set to a higher value to increase the sample size.

To disable the roll up of data, set the 1 hour samples, 12 hour samples, and 24 hour samples retention times to 0.

See [Related Resources for Configuration Management](#) for information on editing the Report Service subsystem property value.

About Server Pools Configuration

The Server Pools subsystem manages the migration script settings.

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.

The following system property is listed for Server Pools subsystem:

- **keep.migration.script:** Subsystem property to retain or discard the migration scripts. Set the value to `true` to retain the migration scripts and set the value to `false` to discard the migration scripts.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the Server Pools subsystem property value.

About Virtualization Configuration

The Virtualization subsystem manages the Oracle VM Server for SPARC failover settings.

In Oracle Enterprise Manager Ops Center, zone migration is a cold migration because the zone is shut down, all applications are stopped, the migration occurs, and then the zone is restarted. When you migrate a non-global zone with a network attached to the global zone, the software adds a router entry for the network on the destination zone. If the non-global zone has several different types of networks (such as management, public, and private) attached to the global zone, the software adds a router entry on the destination zone for each network. You can edit the Virtualization system property to disable this feature. When you disable the feature, a default router is not configured when creating or migrating a zone.

Oracle Enterprise Manager Ops Center UI provides the Migrate option to migrate the logical domains. Temporary user accounts are created dynamically when a logical domain migration is initiated. The user account is deleted after the migration. After creating a user account, you need to update the

Virtualization.Ldoms.Migration.Username system property in the Configuration tab with the user name.

The following properties are displayed for a Virtualization subsystem:

- **ZoneDefaultAddRouter:** Subsystem property to enable or disable configuring a default router when creating or migrating a zone. Set the value to `true` to enable

configuring a default router and set the value to `false` to disable configuring a default router.

- **Virtualization.Ldoms.Migration.Username:** Subsystem property to enter the user name that is to be used for all logical domain migration. Enter the user name in the value field.

Note: Do not modify the property settings unless directed by Oracle.

See [Related Resources for Configuration Management](#) for information on editing the Virtualization subsystem property value.

Related Resources for Configuration Management

List of Oracle Enterprise Manager Ops Center documents with additional information.

For more information, see these Oracle resources:

- For information on modifying the property of Auto Service Request subsystem, see [Blacklisting an Asset](#)
- For information on modifying the property of BUI subsystem, see [Displaying Related Assets In Groups](#)
- For information on defining the console access configuration subsystem property, see *Oracle Enterprise Manager Ops Center Configuration Reference*
- For information on modifying the properties of discovery subsystem, see the following sections in *Oracle Enterprise Manager Ops Center Configuration Reference*:
 - Service Tags
 - Preparing to Discover ALOM Assets
- For information on modifying the property of domain model navigator subsystem, see *Oracle Enterprise Manager Ops Center Security*
- For information on modifying the property of EC manager subsystem, see *Oracle Enterprise Manager Ops Center Security*
- For information on modifying the property of job manager subsystem, see *Oracle Enterprise Manager Ops Center Configuration Reference*
- For information on modifying the property of OCDoctor subsystem, see [Using Diagnostics Mode](#)
- For information on modifying the property of OS Provisioning subsystem, see the following sections:
 - [Generating a Default Set of OS Provisioning Profiles and Plans](#)
 - [Enabling or Disabling WAN Boot](#)
 - Provisioning Oracle Solaris 11 for information on setting SRU version
- For information on modifying the property of Proxy Manager subsystem, see [Enabling and Using Proxy Controller High Availability](#)

- For information on modifying the property of Report Service subsystem, see *Oracle Enterprise Manager Ops Center Sizing and Performance*
- For information on modifying the property of Server Pools subsystem, see [Retaining Migration Scripts in Server Pools](#)
- For information on modifying the property of Virtualization subsystem, see the following sections in *Oracle Enterprise Manager Ops Center Virtualization Reference*:
 - Migrating Zones
 - Setting User Accounts for Migration
- For Enterprise Controller installation procedure for Oracle Solaris OS, see *Oracle Enterprise Manager Ops Center Installation for Oracle Solaris Operating System*
- For Enterprise Controller installation procedure for Linux OS, see *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*
- For information on restoring an Enterprise Controller with an embedded database on a new system, see *Oracle Enterprise Manager Ops Center Restore an Enterprise Controller and Embedded Database on a New System*
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Manage the Database

Oracle Enterprise Manager Ops Center uses an Oracle Database 12c Enterprise Edition instance to store product data. You can manage this database.

This chapter includes the following sections:

- [Introduction to Database Management](#)
- [Roles for Database Management](#)
- [Actions for Database Management](#)
- [Location of Database Management Information in the User Interface](#)
- [Installing and Configuring a Customer-Managed Database](#)
- [Installing and Configuring Oracle 12CDB 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](#)
- [Related Resources for Database Management](#)

Introduction to Database Management

The Enterprise Controller uses an Oracle Database 12c 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 [Perform 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.

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.

Some of the procedures described in this section use the `ecadm` command. See [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.

Roles for Database Management

You require specific roles to perform database management tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 4-1 Database Management Tasks and Roles

Task	Role
Verify the database	Ops Center Admin
Change database credentials	Ops Center Admin

Actions for Database Management

You can perform various database management operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- Install a customer-managed database
- Configure a customer-managed database
- Migrate to customer-managed database from an embedded database
- Change the customer-managed database location
- Verify the database
- Upgrade the customer-managed database
- Change database credentials

- Defragment an embedded database
- Consolidate reports data on customer-managed database

Location of Database Management Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find database information in different locations.

Table 4-2 Location of Database Management Information in the UI

To See	Location
Database management actions	Expand Administration in the Navigation pane and select the Enterprise Controller.
View database credentials	Expand Administration in the Navigation pane and select the Enterprise Controller.

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 database is already installed. This procedure describes the steps to install and configure a customer-managed database.

1. Install the database according to the Oracle Database 12c release 1 (12.1.0.2.0) 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 12.1.0.2.0 Production on Mon Jul 27 13:11:20 2015

Copyright (c) 1982, 2014, Oracle. All rights reserved.

Connected to:
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Real Application Clusters, OLAP, Advanced Analytics 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 12c Enterprise Edition Release 12.1.0.2.0 -
64bit Production
With the Partitioning, Real Application Clusters, OLAP, Advanced Analytics and
Real Application Testing options

$

```

Installing and Configuring Oracle 12CDB Customer-Managed Database

If you want to use a customer-managed database running Oracle 12 multitenant container database (CDB), you must install and configure it to work with Oracle Enterprise Manager Ops Center.

This procedure assumes that the database is already installed. This procedure describes the steps to prepare the Oracle 12CDB customer-managed database for Oracle Enterprise Manager Ops Center installation.

1. Create a pluggable database (PDB) for the Oracle Enterprise Manager Ops Center schema where the database objects will be placed.
2. Create the following tablespaces in the PDB:
 - **Default tablespace:** This is the default tablespace for the Oracle Enterprise Manager Ops Center user. If the default tablespace does not exist, 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_remotePDB.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_remotePDB.sql.
Password:
createOCSchema_remotePDB.sql 100% |*****| 1486 00:00

```

4. As the database administrator, run the `createOCSchema_remotePDB.sql` script and enter the following information:

- **Oracle Enterprise Manager Ops Center pluggable database name:** This is a database to which the Oracle Enterprise Manager Ops Center connects to.
- **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:

```
[oracle@OAK0 OC_Scripts]
$ sqlplus '/as sysdba' @createOCSchema_remotePDB.sql
```

```
SQL*Plus: Release 12.1.0.2.0 Production on Mon Jul 27 13:11:20 2015
```

```
Copyright (c) 1982, 2014, Oracle. All rights reserved.
```

```
Connected to:
```

```
Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Real Application Clusters, OLAP, Advanced Analytics
and Real Application Testing options
```

```
"SQLTrace: Entering createOCSchema_remotePDB.sql"
Enter PDB name for Ops Center database login: PDB_ODAOCDB
Enter username for Ops Center database login: OC
Enter password for Ops Center database login:
Enter username for read only Ops Center database login: OC_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
```

The database properties file contains the location of the customer-managed database and a user name and password that can access the database. With Oracle 12CDB, the database service should point to the pluggable database service name. This 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>/<Pluggable database
service name>
```

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](#) or [Installing and Configuring Oracle 12CDB 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>
```

Note:

If you are using Oracle 12CDB customer-managed database, then the database service name should point to the pluggable database service name. For example: `mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<Pluggable 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 [Perform 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](#) or [Installing and Configuring Oracle 12CDB 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
...
mgmtdb.dburl=jdbc:oracle:thin:@<source database host name>:<port>/<source
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>)))
```

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

For example:

```
...
mgmtdb.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 12.1.0.2.0 - Production on Mon Jul 27 13:24:50 2015
Copyright (c) 1982, 2014, Oracle and/or its affiliates. All rights reserved.
Username: / as sysdba
<output omitted>
Job "SYS"."SYS_EXPORT_SCHEMA_01" successfully 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 12.1.0.2.0 - Production on Mon Jul 27 13:24:50 2015
Copyright (c) 1982, 2014, Oracle and/or its affiliates. All rights reserved.
Username: / as sysdba
<output omitted>
Job "SYS"."SYS_EXPORT_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. As root, log in to the Enterprise Controller system.

14. 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
#
```

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

For example:

```
$ rm OC_schema.dmp
```

Verifying the Database

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

For example:

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

```
./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 12c 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.

The following topics are covered:

- [Changing the Database Credentials for the Ops Center User](#)
- [Changing the Database Credentials for the Read-Only User](#)

Changing the Database Credentials for the Ops Center User

You can change the database credentials for the Ops Center user by using interactive mode or by using a password file.

This section describes the two methods to change the database credentials for the Ops Center user.

- Using interactive mode:

You can change the credentials by using the `ecadm` command with the `change-db-password` subcommand and the `-i` option.

For example:

```
# ./ecadm change-db-password -i
Changing the database password.
The Enterprise Controller will be restarted after the database password is
changed. Continue? (y/n)
y
Enter password:
Re enter password:
ecadm: --- Changed database password, restarting.
```

- Using password file:

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

You can change the database credentials for the read-only user by using interactive mode or by using a password file.

This section describes the two methods to change the database credentials for the read-only user.

- Using interactive mode:

You can change the credentials for a read-only user by using the `ecadm` command with the `change-db-password` subcommand and the `-i` and `-r` options.

For example:

```

# ./ecadm change-db-password -i -r
Changing the read-only database password. Continue? (y/n)
y
Enter password:
Re enter password:
ecadm:    --- Changed database password.

