Oracle® Enterprise Manager Ops Center

Administration Guide

12*c* Release 1 (12.1.4.0.0)

E25143-08

June 2013

ORACLE®

Oracle Enterprise Manager Ops Center Administration Guide, 12*c* Release 1 (12.1.4.0.0)

E25143-08

Primary Author: Owen Allen

Contributing Author: Laura Hartman, Barbara Higgins, Uma Shankar, Shanthi Srinivasan

Contents

6 Auto Service Requests

7 User and Role Management

8 Backup and Recovery

9 High Availability

10 Upgrading

11 Uninstalling and Unconfiguring

A Command Line Administration

Index

Preface

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

Audience

This document is intended for senior system administrators.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

For more information, see the other documents in the Oracle Enterprise Manager Ops Center 12c Release 1 documentation set, located at this site: http://www.oracle.com/pls/topic/lookup?ctx=oc121

Conventions

The following text conventions are used in this document:

Convention	Meaning
italic	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.

1

Introduction to Administration

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

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

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

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

As part of 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:

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

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

2

Infrastructure

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

The following features and topics are covered in this chapter:

Introduction to Infrastructure

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 the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about these commands.

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

Viewing Infrastructure

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

Viewing Agent Controllers

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

- Asset Name
- Zone Type
- Agent Version
- Upgrade Version
- Downgrade Version
- Agent Status (Online or Offline)

To View Agent Controllers

1. Click the Assets section of the Navigation pane.
2. Select a group that contains managed operating systems.
   - Select an operating system smart group from the Operating Systems category, then click the **Summary** tab.
   - Select a user-defined group that contains operating systems, then click the **Membership** tab.
3. Click the **Agent Controllers** tab.

   Agent Controller information is displayed.

Viewing Proxy Controllers

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

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

To View a Proxy Controller

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. 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: 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 location of update libraries.
- Zone Controller: Manages the zone management settings.

Migrating Agent Controllers Between Proxy Controllers

A Proxy Controller manages each Agent Controller. You can migrate an Agent Controller from one Proxy Controller to another to balance job load or if you intend to uninstall a Proxy Controller. The destination Proxy Controller must be on, or associated with, the asset's network.

To Move Agent Controllers Between Proxy Controllers

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.

   The Asset Migration Wizard is displayed.

4. Select the destination Proxy Controller from the list of Proxy Controllers, or select **Auto Balance across Proxy Controllers** to automatically select a destination Proxy Controller.

5. Click **Migrate**.

   A job is launched to migrate the selected assets to the destination Proxy Controller.

Using Connection Modes

Oracle Enterprise Manager Ops Center can operate in either Connected or Disconnected Mode. In Connected Mode, the software communicates with Oracle web sites and other vendors, gathering patch and update information. In Disconnected Mode, the software operates autonomously 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 You Begin

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

To Switch to Disconnected Mode

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**.

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.

To Switch to 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**.

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.

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

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

Identifying a Harvester System

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

Downloading the Harvester Bundle

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

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

Using the Harvester Script

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

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

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

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

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

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

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

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

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

Examples of Running 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

When you have downloaded the Knowledge Base bundle or OS update content, move it to the Enterprise Controller system using portable media.

Copying a Knowledge Base Bundle

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

1. Copy the `standalone-<timestamp>.tar.gz` to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory.
2. Use the Switching to Disconnected Mode procedure to upload the Knowledge Base bundle and enable disconnected mode.

Copying a Knowledge Base Bundle and All Patches

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

1. Copy the `standalone-<timestamp>.tar.gz` to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory.
2. Copy the `all_unsigned` folder, which includes all patches, to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory. You can split this folder across multiple DVDs if needed.
3. Use the Switching to Disconnected Mode procedure to upload the Knowledge Base bundle and enable disconnected mode.
4. Run the `copy_patches_to_oc.sh` script. This script is located in the `all_unsigned` folder.

Copying a Knowledge Base Bundle and Incremental Patches

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

1. Copy the `standalone-<timestamp>.tar.gz` to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory.
2. Copy the `all_unsigned-<timestamp>` folder, which includes the patches downloaded on the day specified by the timestamp, to the Enterprise Controller system. By default, this file is in the `/var/tmp/offline` directory. You can split this folder across multiple DVDs if needed.
3. Use the Switching to Disconnected Mode procedure to upload the Knowledge Base bundle and enable disconnected mode.
4. Run the `copy_patches_to_oc.sh` script. This script is located in the `all_unsigned-<timestamp>` folder.