```

- Using password file:

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.

To defragment an embedded database, perform the following steps:

1. As root, log in to the Enterprise Controller system.
2. If you have a co-located Proxy Controller, use the `proxyadm` command with the `stop` subcommand and the `-w` option to first shut down the Proxy Controller.

For example:

```
./proxyadm stop -w
```

3. 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
#
```

4. 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`. The following options may be used with the `ecadm defrag-db` command:

- `-l|--logfile <logfile>`: Save output from command in `<logfile>`. Log files are stored in the `/var/tmp/sat-defrag-<date>-<time>.log` directory.
- `-T|--tempdir <dir>`: Specify the backup temporary staging directory location.
- `-d|--tempdir <dir>`: Specify the restore temporary staging directory location.

- **-v | --verbose:** Increase verbosity level (may be repeated)

For example:

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

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
#
```

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 or later 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 `OCDdoctor.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/OCDdoctor/OCDdoctor.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
#
```

Related Resources for Database Management

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For information on editing the `createOCSSchema_remote.sql` script to restrict the OC schema user from running certain commands on the database, see *Oracle Enterprise Manager Ops Center Security*
- For information on changing the OC Dump Directory, follow the procedure in [MOS document 1543144.1](#)
- For Enterprise Controller installation procedures, see *Oracle Enterprise Manager Ops Center Installation for Oracle Solaris Operating System* or *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*
- For information on restoring an Enterprise Controller with an embedded database on a new system, see *Oracle Enterprise Manager Ops Center Restore an Enterprise Controller and Embedded Database on a New System*
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Perform 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.

This chapter includes the following sections:

- [Introduction to General Administration](#)
- [Roles for General Administration](#)
- [Actions for General Administration](#)
- [Location of General Administration Information in the User Interface](#)
- [Viewing and Understanding Service Statuses](#)
- [Viewing Logs](#)
- [Adding a Product Alias](#)
- [Adding or Editing Authentications](#)
- [Editing the Energy Cost](#)
- [Related Resources for General Administration](#)

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 [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.

Roles for General Administration

You require specific roles to perform general administration tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 5-1 General Administration Tasks and Roles

Task	Role
View Service Status	Ops Center Admin
View Logs	Ops Center Admin
Add a Product Alias	Ops Center Admin
Add or Edit Authentications	Ops Center Admin
Edit the Energy Cost	Ops Center Admin

Actions for General Administration

You can perform various general administration operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- View service status
- View logs
- Add a product alias
- Add and edit authentications
- Edit the energy cost

Location of General Administration Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find general administration information in different locations.

Table 5-2 Location of General Administration Information in the UI

To See	Location
View Service Status	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Summary tab.
View Logs	Expand Administration in the Navigation pane and select the Enterprise Controller. Select the Logs tab.
Adding a Product Alias	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Add Product Alias in the Actions pane.

Table 5-2 (Cont.) Location of General Administration Information in the UI

To See	Location
Add or Edit Authentications	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Edit Authentications in the Actions pane.
Edit the Energy Cost	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Edit Energy Cost in the Actions pane.

Viewing and Understanding Service Statuses

The status of the Oracle Enterprise Manager Ops Center services is monitored and displayed in the UI.

Oracle Enterprise Manager Ops Center relies on the services listed in [Table 5-3](#). 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 5-3](#) shows the names, FMRI identifiers, and normal statuses of the Oracle Enterprise Manager Ops Center services.

Table 5-3 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

Table 5-3 (Cont.) Oracle Enterprise Manager Ops Center Services

Service Name	FMRI	Normal Status
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

You can view the status of the Oracle Enterprise Manager Ops Center services.

Follow this procedure to view the 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.

The following is the list of different logs which you can view:

- **Cacao log:** It provides logs for the agent running Enterprise Controller, Proxy Controller, Agent Controller, and Virtual Controller. It also provides the job execution startup error messages.
- **UI log:** It is the main log for Oracle Enterprise Manager Ops Center and provides log dedicated to the user interface to troubleshoot the user interface issues.
- **Proxy log:** It is a cacao log for the Proxy Controller and reports the operations invoked by the Proxy Controllers.
- **Update error log:** It provides reports on `server.cgi` downloads, authentications, daemon startups, and database connection issues.
- **Update channel download log:** It provides a specific download log for each channel. It reports the specific download job procedures.
- **Update channel error log:** It provides a specific error log for each channel. It reports authentications and network protocol connections.

This procedure describes the steps to view the logs.

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
 - 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.

To add a product alias, perform the following steps:

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.
The Energy Cost Settings window is displayed.
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.

Related Resources for General Administration

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For more information on viewing service requests, see *Oracle Enterprise Manager Ops Center Use Service Requests*
- For more information on administering concepts, see *Oracle Enterprise Manager Ops Center Administer Your Environment Using Oracle Enterprise Manager Ops Center*
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Manage the OCDoctor

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.

This chapter includes the following sections:

- [Introduction to the OCDoctor](#)
- [Roles for OCDoctor](#)
- [Actions for OCDoctor](#)
- [Location of OCDoctor Information in the User Interface](#)
- [Downloading the OCDoctor](#)
- [Performing Preinstallation Checks](#)
- [Performing Troubleshooting and Tuning](#)
- [Updating the OCDoctor](#)
- [Cleanup Through OCDoctor](#)
- [About Determining the Number of Asset Access Points](#)
- [Related Resources for OCDoctor](#)

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.

Roles for OCDoctor

You require specific roles to perform OCDoctor tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 6-1 OCDoctor Tasks and Roles

Task	Role
Preinstallation checks, troubleshoot and tuning, Update OCDoctor, and determine the number of access points	Ops Center Admin

Actions for OCDoctor

You can perform various OCDoctor operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- Download the OCDoctor
- Perform preinstallation checks
- Perform troubleshooting and tuning
- Update the OCDoctor
- Cleanup Through OCDoctor
- Determine the number of asset access points

Location of OCDoctor Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find OCDoctor information in different locations.

Table 6-2 Location of OCDoctor Information in the UI

To See	Location
To view the OCDoctor subsystem properties	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Configuration in the center pane. Select OCDoctor from the Subsystem drop-down.

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.

Follow this procedure to download the OCDoctor.

1. On an Internet-facing system, download the OCDoctor-LATEST.zip file. See [Related Resources for OCDoctor](#) for the link to download.
2. Move the downloaded file to the target system.
3. If the target system is an existing Enterprise Controller, Proxy Controller, or an Agent Controller, update the OCDoctor using the following command:

```
# /var/opt/sun/xvm/OCDoctor/OCDoctor.sh --update --
file /var/tmp/OCDoctor-latest.zip
```

4. If the target system is a new system, unzip the file and run the OCDoctor.sh script to see the available options.

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.

Follow this procedure to perform the preinstallation checks.

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 4.46 [OC 12.3.0.604,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-wsl.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-wsl.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.

Follow this procedure to 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 4.46 [OC 12.3.0.604,SunOS11] [Read only] [09-Mar-2015 09:22AM
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.

This procedure describes the steps to update the OCDoctor.

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 4.46 [OC 12.3.0.604,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: 4.46, online:
4.46).

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

Note: You can also run the `OCDoctor.sh` script with the `--update` option on Proxy Controllers and Agent Controllers. When you run the `OCDoctor.sh` script with the `--update` on Proxy Controllers and Agent Controllers, it fetches the `OCDoctor` from the Enterprise Controller.

Cleanup Through ODDoctor

To free up the disk space, you can use the `OCDoctor` cleanup feature with `OCDoctor` 4.54 version.

The `./OCDoctor.sh --cleanup` script is used to scan the Enterprise Controller, Proxy Controller, and Agent Controller traces of Oracle Enterprise Manager Ops Center that can be safely removed to free up the disk space.

For example:

```
# /var/opt/sun/xvm/OCDoctor/OCDoctor.sh --cleanup
Cleaning up Ops Center Enterprise Controller Version 12.3.0.1407

List of files/directories to get removed / cleaned up:

/var/opt/sun/xvm/EnterpriseController_installer_12.2.0.2663
/var/opt/sun/xvm/update-saved-state/update_EC_minor_bundle_12.2.2.1103
...
/var/opt/sun/xvm/images/agent/OpsCenterAgent.Solaris.sparc.12.2.0.2663.zip
/var/opt/sun/xvm/images/agent/OpsCenterAgent.Solaris.sparc.12.2.0.2663.zip.sig
/var/opt/sun/xvm/images/agent/OpsCenterAgent.SolarisIPS.all.12.2.0.2663.zip
/var/opt/sun/xvm/images/agent/OpsCenterAgent.SolarisIPS.all.12.2.0.2663.zip.sig

Total size of files/directories = 32774052 KB / 32005.9 MB / 31.3 GB

Ensure that there is no OS Provisisoning Job running using this Proxy Controller
right now!

Please review the list and press <ENTER> to continue or ^C to abort ...

Deleting items, please be patience ..... done
```

Note: In case of further Boot Environments, you may not see any increase in free disk space until the other BEs got destroyed!

About Determining 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.

Note:

Starting from 12.3.1 version, you can view the access point count for the Enterprise Controller and the Proxy Controllers in the user interface. For more information, see [Viewing and Removing Access Points](#).

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](#)
- [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
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
```

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/OCDocctor/toolbox/AssetCount.sh all
```

For example:

```
# /var/opt/sun/xvm/OCDocctor/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 S1lzone101 S1lzone102 S1lzone100 S1lzone103 S1lzone104
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.

Related Resources for OCDocctor

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- To download the OCDocctor-LATEST.zip file, go to <https://updates.oracle.com/OCDocctor/OCDocctor-latest.zip>
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Manage 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.

This chapter includes the following sections:

- [Introduction to ASR](#)
- [Roles for ASR](#)
- [Actions for ASR](#)
- [Location of ASR Information in the User Interface](#)
- [Viewing ASR Status for an Asset](#)
- [Providing Contact Information](#)
- [Enabling ASR](#)
- [Disabling ASR](#)
- [Blacklisting an Asset](#)
- [Testing ASR](#)
- [Moving Assets from Standalone ASR to Oracle Enterprise Manager Ops Center ASR](#)
- [Related Resources for Auto Service Request](#)

Introduction to ASR

Oracle Enterprise Manager Ops Center can use ASR to generate service requests based on known issues.

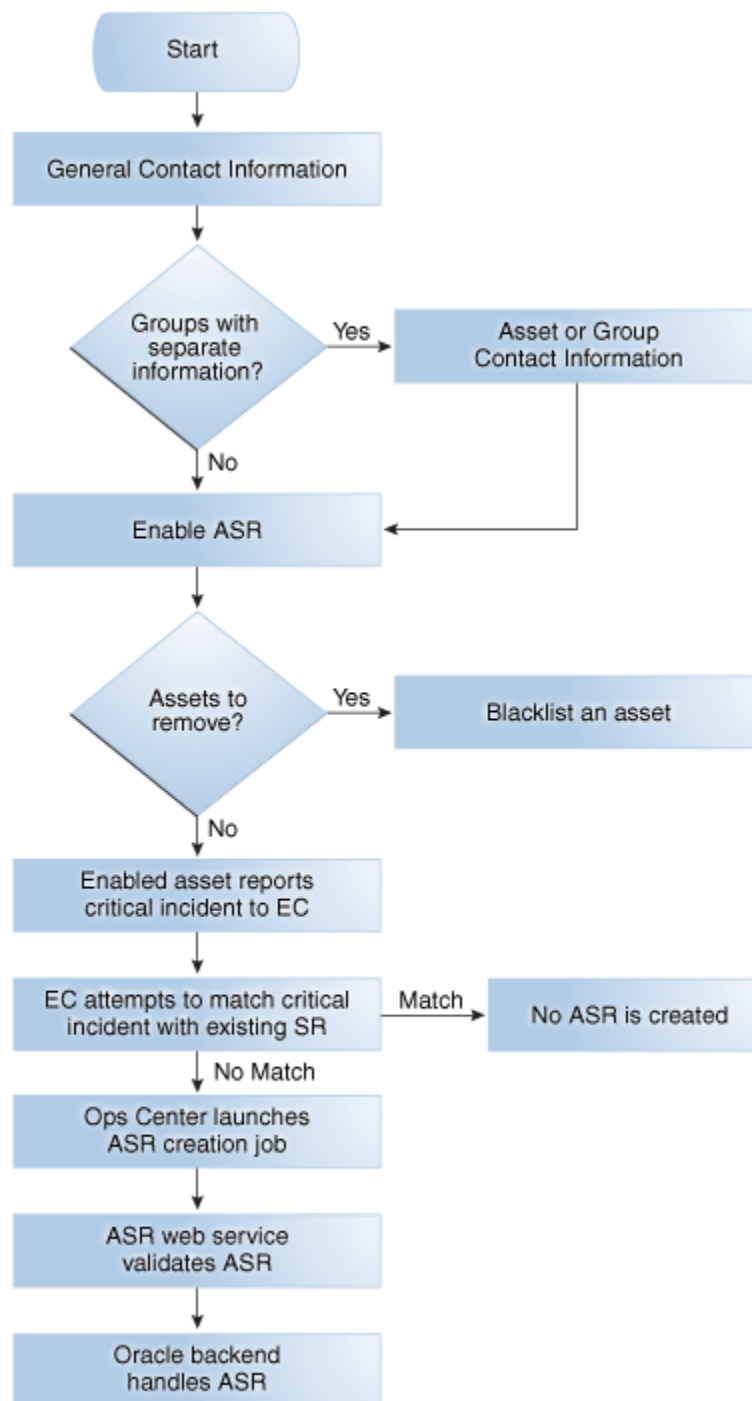
By providing contact information for your assets and enabling ASR, you enable the creation of service requests whenever a new critical incident occurs.

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 7-1 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 My Oracle Support page and log in to verify that your assets are present in MOS. See [Related Resources for Auto Service Request](#) for the link to log in.

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.

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.

Note:

Starting with version 12.3.2, Oracle Enterprise Manager Ops Center can process SNMPv3 fault alerts which uses credentials instead of a public community string for communication exchanges. For more information about SNMPv3, see *Oracle Enterprise Manager Ops Center Configuration Reference*.

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.

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.

Roles for ASR

You require specific roles to perform ASR tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 7-1 ASR Tasks and Roles

Task	Role
Enable or disable ASR	Ops Center Admin
Blacklist ASR	Ops Center Admin
Test ASR	Ops Center Admin

Actions for ASR

You can perform various ASR operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- View ASR status for an asset
- Provide default contact information
- Provide contact information for an asset or group

- Enable ASR
- Disable ASR
- Blacklist an ASR
- Test ASR

Location of ASR Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find information of ASR in different locations.

Table 7-2 Location of ASR Information in the UI

To See	Location
View ASR Status for an Asset	Expand Assets in the Navigation pane and then select Service Requests tab.
Edit ASR Contact Information	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Edit ASR Default Contact in the Actions pane.
Enable ASR/Disable ASR	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Enable ASR/Disable ASR in the Actions pane.

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.

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.

Follow this procedure to provide default contact information.

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.

Follow this procedure to provide contact information for an asset or a 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

You can enable ASR to automatically generate service requests for your assets when a qualified incident occurs.

Follow this procedure to enable ASR.

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.

Follow this procedure to disable ASR.

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. Follow this procedure to test ASR.

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.

Moving Assets from Standalone ASR to Oracle Enterprise Manager Ops Center ASR

You can move the assets from a Standalone ASR to Oracle Enterprise Manager Ops Center and from Oracle Enterprise Manager Ops Center to a Standalone ASR.

Note: To move assets from a Standalone ASR to Oracle Enterprise Manager Ops Center, delete the assets in the Standalone ASR and discover these assets in the Oracle Enterprise Manager ASR.

To move assets from a Standalone ASR to Oracle Enterprise Manager Ops Center ASR:

1. Log in to Oracle ILOM CLI, disable the SNMP trap destinations rule pointing to the ASR manager by using the following command:

```
set /SP|CMM/alertmgmt/rules/n level=disable
```

2. Log in to ASR Manager as a root and run the following command to deactivate every asset:

```
asr deactivate_asset
```

3. Discover the assets in Oracle Enterprise Manager Ops Center.
4. Enter the MOS credentials for the discovered assets as described in [Adding or Editing Authentications](#).

Note: To move assets from Oracle Enterprise Manager Ops Center to a Standalone ASR, delete the assets in Oracle Enterprise Manager Ops Center and discover these assets in a Standalone ASR.

Related Resources for Auto Service Request

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For My Oracle Support page, go to <https://support.oracle.com>
- See the following chapters in the *Oracle Enterprise Manager Ops Center Configuration Reference*:
 - See Manage Assets for information about adding credentials
 - See About Discovering Assets for information about discovering assets
 - See Deleting Assets for information about deleting assets
 - See Configure Storage for information about enabling assets with embedded ASR support
- For information on Oracle Auto Service Request Documentation on Fault Coverage reports, see http://docs.oracle.com/cd/E37710_01/nav/faultcoverage.htm
- For information on 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>
- For information on Oracle Auto Service Request Documentation on Products Qualified for ASR, see http://docs.oracle.com/cd/E37710_01/nav/products.htm
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Manage the Users and Roles

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.

This chapter includes the following sections:

- [Introduction to User and Role Management](#)
- [Roles for User and Role Management](#)
- [Actions for User and Role Management](#)
- [Location of User and Role Management Information in the User Interface](#)
- [Adding a User](#)
- [Deleting a User](#)
- [Viewing User Role Details](#)
- [Adding a Directory Server](#)
- [About Synchronizing Remote Users and Roles](#)
- [Deleting a Directory Server](#)
- [About Roles and Permissions](#)
- [Managing Roles](#)
- [Replicating a User](#)
- [About Notification Profiles](#)
- [Viewing the Audit Log](#)
- [Related Resources for User and Role Management](#)

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.

Roles for User and Role Management

You require specific roles to manage users and roles in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 8-1 User and Role Management Tasks and Roles

Task	Role
Add, replicate, or delete a user	Ops Center Admin
View user role details	Ops Center Admin
Add or delete a directory server	Ops Center Admin
Synchronize remote users and roles	Ops Center Admin
Manage Roles	Ops Center Admin
Configure or delete a notification profile	Ops Center Admin
Ops Center Admin	Ops Center Admin

Actions for User and Role Management

You can perform several user and role management operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- Add a user
- Delete a user
- View user role details
- Add a directory server
- Synchronize remote users and roles

- Deleting a directory server
- Manage roles
- Replicate a user
- Configure a Notification Profile
- Delete a Notification Profile
- View the audit log

Location of User and Role Management Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find users and roles information in different locations.

Table 8-2 Location of User and Role Management Information in the UI

To See	Location
View/Add/Replicate/Delete a user	Expand Administration in the Navigation pane and select Local Users.
View/Add/Modify/Delete Directory Servers	Expand Administration in the Navigation pane and select Directory Servers.
View/Update Credentials	Expand Administration in the Navigation pane and select Credentials.
Sync Remote Users and Roles	Expand Administration in the Navigation pane and select Directory Servers.
Manage Roles	Expand Administration in the Navigation pane and select the Roles tab in the center pane.
Configure or delete a Notification Profiles	Expand Administration in the Navigation pane and select Local Users.

For more details on Credentials, see <Config Guide>.

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.

To add a user, perform the following steps:

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.

To delete a user, perform the following steps:

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.

To view user role details, perform the following steps:

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**.

About Synchronizing Remote Users and Roles

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

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

Note:

Oracle Enterprise Manager Ops Center does not support synchronizing active directory servers.

Synchronizing Remote Users and Roles With One Directory Server

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

To synchronize Oracle Enterprise Manager Ops Center with a single directory server, perform the following steps:

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.

To synchronize Oracle Enterprise Manager Ops Center with all known directory servers, perform the following steps:

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.

To delete a directory server, perform the following steps:

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

Some of the permissions are mapped to the roles.

[Table 8-3](#) shows the permissions granted by each role.

Table 8-3 Roles and Permissions

Table 8-3 (Cont.) 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 8-3 (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
	Virtualization Guest Creation
	Virtualization Guest Deletion
	Virtualization Guest Management
	Virtualization Guest Usage
	Virtualization Host Management
	Virtualization Host Usage
	Write Access

Table 8-3 (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 8-3 (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 8-3 (Cont.) Roles and Permissions

Role	Permissions
Plan/Profile Admin	Plan/Profile Management Read Access Write Access
Proxy Controller Admin	Proxy Controller Management Write Access Read 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 8-3 (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 8-3 (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 8-3 (Cont.) Roles and Permissions

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

Table 8-3 (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 Virtualization Guest Usage Virtualization Host Creation Virtualization Host Deletion Virtualization Host Management Virtualization Host Usage Write Access

How Permissions are Mapped to Tasks

Some of the permissions are mapped to tasks.

[Table 8-4](#) shows the tasks that a user with a given permission can perform.