Configuring Local Agent Controllers

A local Agent Controller is an Agent Controller installed on the Enterprise Controller or Proxy Controller OS. This enables you to monitor the systems that supports the Enterprise Controller or Proxy Controller and launch some jobs that target the system.

Configuring the Local Agent Controller on the Enterprise Controller

Configuring the Local Agent Controller on the Enterprise Controller system enables you to monitor the system that supports the Enterprise Controller and launch jobs that target it.

Jobs that target the Enterprise Controller's hardware or OS that would cause the Enterprise Controller system to restart, such as an OS update that requires a reboot, cannot be performed through the product.

To Configure the Local Agent 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 page is displayed.
3. Click OK. A job is launched to configure the local Agent Controller.

Unconfiguring the Local Agent Controller on the Enterprise Controller

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

To Unconfigure the Local Agent 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.

To Configure a Local Agent 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. 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.

To Unconfigure a Local Agent 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.

Before You Begin

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

To Configure Oracle Configuration Manager

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.

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.

To Run a Self Diagnosis

1. Select the target asset in the Assets section or Administration section of the Navigation pane.
2. Click **Self Diagnosis** in the Actions pane.
3. Select a task.
   - Select **Run New Self Diagnosis** to launch a new self diagnosis job.

     If the target operating system supports the Enterprise Controller or a Proxy Controller, you can also select Optimize Enterprise Controller or Proxy Controller. This option uses the `--tuning` option to optimize the system for Enterprise Controller or Proxy Controller performance.
   - Select **Work on Previous Self Diagnosis** and select a prior self diagnosis job to review the data from a prior self diagnosis.
4. If you selected Work on Previous Self Diagnosis, the data from the prior self diagnosis is displayed. Review the data, then select a task.
   - Select **re-run Self Diagnosis** to re-run the prior Self Diagnosis.

     You can also check Attempt to Fix Issues to automatically fix certain issues.
   - Select **Collect Logs** to collect logs from the system.

   Click Next.
5. Review the summary information, then click **Finish** to launch the job.
6. Review the job details or rerun the wizard and select **Work on Previous Self Diagnosis** to view the data gathered by the self diagnosis.

Viewing and Changing the Enterprise Controller and Proxy Controller Status

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

Checking the Status of the Enterprise Controller

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

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

To Check the Status of the Enterprise Controller

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.

To Start the Enterprise Controller

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

   The following options may be used:

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

   For example:

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

```
#
```

The Enterprise Controller is started.

Stopping the Enterprise Controller

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

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

To Stop the Enterprise Controller

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

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.

To Start a Proxy Controller

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.

To Stop a Proxy Controller

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. However, the Proxy Controller continues to manage its current assets.

1. In the Administration pane, select a Proxy Controller.

2. Click **Put in Maintenance Mode** in the Actions pane.

   A confirmation window is displayed.

3. Click **OK**.

   The Proxy Controller is placed in maintenance mode.

Removing a Proxy Controller from Maintenance Mode

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

1. In the Administration pane, select a Proxy Controller.
2. Click **Clear Maintenance Mode** in the Actions pane.

   A confirmation window is displayed.

3. Click **OK**.

   The Proxy Controller is removed from maintenance mode.

Managing Proxy Controller Networks

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

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

Associating Networks With a Proxy Controller

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

To Associate Networks

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.

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.

To Enable or Disable Networks

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

The selected networks are enabled or disabled.

Configuring Proxy Controllers to Use a Strong Cipher Suite Configuration

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

To Configure Proxy Controllers to Use a Strong Cipher Suite Configuration

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

Configuring DHCP and Subnets for OS Provisioning

To perform OS provisioning, a Proxy Controller must have DHCP configured. 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.