Table 8-4 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
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

Table 8-4 (Cont.) Permissions and Tasks

Permission	Tasks
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
Cloud Control Management	Configure/Connect Disconnect/Unconfigure Cloud Control Console
Windows Update Management	Unconfigure SCCM Configuration

Table 8-4 (Cont.) Permissions and Tasks

Permission	Tasks
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

Table 8-4 (Cont.) Permissions and Tasks

Permission	Tasks
EC Local Agent Management	Configure Local Agent Unconfigure Local Agent
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

Table 8-4 (Cont.) Permissions and Tasks

Permission	Tasks
Virtualization Guest Creation	Create Logical Domains Create zones Create OVM virtual servers
Virtualization Guest Deletion	Delete Logic Domain Delete Zones Delete OVM Virtual Servers
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

Table 8-4 (Cont.) Permissions and Tasks

Permission	Tasks
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
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.

To grant users different roles and privileges, perform the following steps:

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.
3. Select the source user from the list of users.
4. Click the **Replicate User Roles** icon.

The users are 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.

To receive notifications, a user must have either of the following roles assigned.

- To receive notifications about all the assets, a user must have an Ops Center Admin role.
- To receive notifications only about the assets in a specific user-defined group, a user must have a Read role. When assigning the Read role to a user, uncheck the **Use the default Role associations** option to apply the role only to specific groups.

Note:

To receive email notifications about assets, a user must have a Read role. You can receive email notifications either in HTML or plain text format by using the `alert.mail.format` property. See [About EC Manager Configuration](#) for more information on how to set the property value to receive email notification in HTML or plain text format.

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.

To configure a new notification profile for a user or to 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.

Note: The name of the asset that caused the notification appears in the subject of the email.

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.

To delete a notification profile, perform the following steps:

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.

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>`.

Related Resources for User and Role Management

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For more information on audit logs, see *Oracle Enterprise Manager Ops Center Configuration Reference*
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Perform 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.

This chapter includes the following sections:

- [Introduction to Backup and Recovery](#)
- [Roles for Backup and Recovery](#)
- [Actions for Backup and Recovery](#)
- [Location of Backup and Recovery Information in the User Interface](#)
- [Backing Up and Restoring an Enterprise Controller](#)
- [Backing Up and Restoring a Proxy Controller](#)
- [Related Resources for Backup and Recovery](#)

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 `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 you are restoring the Enterprise Controller on a new system, you must verify that the new system is compatible.

- 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 host name of the new system should be the same as the old system. You can change the host name of the new system, provided the old host name is added as an alias host name in the new system.
- The IP address of the new system can be different. If the new system has a different IP address, the restore process includes a step to configure any remote Proxy Controllers to use the new Enterprise Controller IP address. The MAC address of the new system can be different.
- The new system's Enterprise Controller software version must also match those of the backed up system.

For a regular back up and restore procedure, the IP address and the host name of the new system should match that of the old system. For a disaster recovery procedure, the IP address and the host name of the new system can be different than that of the old system.

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 [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.

Roles for Backup and Recovery

You require specific roles to perform backup and recovery tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 9-1 Backup and Recovery Tasks and Roles

Task	Role
Backup and Restore an Enterprise Controller	Ops Center Admin
Backup and Restore an Proxy Controller	Ops Center Admin

Actions for Backup and Recovery

You can perform various backup and recovery operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- Backup an Enterprise Controller

- Restore an Enterprise Controller
- Backup an Proxy Controller
- Restore an Proxy Controller

Location of Backup and Recovery Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find information of Backup and Recovery in different locations.

Table 9-2 Location of Backup and Recovery Information in the UI

To See	Location
Back up or Restore Enterprise Controller	Command Line
Back up or Restore Proxy Controller	Command Line

Backing Up and Restoring an Enterprise Controller

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

Following topics are covered:

- [Backing Up an Enterprise Controller](#)
- [Restoring 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.

Note:

The `ecadm backup` command does not back up the `/var/opt/sun/xvm/locallib/` local library and `/var/opt/sun/xvm/images/os` directory.

In addition to running the `ecadm backup` command, you should back up the `/var/opt/sun/xvm/locallib/` local library and `/var/opt/sun/xvm/images/os` directory and manually archive the files to another server, file-share facility, or a location outside of the `/var/opt/sun` directory.

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. Stop the Enterprise Controller by running the `ecadm` command with the `stop` subcommand and the `-w` option.

For example:

```
ecadm stop -w
```

3. 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`.
- **-l | --logfile <logfile>**: Save output from command in `<logfile>`. Log files are stored in the `/var/tmp/` 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
```

4. Copy the backup file to a separate system.
5. Start the Enterprise Controller by running the `ecadm` command with the `start` subcommand and the `-w` option.

For example:

```
ecadm start -w
```


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 describes the steps for disaster recovery. It restores the data from the backup file, which is the archive created by the `ecadm backup` operation. It also defines the procedure to change the host name and the IP address of an Enterprise Controller.

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 do not use this option to restore the Enterprise Controller without restoring the database.

Note: Before you restore on a system, you must uninstall any previously existing Enterprise Controllers, Proxy Controllers, and Agent Controllers from the system.

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 the host name does not match, add the old host name as an alias to the `/etc/hosts` file.
 - 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
```

2. Install the Enterprise Controller to the same version that was running when the backup was made, but do not configure the Enterprise Controller, as the `ecadm restore` command restores your configuration settings.

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. 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.
- **-l | --logfile <logfile>**: Save output from command in <logfile>. Log files are stored in the `/var/tmp/` 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 co-located Proxy Controller should not be restored.
- **-d | --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
```

4. For an Enterprise Controller with an enabled co-located Proxy Controller, the restore should restore and start the co-located Proxy Controller. The co-located Proxy Controller starts only if the Proxy Controller was enabled during the backup procedure. Check the co-located 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
#
```

5. If you restored the Enterprise Controller on a new system, restart each remote Proxy Controller to use the new Enterprise Controller.

- a. Stop the Proxy Controller using the `proxyadm` command with the `stop` subcommand and the `-w` option. For example:

```
# proxyadm stop -w
```

- b. On the remote Proxy Controller, update the `/var/opt/sun/xvm/persistence/scn-proxy/connection.properties` URL property to point to the IP address of the new Enterprise Controller. Update this URL property through the command line interface using the `proxyadm` command with the `update` subcommand and the `-s` option:

```
proxyadm update -s|--satellite-ip <ip>
```

- c. Restart the Proxy Controller using the `proxyadm` command with the `start` subcommand and the `-w` option. For example:

```
# proxyadm start -w
```

6. Restart the co-located Agent Controllers using the `agentadm` command with the `start` subcommand and the `-w` option. For example:

```
/opt/SUNWxvmoc/bin/agentadm start -w
```

Note:

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

Note:

During the database schema restore, an import log is created. The name of the import log appears in the Enterprise Controller restore log file with the `OC_import<timestamp>.log` format. You can check the progress of the database import status using this import log.

Example 9-1 Restoring an Enterprise Controller With an Embedded Database

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

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.

Example 9-2 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 9-3 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.

The following topics are covered:

- [Backing Up a Proxy Controller](#)
- [Restoring a Proxy Controller](#)

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`.
- `-l | --logfile <logfile>`: Save output from command in `<logfile>`. Log files are stored in the `/var/tmp/` 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.
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.
- `-l|--logfile <logfile>`: Save output from command in `<logfile>`. Log files are stored in the `/var/tmp/` 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
```

Related Resources for Backup and Recovery

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For more information on installing Enterprise Controller, see *Oracle Enterprise Manager Ops Center Installation for Oracle Solaris Operating System* or *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*
- For information on restoring Enterprise Controller with an embedded database on a new system, see *Oracle Enterprise Manager Ops Center Restore an Enterprise Controller and Embedded Database on a New System*
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Manage 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.

This chapter includes the following sections:

- [Introduction to High Availability](#)
- [Roles for High Availability](#)
- [Actions for High Availability](#)
- [Location of High Availability Information in the User Interface](#)
- [About Enabling and Using Enterprise Controller High Availability](#)
- [Enabling and Using Proxy Controller High Availability](#)
- [Related Resources for 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 [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.

About Enterprise Controller High Availability

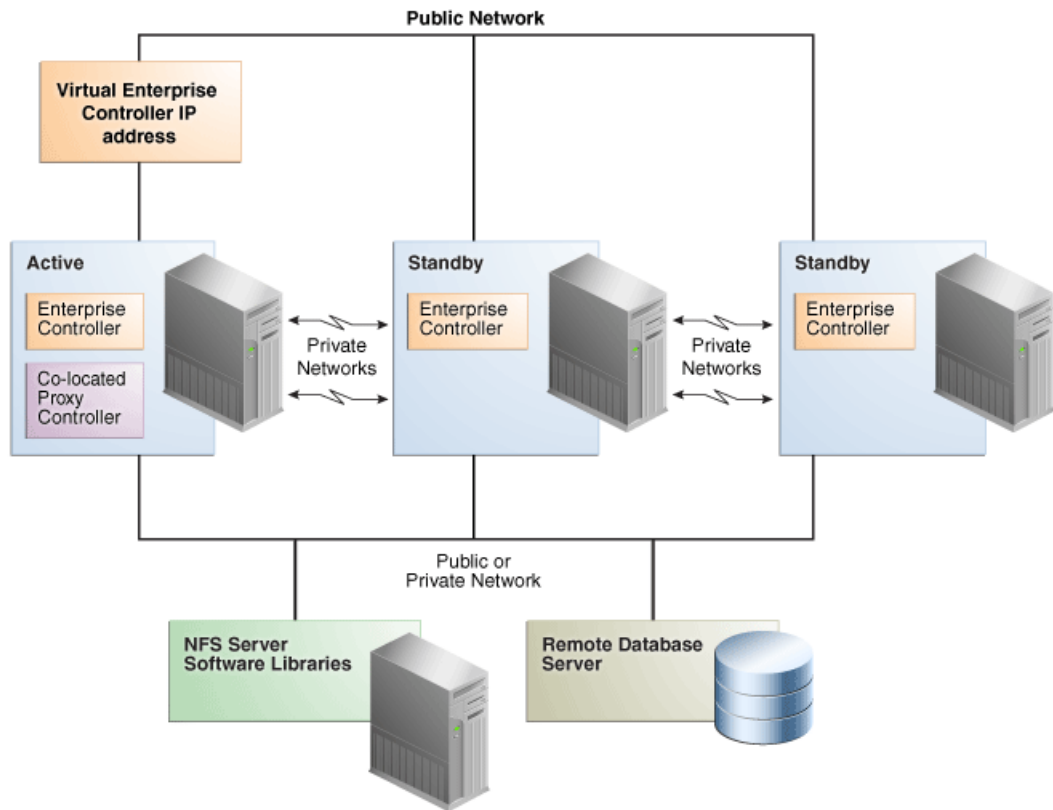
High Availability is a setup involving multiple Enterprise Controllers using Oracle Clusterware and a remote database.

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 10-1 shows an example Enterprise Controller High Availability configuration.

Figure 10-1 Enterprise Controller High Availability Configuration



Note:

If you have not yet installed Oracle Enterprise Manager Ops Center, make sure to install it 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==12.3.0.604
product.installLocation=/var/opt/sun/xvm/
EnterpriseController_installer_=12.3.0.604
#
```

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.