Configuring DHCP

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

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

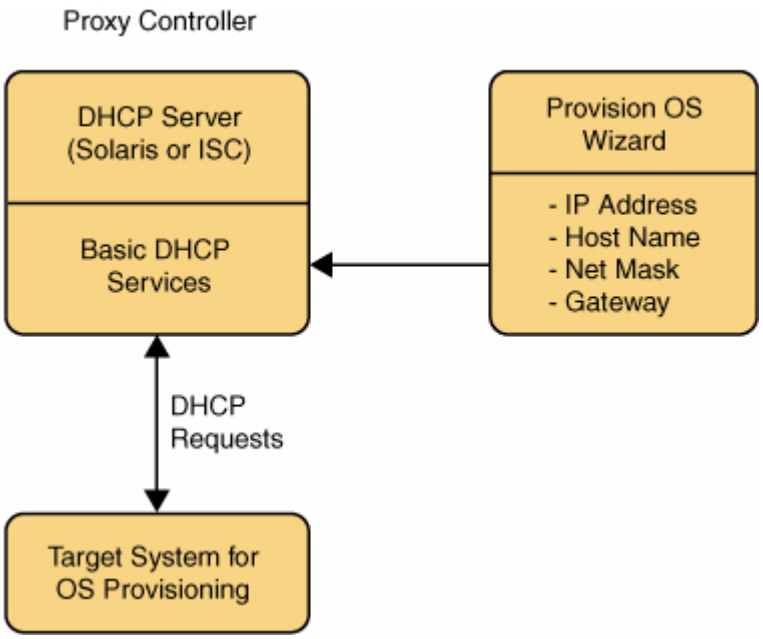
The DHCP Config action requires that you specify the Ethernet interface through which the Proxy Controller should provide DHCP services, for example bge0. You can establish DHCP services on all the Ethernet interfaces in the Proxy Controller. The Proxy Controller's Ethernet interface that you specify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

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

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

Figure 2–1, "Basic DHCP Configuration" shows the basic DHCP configuration.

Figure 2–1 Basic DHCP Configuration



To Configure DHCP Services

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 Configuration dialog box, provide the following information:
   - **DHCP Server**: Select either ISC or Oracle Solaris to implement either the Internet Standards Consortium (ISC) reference DHCP server, or the Oracle Solaris native DHCP server. The ISC server is generally preferred.

- **Interfaces**: 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.
- **Enable DHCP**: Select this option to enable the DHCP server that you selected.