About 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.

Roles for High Availability

You require specific roles to perform high availability tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 10-1 High Availability Tasks and Roles

Task	Role
Enable or disable Enterprise Controller High Availability	Ops Center Admin
Enable or disable Proxy Controller High Availability	Ops Center Admin
Enable or disable Automatic Failover for Proxy Controller	Ops Center Admin
Set relative power for Proxy Controller	Ops Center Admin

Actions for High Availability

You can perform various High Availability operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- Enable Enterprise Controller High Availability
- Convert a Single Enterprise Controller to High Availability
- Convert a High Availability Configuration to a Single Enterprise Controller
- Relocate from the current Enterprise Controller to a standby Enterprise Controller manually
- Manage HA Network Resources
- Remove a Standby Enterprise Controller Node
- Check the Status of the Enterprise Controller Cluster
- Shut Down the Enterprise Controller Temporarily Without Relocating
- Access the Cluster Management UI
- Enable Proxy Controller High Availability
- Enable Automatic Failover for a Proxy Controller

- Disable Automatic Failover for a Proxy Controller
- Set relative power for Proxy Controller
- Recover after an Automatic Failover for a Proxy Controller
- Migrate assets between Proxy Controllers
- Migrate assets from a failed Proxy Controller

Location of High Availability Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find High Availability information in different locations.

Table 10-2 Location of High Availability Information in the UI

To See	Location
Enterprise Controller High Availability	Expand Administration in the Navigation pane and select the Enterprise Controller. In the Configuration tab and select EC Manager.
View Cluster Management UI	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Manage Cluster Configuration in the Actions pane.
Proxy Controller High Availability	Expand Administration in the Navigation pane and select the Enterprise Controller. In the Configuration tab and select Proxy Manager.
Migrate assets between Proxy Controllers	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Manage Assets tab.

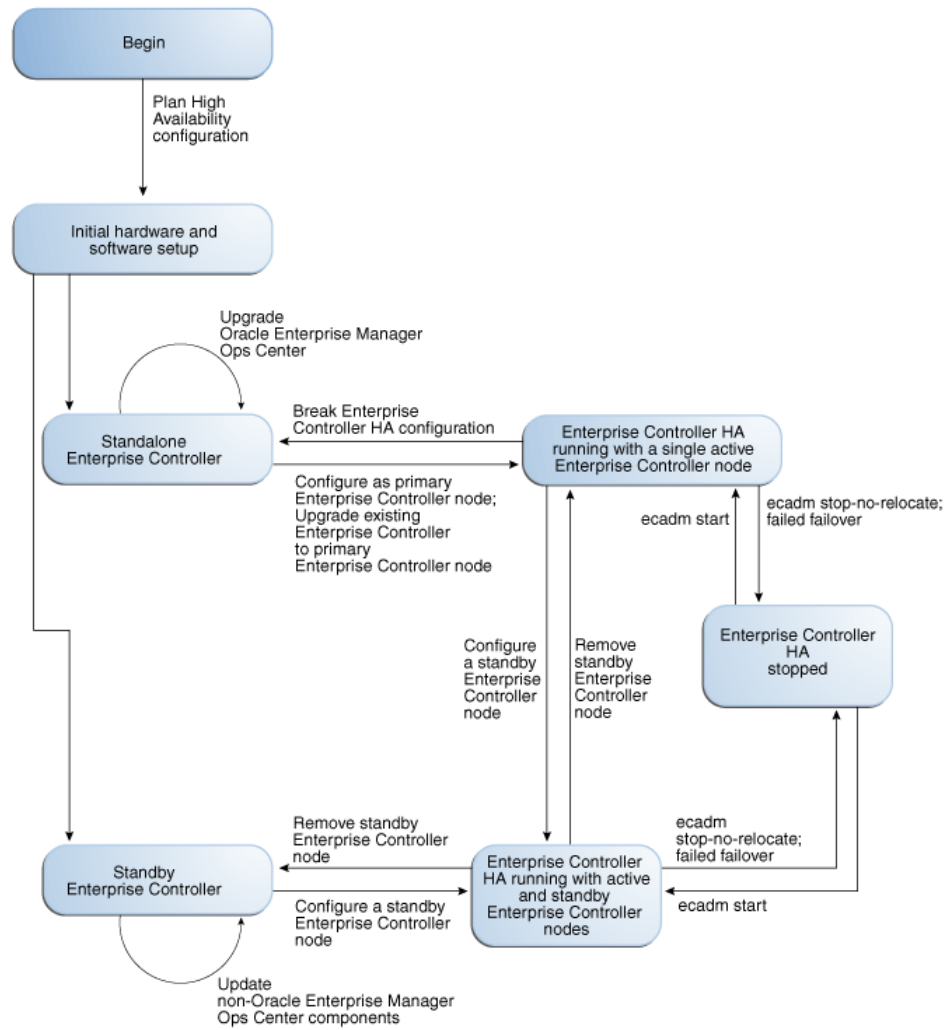
About Enabling and Using Enterprise Controller High Availability

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 10-2](#) shows the possible states of an Enterprise Controller High Availability configuration and the steps needed to move between them.

Figure 10-2 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.

The procedure described in this section assumes that you have already installed and configured a single Enterprise Controller.

Preparing for High Availability with Oracle Clusterware

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

To install and configure Oracle Clusterware, perform the following steps:

1. Install Oracle Clusterware in your environment using the Grid Infrastructure Installation Guide.
2. If you are using a local database, switch to a remote database. See [Manage the Database](#) for more information.

Making the Current Enterprise Controller as the Primary Node

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

To configure the current Enterprise Controller as the primary node, perform the following steps:

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/doHStart() starting resource='EnterpriseController'
on node='primary-system'
INFO: HAECClusterwareAdapter/doHStart()statusSB='CRS-2672: Attempting to start
'EnterpriseController' on 'primary-system'
CRS-2676: Start of 'EnterpriseController' on 'primary-system' succeeded'
INFO: HAECClusterwareAdapter/doHStart() 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.

To install and configure standby nodes, perform the following steps:

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.i386.12.3.0.604.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.i386.12.3.0.604.zip
# ls
enterprise-controller.Solaris.i386.12.3.0.604.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.i386.12.3.0.604.tar.zip | tar xf -
# ls
enterprise-controller.Solaris.i386.12.3.0.604.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=TCPS)(HOST=<host>)
(PORT=<port>))(CONNECT_DATA=(SERVICE_NAME=<service>)))
```

Note: If you are using an Oracle 12CDB customer-managed database, then the database service name should point to the pluggable database service name. For example: `mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<Pluggable database service name>`. See [Installing and Configuring Oracle 12CDB Customer-Managed Database](#) for more information on preparing the Oracle 12CDB customer-managed database for Oracle Enterprise Manager Ops Center installation.

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 12.3.0.604 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/doHAStatus() 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.

To convert your High Availability configuration to a single Enterprise Controller, perform the following steps:

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.

To manually relocate from the current Enterprise Controller to a standby Enterprise Controller, perform the following steps:

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.

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_DIS  
CONNECT=false,USR_ORA_PRECONNECT=none,HOSTING_MEMBERS=<node1>:<n  
ode2>
```

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`

Modifying a Network Resource Timeout Value

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

The default timeout value required by an Enterprise Controller to perform different actions such as, start, stop, check, and clean is 900 seconds. If the Enterprise Controller takes more than 900 seconds to perform any of these actions, then the timeout value can be modified to accommodate the actual time in seconds required by the Enterprise Controller to perform any of the action.

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

```
./crsctl modify resource EnterpriseController -attr "START_TIMEOUT=<time in seconds>, STOP_TIMEOUT=<time in seconds>, SCRIPT_TIMEOUT=<time in seconds>"
```

For example:

```
./crsctl modify resource EnterpriseController -attr "START_TIMEOUT=1800, STOP_TIMEOUT=1800, SCRIPT_TIMEOUT=1800"
```

The following attributes can be modified:

- `START_TIMEOUT=<time in seconds>`: The maximum time in which a start action can run. Oracle Clusterware returns an error message if the action does not complete within the time specified. If you do not specify a value for this attribute or you specify 0 seconds, then Oracle Clusterware uses the value of the `SCRIPT_TIMEOUT` attribute.
- `STOP_TIMEOUT=<time in seconds>`: The maximum time in which a stop or clean action can run. Oracle Clusterware returns an error message if the action does not complete within the time specified. If you do not specify this attribute or if you specify 0 seconds, then Oracle Clusterware uses the value of the `SCRIPT_TIMEOUT` attribute.
- `SCRIPT_TIMEOUT=<time in seconds>`: The maximum time for an action to run. Oracle Clusterware returns an error message if the action script does not complete within the time specified. The timeout applies to all actions.

To double the default timeout value of the Enterprise Controller, we can use the timeout value as 1800 seconds. However, this value may be excessive if the Enterprise Controller uses less than 1800 seconds to perform an action. You can modify the timeout value of these attributes individually or all at the same time, depending on the timeout value required by each attribute.

Removing a Standby Enterprise Controller Node

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

To remove a standby Enterprise Controller node from the cluster, perform the following steps:

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.

To check the status of the cluster from any Enterprise Controller node, perform the following steps:

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.

To shutdown the Enterprise Controller temporarily without relocating, perform the following steps:

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.

To view the cluster configuration from the user interface, perform the following steps:

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.

To disable automatic failover, perform the following steps:

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 [Manage 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 [Removing Access Points](#) for more information.

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.

To migrate assets between Proxy Controllers, perform the following steps:

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.

Removing Access Points

When a Proxy Controller fails, the assets from the failed Proxy Controller can be migrated to the desired Proxy Controllers. After migration, if the old Proxy Controller is expected to be back online, then you must delete the access point from the old Proxy Controller.

To manually remove the access point from an old Proxy Controller:

1. Click **Assets** in the Navigation pane and select the asset.
2. Click the **Configuration** tab.

The Access Points are displayed in the center pane. Select the specific Access Point to delete.

3. Click the **Delete Access Point** icon.

Related Resources for High Availability

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For more information on installing Enterprise Controller High Availability, see *Oracle Enterprise Manager Ops Center Installation for Oracle Solaris Operating System* or *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*
- For information on installing Oracle Clusterware, see [Grid Infrastructure Installation Guide for Oracle Solaris Systems](#) or [Grid Infrastructure Installation Guide for Linux Systems](#)
- For information on Clusterware `crsctl` command and network resources status, see [Oracle Clusterware Administration and Deployment Guide 11g Release 2](#)
- For information about deleting access points, see *Oracle Enterprise Manager Ops Center Configuration Reference*
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Perform Upgrades

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.

This chapter includes the following sections:

- [Introduction to Upgrade](#)
- [Roles for Upgrade](#)
- [Actions for Upgrade](#)
- [Location of Upgrade Information in the User Interface](#)
- [Versions Supported for Upgrade](#)
- [Planning the Upgrade](#)
- [Database Requirements](#)
- [Upgrading Your Environment](#)
- [Related Resources for Upgrade](#)

Introduction to Upgrade

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 [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.

Roles for Upgrade

You require specific roles to perform upgrade tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 11-1 Upgrade Tasks and Roles

Table 11-1 (Cont.) Upgrade Tasks and Roles

Task	Role
Upgrading Enterprise Controller High Availability	Ops Center Admin
Upgrading Proxy Controller	Ops Center Admin
Upgrading Agent Controller	Ops Center Admin

Actions for Upgrade

You can perform various upgrade operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- Upgrade from version 12.3
- Upgrade from version 12.2
- Upgrade from version 12.1
- Upgrade from version 11g

Location of Upgrade Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find upgrade information in different locations.

Table 11-2 Location of Upgrade Information in the UI

To See	Location
Download Upgrades	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Ops Center Downloads in the Actions pane.
Upgrade Enterprise Controller	Expand Administration in the Navigation pane and select the Enterprise Controller. Select Upgrade Enterprise Controllers in the Actions pane.
Upgrade Enterprise Controllers	Expand Administration in the Navigation pane and select the Proxy Controllers tab. Select Upgrade to Latest Available Version icon in the center pane.
Upgrade Agent Controllers	Expand Assets in the Navigation pane and select All Assets. Select an asset or a group.

Versions Supported for Upgrade

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

This section details the supported upgrade paths.

The following topics are covered:

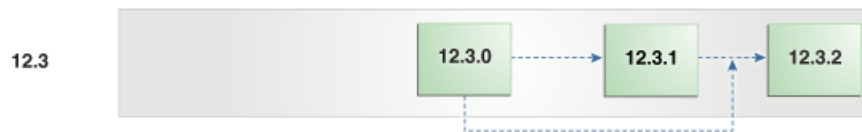
- [Upgrading From Version 12.3](#)

- [Upgrading From Version 12.2](#)
- [Upgrading From Version 12.1](#)
- [Upgrading From Version 11g](#)

Upgrading From Version 12.3

Use the following upgrade path when you are upgrading from Oracle Enterprise Manager Ops Center 12.3.0 to later versions.

If you are currently using version 12.3.0 or 12.3.1, you can upgrade directly to version 12.3.2.

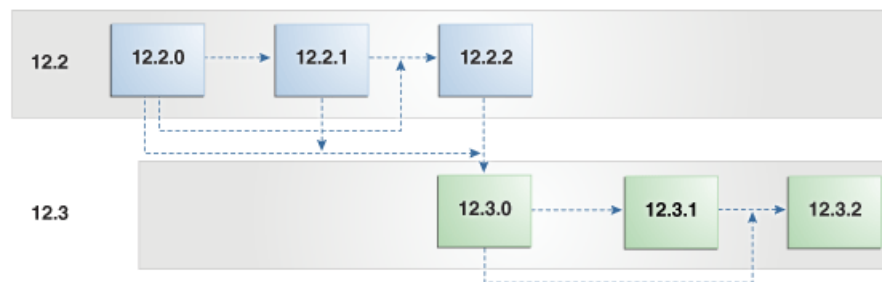


Upgrading From Version 12.2

Use the following upgrade path when you are upgrading from Oracle Enterprise Manager Ops Center 12.2 to later versions.

If you are currently using version 12.2.0, 12.2.1, or 12.2.2, you can upgrade to version 12.3.0, and finally upgrade to the latest version.

Figure 11-1 Supported Upgrade Paths From Version 12.2

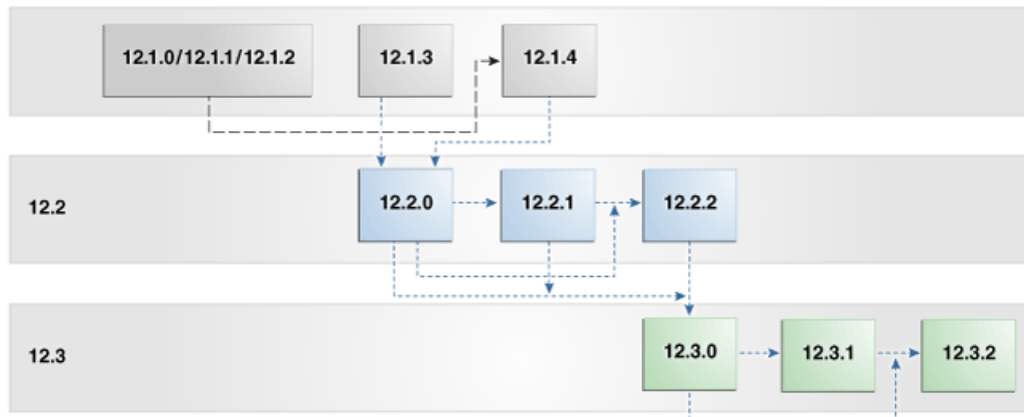


Upgrading From Version 12.1

Use the following upgrade path when you are upgrading from Oracle Enterprise Manager Ops Center 12.1 to later versions.

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, then upgrade to version 12.3.0, and finally upgrade to the latest version.

Figure 11-2 Supported Upgrade Paths From Version 12.1



You must upgrade in this order:

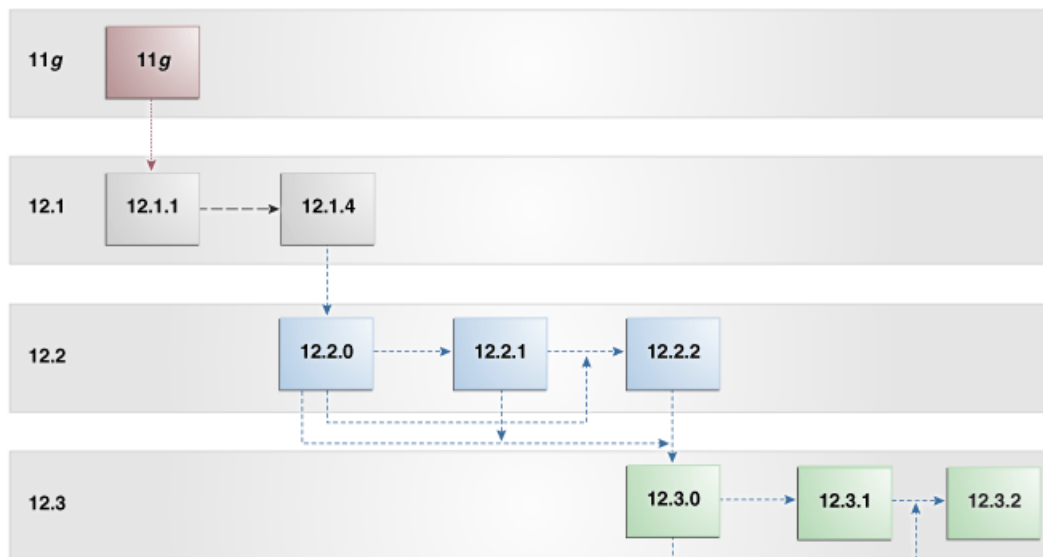
1. If you are using version 12.1.0, 12.1.1, or 12.1.2, upgrade to version 12.1.4.0.0 as described in [Related Resources for Upgrade](#).
2. Upgrade to version 12.2.0.0.0 as described in this guide.
3. Upgrade to version 12.3.0.0.0 as described in this guide.
4. Upgrade to version 12.3.2.0.0 as described in this guide.

Upgrading From Version 11g

Use the following upgrade path when you are upgrading from Oracle Enterprise Manager Ops Center 11g to later versions.

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, then upgrade to 12.3.0, and finally upgrade to the latest version.

Figure 11-3 Supported Upgrade Paths From Version 11g



You must upgrade in this order:

1. Upgrade to version 12.1.1.0.0 as described in [Related Resources for Upgrade](#).
2. Upgrade to version 12.1.4.0.0 as described in [Related Resources for Upgrade](#).
3. Upgrade to version 12.2.0.0.0 as described in this guide.
4. Upgrade to version 12.3.0.0.0 as described in this guide.
5. Upgrade to version 12.3.2.0.0 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.

Follow this procedure to plan your upgrade.

- Review the pre-installation requirements and known issues. See [Related Resources for Upgrade](#) for information on reviewing the pre-installation requirements and known issues.
- Verify that your system meets the operating system requirements. See [Related Resources for Upgrade](#) for information on verifying the operating system requirements.
- Verify that your system meets the system requirements, since some system requirements have changed. See [Related Resources for Upgrade](#) for information on verifying the system requirements.

You can use the OCDoctor to check system requirements and to identify and address some known issues. See [Manage the OCDoctor](#) for more information on using OCDoctor.

- Check if there are any traces from previous Enterprise Controller installation or upgrade procedure. Remove the `/tmp/CVU_12.1.0.2.0_oracleoc` directory and `/tmp/CVU_11.2.0.4.0_oracleoc` directory before installing or upgrading the Enterprise Controller.
- 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. See *Oracle Enterprise Manager Ops Center Security* for information on replacing the self-signed web server 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.
- If your Enterprise Controller is installed on Oracle Solaris 11, your Oracle Solaris 11 publisher must point to an Oracle Solaris 11 repository that contains the specific version of Oracle Solaris 11 installed on the Enterprise Controller before you begin the upgrade. If not, the upgrade process does not proceed.
- While installing or upgrading Enterprise Controllers with a colocated Oracle 12c database, set either the `zfs_arc_max` parameter value or the `user_reserve_hint_pct` parameter value in the `/etc/system` file or a configuration file located in the `/etc/system.d` directory for Oracle Solaris 11.x

platforms. You can use the OC Doctor to calculate the parameter value. Once the parameter value is set, restart the system for the configuration to take effect.