4. Click **Configure DHCP** to save the DHCP configuration that you specified.
5. A warning indicates that the procedure removes existing subnets in the DHCP configuration. Click **Yes** to accept that action and continue.
6. A message indicates that the DHCP configuration job has been submitted. Click **OK** to dismiss the message. When the job is complete, 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  10.0.0.2
e1000g1  192.168.1.2
e1000g2  172.16.12.2
```

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 192.168.1.0/24 or 172.16.12.0/24.

Configuring Subnets

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

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

You configure subnets for the following reasons:

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

Specifying IP Address Ranges

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

The IP addresses within the range that you specify cannot be used for OS provisioning operations. For example, if you specify 192.168.0.64 and 192.168.0.128 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.

To Configure a Subnet

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.

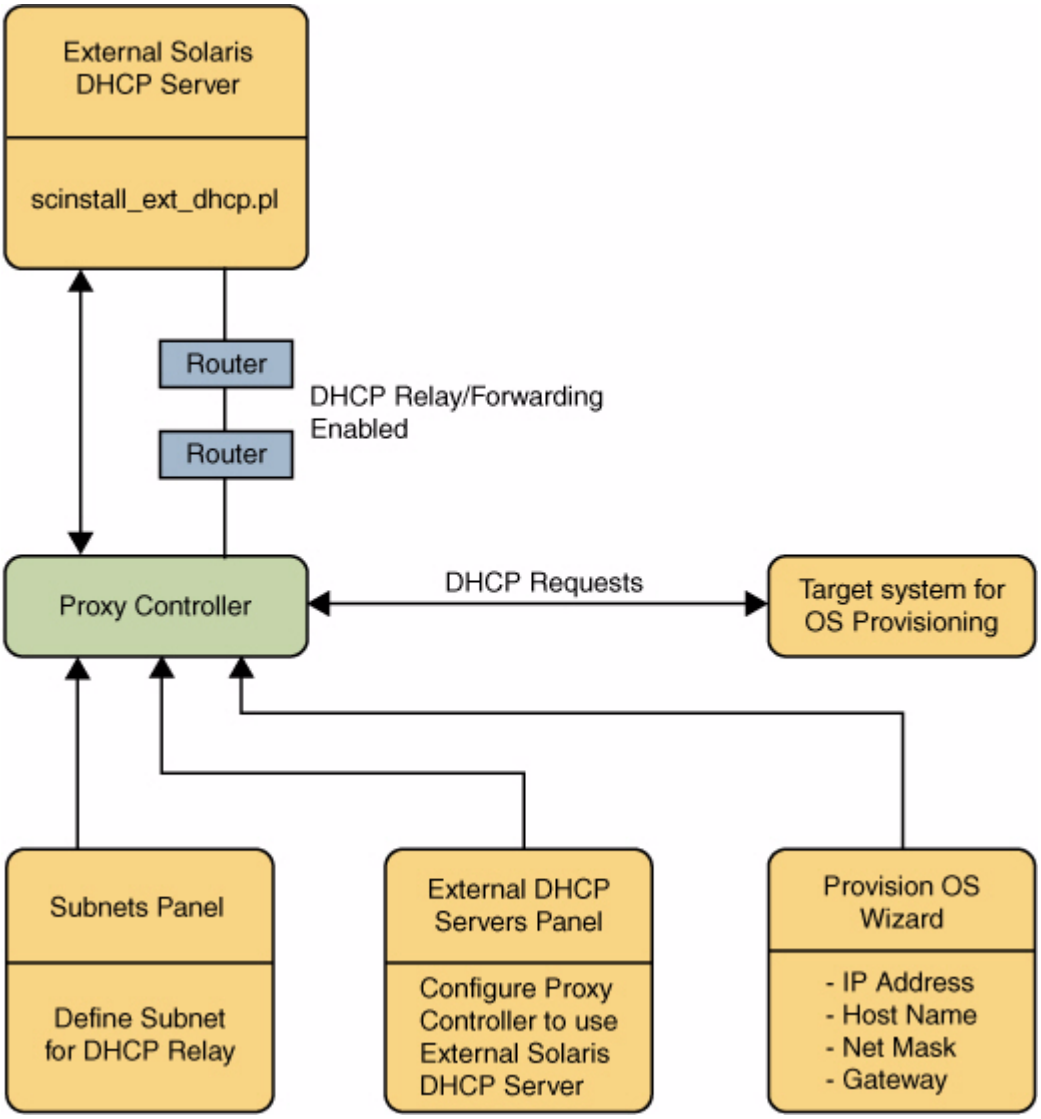
Configuring External DHCP Servers

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

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

Figure 2–2, "DHCP Configuration Using External DHCP Servers" illustrates DHCP configuration using External DHCP servers.

Figure 2–2 DHCP Configuration Using External DHCP Servers



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

External DHCP Server Requirements

The External DHCP Servers action is only compatible with Oracle Solaris DHCP server and not with ISC DHCP server.

Before You Begin

Configuring External DHCP servers requires the following prerequisite tasks:

- Establish DHCP relay or forwarding services on the network routers, switches, or systems that comprise your network. Refer to the documentation for those components for the required procedures.
- Use the scninstall_ext_dhcp.pl script to establish the communication channel between a Proxy Controller and the External DHCP server. The scninstall_ext_dhcp.pl script enables ssh access to the DHCP server without requiring passwords.

To Install the scninstall_ext_dhcp.pl Script on the External DHCP Server

You must use `wget` to get the `scninstall_ext_dhcp.pl` script from the Proxy Controller to the External DHCP server.

1. 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.

2. Grant execute permissions for the script.

   ```
   # chmod +x scninstall_ext_dhcp.pl
   ```

3. 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.

> **Note:** Ensure that you use `wget` to copy the `scninstall_ext_dhcp.pl` script from the Proxy Controller to another external DHCP server.

To Configure External DHCP Servers

1. In the Administration pane, select the Proxy Controller where you want to configure an external DHCP server.
2. Select **External DHCP Servers** in the Actions pane. The External DHCP Servers Configuration dialog box is displayed.
3. 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.
4. 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.

5. Click **Create DHCP Server** to create the DHCP server configuration that you specified. A message indicates that a job to create the external DHCP server was submitted. Click **OK** to dismiss the message.

Configuring the Enterprise Controller for WAN Boot

The Enterprise Controller is configured to be a WAN boot server when Oracle Enterprise Manager Ops Center is installed on an Oracle Solaris operating system.

WAN boot is the default connection for Oracle Solaris 11 provisioning. You can use DHCP or WAN boot for Oracle Solaris 10 provisioning.

Checking the WAN Boot Status

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.

Enabling or Disabling WAN Boot

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

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

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

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.

3

Database Management

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

The following features and topics are covered in this chapter:

Introduction to Database Management

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

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

Some of the procedures described in this section use the `ecadm` command. See the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about this command.

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

Installing and Configuring a Customer-Managed Database

If you want to use a customer-managed database, you must install and configure it to work with Oracle Enterprise Manager Ops Center.

To Install and Configure a Customer-Managed Database

1. Install the database according to the Oracle Database 11g Enterprise Edition installation documentation.
2. 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
```

3. 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.
   - **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.