At the beginning of the installation or upgrade of an Enterprise Controller, if the parameter values are not set, then the install or the upgrade wizard provides information on the parameter value to be set and how to set the parameter value.

- If you are upgrading to version 12.2.2.0.0 or 12.3.0.0.0, and are using the embedded database, you must download installation bundles for Oracle Database version 11.2.0.4, as the Oracle Enterprise Manager Ops Center upgrade also upgrades the embedded database. The download procedure is described in the Before You Begin section in each upgrade chapter.

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 or later 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.

- If you are upgrading to version 12.3.1.0.0 or later, and are using the embedded database, you must download installation bundles for Oracle Database version 12.1.0.2, as the Oracle Enterprise Manager Ops Center upgrade also upgrades the embedded database. The download procedure is described in the Before You Begin section in each upgrade chapter.
- Any Oracle Enterprise Manager Ops Center IDRs that are installed prior to upgrading are automatically removed during the upgrade. If the upgrade fails and a rollback takes place, these IDRs must be manually re-installed. When the upgrade is successful, these IDRs will no longer be needed and no further action is required. The Ops Center IDRs uninstalled are listed in the upgrade log.
- Do not upgrade the Java version on Oracle Solaris 10 Control Domains or Logical Domains that have LDOM Manager version 3.2 or earlier installed. If you have upgraded the Java on these systems to version 1.6.0_101 or higher, downgrade to Java 1.6.0_95.

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/mgmt` 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

There are several upgrade procedures available for a variety of environments.

Several factors will determine the procedure that is most appropriate for your environment. The [Table 11-3](#) 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 11-3 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

Related Resources for Upgrade

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For information on upgrading 12.1 versions, see the Upgrading chapter in [Version 12.1 Administration Guide](#)
- For pre-installation and known issues, see *Oracle Enterprise Manager Ops Center Release Notes*
- For information on operating system requirements, see *Oracle Enterprise Manager Ops Center Certified Systems Matrix*
- For information on system requirements, see *Oracle Enterprise Manager Ops Center Installation for Oracle Solaris Operating System* or *Oracle Enterprise Manager Ops Center Installation for Linux Operating Systems*
- To download OCDoctor, go to <https://updates.oracle.com/OCDoctor/OCDoctor-latest.zip>

- For information on vServer Management, see *Oracle Enterprise Manager Ops Center Virtualization Reference*
- For information on upgrading procedures, see *Oracle Enterprise Manager Ops Center Upgrade*
- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Uninstall and Unconfigure the Software

You can unconfigure and uninstall the Agent Controller, Proxy Controller, and Enterprise Controller components of Oracle Enterprise Manager Ops Center.

This chapter describes the procedure to unconfigure and uninstall the Agent Controller, Proxy Controller, and Enterprise Controller.

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

This chapter includes the following sections:

- [Introduction to Uninstall and Unconfigure](#)
- [Roles for Uninstall and Unconfigure](#)
- [Actions for Uninstall and Unconfigure](#)
- [Location of Uninstall and Unconfigure Information in the User Interface](#)
- [Uninstalling and Unconfiguring Agent Controllers](#)
- [Uninstalling and Unconfiguring a Proxy Controller](#)
- [Uninstalling and Unconfiguring the Enterprise Controller](#)
- [Related Resources for Uninstall and Unconfigure](#)

Introduction to Uninstall and Unconfigure

You can 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 [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.

Roles for Uninstall and Unconfigure

You require specific roles to perform uninstallation and unconfiguration tasks in Oracle Enterprise Manager Ops Center.

The following table lists the tasks and the role required to complete the task. Contact your administrator if you do not have the necessary role or privilege to complete a task.

Table 12-1 Uninstall and Unconfigure Tasks and Roles

Task	Role
Uninstall and unconfigure Agent Controllers	Ops Center Admin
Uninstall and unconfigure Proxy Controllers	Ops Center Admin
Remove a Proxy Controller	Ops Center Admin
Uninstall and unconfigure Enterprise Controllers	Ops Center Admin

Actions for Uninstall and Unconfigure

You can perform various uninstallation and unconfiguration operations using Oracle Enterprise Manager Ops Center.

Using Oracle Enterprise Manager Ops Center, you can perform the following tasks:

- Unconfigure and Uninstall Agent Controllers
- Unconfigure and Uninstall Proxy Controllers
- Unconfigure and Uninstall Enterprise Controllers

Location of Uninstall and Unconfigure Information in the User Interface

In the Oracle Enterprise Manager Ops Center user interface, you can find uninstallation and unconfiguration information in different locations.

Table 12-2 Location of Uninstall and Unconfigure Information in the UI

To See	Location
Uninstall and Unconfigure Agent Controllers	Expand Assets in the Navigation pane and select Managed Assets.
Uninstall and Unconfigure Proxy Controllers	Expand Administration in the Navigation pane and select a Proxy Controller. Select Unconfig/uninstall Proxy in the Actions pane.
Uninstall and Unconfigure Enterprise Controllers	Expand Administration in the Navigation pane and select a Enterprise Controller. Select Unconfigure in the Actions pane.

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.

The following topics are covered:

- [Uninstalling and Unconfiguring Agent Controllers from the User Interface](#)
- [Uninstalling and Unconfiguring Agent Controllers from the Command Line](#)

Uninstalling and Unconfiguring Agent Controllers from the User Interface

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

Follow this procedure to 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.

Follow this procedure to 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.

Note: Do not remove the management `/em-sysmgmt-p/cacao_pers_dirs` IPS package from the system even when the Oracle Enterprise Manager Ops Center is uninstalled. This IPS package contains a `cacao` directory which might be in use by the other applications on the system.

The following topics are covered:

- [Unconfiguring and Uninstalling a Proxy Controller from the User Interface](#)
- [Removing a Proxy Controller from the User Interface](#)

- [Unconfiguring a Proxy Controller from the Command Line](#)
- [Uninstalling a Proxy Controller 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.

Follow this procedure to unconfigure and uninstall the 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.

Follow this procedure to remove a Proxy Controller 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. 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.

Follow this procedure to unconfigure a Proxy Controller from the command line.

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 12.3.0.604 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.

Following topics are covered:

- [Unconfiguring the Enterprise Controller](#)
- [Uninstalling the Enterprise Controller](#)

Unconfiguring the Enterprise Controller

You can unconfigure an Enterprise Controller to reconfigure it or as a precursor to uninstalling.

Follow this procedure to unconfigure the Enterprise Controller.

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.

Follow this procedure to uninstall the Enterprise Controller.

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 12.3.0.604 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.

Related Resources for Uninstall and Unconfigure

You can view the Oracle Enterprise Manager Ops Center documents for additional information.

For more information, see these Oracle resources:

- For more information on product administration, see http://docs.oracle.com/cd/E59957_01/nav/administer.htm
- For end-to-end examples, see the Deploy How To library at http://docs.oracle.com/cd/E59957_01/nav/deploy.htm and the Operate How To library at http://docs.oracle.com/cd/E59957_01/nav/operate.htm
- For more information on Enterprise Manager Ops Center, see the Ops Center blog at <https://blogs.oracle.com/opscenter/>

Command Line Administration

You can manage the Oracle Enterprise Manager Ops Center Enterprise Controller, Proxy Controller, and Agent Controller from the command line.

The following information is included in this chapter:

- [About Configuring the Enterprise Controller: ecadm](#)
- [About Configuring the Proxy Controller: proxyadm](#)
- [About Configuring the Agent Controller: agentadm](#)

About Configuring the Enterprise Controller: ecadm

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

The `ecadm` command helps to configure, unconfigure, and perform administrative tasks on the Oracle Enterprise Manager Ops Center Enterprise Controller.

The following topics are covered:

- [Synopsis for ecadm](#)
- [Options for ecadm](#)
- [Subcommands for ecadm](#)
- [Subcommand Options for ecadm](#)
- [Exit Status for ecadm](#)

Synopsis for ecadm

Lists the synopsis for the Enterprise Controller.

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 for ecadm

Lists the common options for the Enterprise Controller.

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 for ecadm

Lists the subcommands for the Enterprise Controller.

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.

rebuild-db-index

Checks the indexes with more than 1 million leaf rows and coalesces the index if the deleted leaf rows are between 10-15% of the index size or rebuilds the index if the deleted leaf rows of the index are more than 50% of the total index leaf rows. This command can only be executed on an Enterprise Controller with a co-located database and can be used only when the Enterprise Controller is in the maintenance mode.

Subcommand Options for ecadm

Lists the subcommand options for the Enterprise Controller.

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 ] [ -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.

-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> [ -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.

-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 for ecadm

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

About Configuring the Proxy Controller: proxyadm

You can configure the Proxy Controller using `proxyadm` command.

The `proxyadm` command helps to start, stop, configure and unconfigure the Oracle Enterprise Manager Ops Center Proxy Controller services.

The following topics are covered:

- [Synopsis](#)
- [Options for proxyadm](#)
- [Subcommands for proxyadm](#)
- [Subcommand Options for proxyadm](#)
- [Exit Status for proxyadm](#)

Synopsis

Lists the synopsis for the Proxy Controller.

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 for proxyadm

Lists the common options for the Proxy Controller.

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 for proxyadm

There are different subcommands used for the Proxy Controller.

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.

backup

Creates a backup archive of the state data of the Proxy Controller. This command does not back up any installed software.

restore

Restores the state data of the Proxy Controller from a backup archive.

update

Updates the URL property of a remote Proxy Controller to point to the new IP address of the Enterprise Controller, if the Enterprise Controller is restored on a new system.

Subcommand Options for proxyadm

There are different subcommand options used for the Proxy Controller.

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.

backup

Enter `proxyadm backup [-o | --output <backup-file>] [-t | --tag <tag>] [-d | --description <description>] [-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/proxy-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).

`-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 `proxyadm restore [-i | --input <backup-file>] [-l | --logfile <logfile>] [-T | --tempdir <temp-dir>] [-v | --verbose]`.

`-i | --input <backup-file>`: Restores state data from `<backup-file>` which is the archive created by the `proxy backup` operation. This parameter is required.

`-T | --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.

update

Enter `proxyadm update -s|--satellite-ip <ip address of EC>`

`-s|--satellite-ip <ip address of EC>`: Uses the IP address of the Enterprise Controller to connect the remote Proxy Controller to the Enterprise Controller.