   For example:

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

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

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


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

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

```
Enter username for read only Ops Center database login: TESTSCHEMA_RO
Enter password for read only Ops Center database login:
Enter default tablespace for Ops Center user: USERS
Enter temporary tablespace for Ops Center user: TEMP
Enter Oracle Data Pump destination directory: /var/tmp/ocdumpdir

"Done creating OC_SYSTEM_ROLE and OC_RO_ROLE"
"Done creating Schema 'TESTSCHEMA'. Roles and privileges have been granted."
"Done creating Schema 'TESTSCHEMA_RO'. Roles and privileges have been granted."
"Done creating OC_DUMP_DIR at /var/tmp/ocdumpdir"
"Done granting privs to users and profiles"
"Testing connectivity to the new schema: 'TESTSCHEMA'"
Connected.
"Testing connectivity to the new read only schema: 'TESTSCHEMA_RO'"
Connected.

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


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

Migrating to a Customer-Managed Database

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

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

To Migrate to a Customer-Managed Database

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.

   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>
   ```

2. Use the `ecadm` command with the `backup` subcommand to back up the Enterprise Controller. This procedure is described in Chapter 8, "Backup and Recovery".

3. Use the `ecadm` command with the `migrate` subcommand and the `--remoteDBprops <path to properties file>` and `-l <log file>` options to migrate to a customer-managed database. The log file is created in the `/var/opt/sun/xvm/logs` directory.

For example:

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

Changing the Customer-Managed Database Location

You can change the location of the customer-managed database. You must install and configure the database in the destination location as described in the Installing and Configuring a Customer-Managed Database section before beginning this procedure.

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

To Change the Customer-Managed Database Location

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>
   ```

   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 11.2.0.1.0 - Production on Mon May 23 10:14:33 2011
   Copyright (c) 1982, 2009, Oracle and/or its affiliates. All rights reserved.
   Username: / as sysdba
   <output omitted>
   Job "SYS"."SYS_EXPORT_SCHEMA.01" succesfully completed at <timestamp>
   $
   ```

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

   For example:

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

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

   For example:

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

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

   For example:

   ```
   $ rm OC_schema.dmp
   ```

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

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

    For example:

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

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

    For example:

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

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

    For example:

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

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

    For example:

    ```
    $ rm OC_schema.dmp
    ```

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

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

    For example:

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

Verifying the Database

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

To Verify the Database

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

   For example:

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

Upgrading a Customer-Managed Database

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

To Upgrade the Customer-Managed Database

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

   For example:

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

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

   For example:

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

Changing the Database Credentials

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

Changing the Database Credentials for the Ops Center User

To Change the Database Credentials for the Ops Center User

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

   For example:

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

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

   For example:

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

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

   For example:

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

4. Remove the temporary file containing the new password.

   For example:

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

Changing the Database Credentials for the Read-Only User

To Change the Database Credentials for the Ops Center User

1. Create a temporary file containing the new password.

   For example:

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

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

   For example:

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

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

   For example:

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

4. Remove the temporary file containing the new password.

   For example:

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

4

General Administration

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

The following features and topics are covered in this chapter:

Introduction to General Administration

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 the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about these commands.

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

Viewing Service Status

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

Do not disable these services outside of the software. Use the `ecadm`, `proxyadm`, and `agentadm` commands to manage the services.

Table 4–1, " Oracle Enterprise Manager Ops Center Services" shows the names, FRMI identifiers, and normal statuses of the Oracle Enterprise Manager Ops Center services.

Table 4–1 Oracle Enterprise Manager Ops Center Services

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

To View Service Status

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

To View 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
   - DB transaction log
   - DB report log
   - Proxy log
   - Update error log

- Update channel download log
- Update channel error log

The log is displayed.

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

Adding a Product Alias

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

> **Note:** Use this feature as directed by Oracle Support.

To Add a Product Alias

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.

To Add or Edit Authentications

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.

To Set the Cost of Energy

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**.

5

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.

The following features and topics are covered in this chapter:

Introduction to the OCDoctor

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

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

Downloading the OCDoctor

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

To Download the OCDoctor

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

Performing Preinstallation Checks

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

To Perform 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 version 3.06 (Jan 21 2012 [Build 450]), OC Version 12.1
(SunOS)
======================== Checking Network Connectivity
============================
Using Ops Center Proxy server:www-proxy.us.oracle.com   Port:80 (you may
overwrite it by setting https_proxy)
Please enter the My Oracle Support (MOS) Username: owen.allen@oracle.com
Password:
Test 1/2: Downloading Knowledge Channels file from updates.oracle.com
================================================================================
OK: Knowledge download was successful!

Test 2/2: Downloading patch 108437-06 from updates.oracle.com
================================================================================
OK: Patch download was successful!
```

Performing Troubleshooting and Tuning

The OCDoctor can help you troubleshoot issues and tune systems.

To Perform Troubleshooting and Tuning

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
======================== Checking Enterprise Controller...
==============================
OK: Total number of agents: 12
OK: Number of agents with inventories: 12
OK: Enterprise Controller requirements are met
OK: SUNWj6rt version matches SUNWj6rtx version (1.6.0_21)
OK: Apache logs are smaller than 2 GB
OK: n1gc folder has the right permissions
OK: All Enterprise Controller packages are installed properly
OK: All agent packages are installed properly
OK: All agent patches are installed properly
WARNING: Enterprise Controller status is not online - try starting it using the
command:
         /opt/SUNWxvmoc/bin/ecadm start -w
<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.

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 version 3.06 (Jan 21 2012 [Build 450]), OC Version 12.1
(SunOS)
Trying to download updates...
Using Ops Center Proxy server:www-proxy.us.oracle.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: 3.06, online:
3.06).

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

6

Auto Service Requests

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

The following features and topics are covered in this chapter:

Introduction to ASR

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. 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 can be a direct or an indirect 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.

When ASR creation is enabled, Oracle Enterprise Manager Ops Center periodically launches a job to activate assets for ASR, and attempts to activate all assets when they are discovered. You can view the details of this job to see what assets have been activated. You can also view an asset's ASR status. 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 creation.

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 assets in MOS. The status of these assets 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 assets' status is changed to the standard ASR status of "Active".

When a qualified critical incident causes an ASR creation attempt, a job is run to create the ASR, and an annotation is added to the incident indicating the ASR creation

attempt. If the ASR creation is successful, another annotation is added, indicating that the ASR was succesfully 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.

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

Note: Some assets, such as Sun ZFS Storage Appliances, can report ASRs independently. You can choose whether to let these assets report ASRs independently or report them through Oracle Enterprise Manager Ops Center. See the Storage Libraries chapter of the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information.

Viewing ASR Status for an Asset

You can view an asset's ASR activation status. If the asset is activated for ASR, an ASR is generated for any qualified critical issues. 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.

To View the ASR Status for an Asset

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.

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.

To Provide Contact Information for an Asset or Group

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

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

Enabling ASR

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

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

To Enable Auto Service Requests

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**.

   Auto Service Requests are enabled.

Disabling ASR

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

To Disable Auto Service Requests

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.

To Blacklist an Asset

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

7

User and Role Management

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

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

The following features and topics are covered in this chapter:

Introduction to User and Role Management

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.

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

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

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

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.

Before You Begin

You must configure the remote directory server before adding it to Oracle Enterprise Manager Ops Center.

1. Create the following user groups on the directory server:
   - ASSET_ADMIN
   - CLOUD_ADMIN
   - CLOUD_USER
   - EXALOGIC_ADMIN
   - 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.

To Add a Directory Server

1. Select **Administration** in the Navigation pane.
2. Click **Directory Servers**.
3. Click the **Add Directory Server** icon.

   The Remote Directory Server Connection Settings page is displayed.