Exit Status for proxyadm

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

About Configuring the Agent Controller: agentadm

You can configure the Agent Controller using `agentadm` command.

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.

The following topics are covered:

- [Synopsis for agentadm](#)
- [Usage](#)
- [Options for agentadm](#)
- [Subcommands for agentadm](#)
- [Subcommand Options for agentadm](#)

Synopsis for agentadm

Lists the synopsis for the Agent Controller.

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 for agentadm

Lists the common options for the Agent Controller.

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 for agentadm

There are different subcommands used for the Agent Controller.

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.

status

Displays the online or offline status of the Agent Controller services to the standard output.

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 for agentadm

There are different subcommand options used for the Agent Controller.

The following are the subcommand options for agentadm:

start

Enter `agentadm start`.

stop

Enter `agentadm stop`.

status

Enter `agentadm status [-h | --help]`

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

Access Points, [10-19](#)
access points removal, [10-19](#)
accessing the cluster management UI, [10-15](#)
adding a directory server, [8-4](#)
adding a product alias, [5-5](#)
adding authentications, [5-5](#)
adding users, [8-3](#)
Agent Controllers
 agentadm command, [A-11](#)
 checking the status, [2-21](#)
 local Agent Controllers
 configuring on the Enterprise Controller, [2-14](#)
 configuring on the Proxy Controller, [2-15](#)
 unconfiguring on the Enterprise Controller, [2-14](#)
 unconfiguring on the Proxy Controller, [2-15](#)
 migrating between Proxy Controllers, [10-18](#)
 uninstalling, [12-2](#)
 viewing, [2-5](#)
agentadm command, [A-11](#)
ASR
 roles, [7-4](#)
Assets
 determining the number of, [6-6](#)
associating networks with a Proxy Controller, [2-22](#)
authentications
 adding, [5-5](#)
 editing, [5-5](#)
Auto Service Requests
 blacklisting an asset, [7-8](#)
 disabling, [7-7](#)
 enabling, [7-7](#)
 providing contact information, [7-5](#)
 providing contact information for an asset or group, [7-6](#)
 providing default contact information, [7-6](#)
 viewing an asset's ASR status, [7-5](#)

B

Backup and Recovery

Backup and Recovery (*continued*)
 roles, [9-2](#)
backup and restore
 backing up an Enterprise Controller, [9-3](#)
 restoring an Enterprise Controller, [9-5](#)
blacklisting an asset for Auto Service Requests, [7-8](#)

C

changing the customer-managed database location, [4-8](#)
changing the database credentials, [4-10](#)
changing the HTTP Proxy, [2-33](#)
checking the Agent Controller status, [2-21](#)
checking the Enterprise Controller Cluster status, [10-14](#)
checking the Enterprise Controller status, [2-18](#)
checking the Proxy Controller status, [2-19](#)
command line administration, [A-1](#)
configuration management
 roles, [3-2](#)
configuring a notification profile, [8-24](#)
configuring a Proxy Controller to use a strong cipher suite configuration, [2-23](#)
configuring DHCP, [2-24](#)
configuring external DHCP servers, [2-27](#)
configuring Oracle Configuration Manager, [2-15](#)
configuring subnets, [2-26](#)
configuring the Enterprise Controller for WAN Boot, [2-30](#)
Connected Mode, [2-8](#)
connection modes
 switching to Connected Mode, [2-8](#)
 switching to Disconnected Mode, [2-7](#)
converting a single Enterprise Controller to high availability, [10-6](#)
converting to a single Enterprise Controller, [10-11](#)

D

database
 changing credentials, [4-10](#)

database (*continued*)
 changing the customer-managed database
 location, [4-8](#)
 Installing and configuring a customer-managed
 database, [4-3](#), [4-5](#)
 migrating to a customer-managed database, [4-7](#)
 upgrading a customer-managed database, [4-10](#)
 verifying, [4-10](#)
database management
 roles, [4-2](#)
delete access points, [10-19](#)
deleting a directory server, [8-7](#)
deleting a notification profile, [8-26](#)
deleting users, [8-4](#)
DHCP configuration, [2-24](#)
directory servers
 adding, [8-4](#)
 deleting, [8-7](#)
disabling Auto Service Requests, [7-7](#)
disabling networks for a Proxy Controller, [2-22](#)
Disconnected Mode, [2-7](#)
Discovery
 assets, [3-5](#)
downloading the OCDoctor, [6-2](#)

E

ecadm command, [A-1](#)
editing authentications, [5-5](#)
editing the energy cost, [5-6](#)
enabling Auto Service Requests, [7-7](#)
enabling networks for a Proxy Controller, [2-22](#)
energy cost
 editing, [5-6](#)
Enterprise Controller
 backing up, [9-3](#)
 checking the status, [2-18](#)
 ecadm command, [A-1](#)
 high availability, [10-5](#)
 registering, [2-16](#)
 restoring, [9-5](#)
 starting, [2-18](#)
 stopping, [2-19](#)
 uninstalling, [12-7](#)
 viewing configuration, [2-6](#)
 WAN boot configuration, [2-30](#)
external DHCP server configuration, [2-27](#)

F

Find Assets, [3-5](#)

G

general administration
 roles, [5-2](#)

H

harvester script
 copying content to the Enterprise Controller, [2-12](#)
 downloading, [2-9](#)
 identify a harvester system, [2-8](#)
 using, [2-9](#)
high availability
 accessing the cluster management UI, [10-15](#)
 checking the cluster status, [10-14](#)
 converting to a single Enterprise Controller, [10-11](#)
 converting to high availability, [10-6](#)
 managing network resources, [10-12](#)
 manually relocating, [10-12](#)
 removing a standby Enterprise Controller, [10-14](#)
 roles, [10-4](#)
 shutting down an Enterprise Controller without
 relocating, [10-15](#)
HTTP Proxy
 changing, [2-33](#)

I

Infrastructure
 roles, [2-2](#)
installing and configuring a 12CDB customer-
 managed database, [4-5](#)
installing and configuring a customer-managed
 database, [4-3](#)

L

logs, [5-4](#)

M

managing HA network resources, [10-12](#)
managing Proxy Controller networks, [2-21](#)
managing roles, [8-23](#)
manually relocating the Enterprise Controller, [10-12](#)
migrating to a customer-managed database, [4-7](#)

N

networks
 associating with a Proxy Controller, [2-22](#)
 enable or disable, [2-22](#)
notification profiles
 configuring, [8-24](#)
 deleting, [8-26](#)

O

OCDoctor
 downloading, [6-2](#)
 preinstallation checks, [6-3](#)
 roles, [6-1](#)

OCDocor (*continued*)
running a self-diagnosis, [2-17](#)
troubleshooting and tuning, [6-4](#)
updating, [6-4](#)
Oracle Configuration Manager
configuring, [2-15](#)

P

performing preinstallation checks, [6-3](#)
performing troubleshooting and tuning, [6-4](#)
permissions
granted by roles, [8-8](#)
required for tasks, [8-18](#)
preinstallation checks, [6-3](#)
product aliases, [5-5](#)
providing ASR contact information, [7-5](#)
Proxy Controllers
associate networks, [2-22](#)
automatic failover, [10-15](#)
checking the status, [2-19](#)
configuring to use a strong cipher suite
configuration, [2-23](#)
DHCP configuration, [2-24](#)
enable or disable networks, [2-22](#)
high availability, [10-15](#)
maintenance mode, [2-20](#)
manage networks, [2-21](#)
proxyadm command, [A-8](#)
putting in maintenance mode, [2-20](#)
removing from maintenance mode, [2-21](#)
starting, [2-19](#)
stopping, [2-20](#)
subnet configuration, [2-26](#)
uninstalling, [12-4](#)
viewing, [2-6](#)
proxyadm command, [A-8](#)
putting a Proxy Controller in maintenance mode, [2-20](#)

R

registering the Enterprise Controller, [2-16](#)
relocating the Enterprise Controller, [10-12](#)
removing a Proxy Controller from maintenance mode,
[2-21](#)
removing a standby Enterprise Controller, [10-14](#)
replicating a user, [8-24](#)
roles
copying to a new user, [8-24](#)
managing, [8-23](#)
permissions granted by roles, [8-8](#)
tasks available based on permissions, [8-18](#)
Roles
Auto Service Request, [7-4](#)
Backup and Recovery, [9-2](#)
configuration management, [3-2](#)

Roles (*continued*)
database management, [4-2](#)
general administration, [5-2](#)
High Availability, [10-4](#)
infrastructure, [2-2](#)
OCDocor, [6-1](#)
uninstall and unconfigure, [12-1](#)
upgrade, [11-1](#)
user and role management, [8-2](#)
running a self-diagnosis, [2-17](#)

S

self-diagnosis, [2-17](#)
service status, [5-3](#)
Service tags, [3-5](#)
shutting down an Enterprise Controller without
relocating, [10-15](#)
starting a Proxy Controller, [2-19](#)
starting the Enterprise Controller, [2-18](#)
stopping a Proxy Controller, [2-20](#)
stopping the Enterprise Controller, [2-19](#)
strong cipher suite configuration, [2-23](#)
subnet configuration, [2-26](#)
synchronizing remote users and roles, [8-6](#)

T

Tags
service, [3-5](#)
troubleshooting with the OCDocor, [6-4](#)
tuning with the OCDocor, [6-4](#)

U

Uninstall and Unconfigure
roles, [12-1](#)
uninstalling
Agent Controllers, [12-2](#)
Enterprise Controllers, [12-7](#)
Proxy Controllers, [12-4](#)
updating the OCDocor, [6-4](#)
Upgrade
roles, [11-1](#)
upgrading
planning the upgrade, [11-5](#)
upgrading a customer-managed database, [4-10](#)
User and role management
roles, [8-2](#)
users
adding, [8-3](#)
configuring notification profiles, [8-24](#)
deleting, [8-4](#)
deleting notification profiles, [8-26](#)
managing user roles, [8-23](#)
replicating, [8-24](#)

users (*continued*)
 viewing role details, [8-4](#)
using connection modes, [2-7](#)

V

verifying the database, [4-10](#)
viewing Agent Controllers, [2-5](#)
viewing ASR status for an asset, [7-5](#)

viewing logs, [5-4](#)
viewing Proxy Controllers, [2-6](#)
viewing service status, [5-3](#)
viewing the Enterprise Controller configuration, [2-6](#)
viewing user role details, [8-4](#)

W

WAN boot configuration, [2-30](#)