4. 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 Remote Directory Server Schema Settings page is displayed.
5. 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 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.

   Click **Next**.

   The Summary page is displayed.
6. Review the summary, then click **Add Directory Server**.

Synchronizing Remote Users and Roles

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

Synchronizing Remote Users and Roles With One Directory Server

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

To Sync Remote Users and Roles

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 Sync Remote Users and Roles

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

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

   A confirmation window is displayed.
4. Click **OK**.

About Roles and Permissions

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

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

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

How Roles are Mapped to Permissions

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

Table 7–1 Roles and Permissions

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

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Cloud Admin	Asset Management
	Asset Network Management
	Cloud Management
	Cloud Usage
	Fabric Creation
	Fabric Deletion
	Fabric Management
	Fabric Usage
	IPMP Groups
	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 Usage
	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 7–1 (Cont.) Roles and Permissions

Role	Permissions
Cloud User	Asset Management
	Asset Network Management
	Cloud Usage
	Fabric Creation
	Fabric Deletion
	Fabric Usage
	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 Usage
	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

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Exalogic Systems Admin	Asset Management
	Credential Management
	Directory Server Management
	EC Energy Cost Management
	EC HTTP Proxy Management
	EC Registration
	Fabric Creation
	Fabric Deletion
	Fabric Management
	Fabric Usage
	Job Management
	Link Aggregation
	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
	Operation Execution
	OVM Manager Management
	OVM Manager Usage
	Power Distribution Unit Management
	Power Distribution Unit Usage
	Profile Plan Management
	Proxy Controller Management
	Read Access
	Report Management
	Role Management
	Server Deployment
	Server Management
	Server Usage
	Service Request
	Storage Creation
	Storage Deletion
	Storage Management
	Storage Server Management
	Storage Server Usage
	Storage Usage
	Switch Usage
	Update Firmware
	User Management
	Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Fault Admin	Fault Management
	Read Access
	Write Access
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

Table 7–1 (Cont.) Roles and Permissions

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

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Apply Deployment Plans	Operation Execution
	Read Access
	Server Deployment
	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

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Supercluster Systems Admin	Asset Management Cluster Management Credential Management Directory Server Management EC Energy Cost Management EC HTTP Proxy Management EC Registration Fabric Creation Fabric Deletion Fabric Management Fabric Usage Job Management Link Aggregation 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 Operation Execution Power Distribution Unit Management Power Distribution Unit Usage Profile Plan Management Proxy Controller Management Read Access Report Management Role Management Server Deployment Server Management Server Usage Service Request Storage Creation Storage Deletion Storage Management Storage Server Management Storage Server Usage Storage Usage Switch Usage Update Firmware User Management Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Update Admin	Boot Environment Management
	Read Access
	Update
	Update Simulation
	Windows Update Management
	Write Access
Update Simulation Admin	Read Access
	Update Simulation
	Write Access
User Management Admin	Directory Server Management
	Read Access
	User Management
	Write Access

Table 7–1 (Cont.) Roles and Permissions

Role	Permissions
Virtualization Admin	Asset Management
	Asset Network Management
	Fabric Creation
	Fabric Deletion
	Fabric Management
	Fabric Usage
	IPMP Groups
	Link Aggregation
	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
	Read Access
	Server Deployment
	Server Management
	Server Pool Creation
	Server Pool Deletion
	Server Pool Management
	Server Pool Usage
	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

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

Table 7–2 Permissions and Tasks

Permission	Tasks
Read Access	Read Access
Discover Assets	Add Assets
	Find Assets
Manage Assets	Manage Assets
	Delete Assets
Asset Group Management	Create Group
	Edit Group
	Add Assets to Group
	Delete Group
Update	New Update OS Job
	Deploy or Update Software
	Compare System Catalog
	Create Catalog Snapshot
	View and Modify Catalog
Update Simulation	New Simulated OS Update Job
Server Deployment	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
Credential Management	Update Management Credentials
	Any Actions related to changing credentials

Table 7–2 (Cont.) Permissions and Tasks

Permission	Tasks
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
User Management	Add Users
	Remove Users
Role Management	Assign Roles
Asset Management	Asset Management

Table 7–2 (Cont.) Permissions and Tasks

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

Table 7–2 (Cont.) Permissions and Tasks

Permission	Tasks
Boot Environmnent Management	Activate Boot Env and Reboot
	Create New Boot Env.
	Synchronize Boot Env.
Server Pool Creation	Create Server Pool
Server Pool Deletion	Delete Server Pool
Server Pool Management	Rebalance Resource
	Edit Server Pool Attribute
	Attach Network to Server Pool
	Associate Library to Server Pool
	Add/Remove Virtual Host
Server Pool Usage	Create OVM virtual Servers
	Create zone servers
	Create Logical Domains
Virtualization Host Creation	Create Virtualization Host
Virtualization Host Deletion	Delete Virtualization Host
Virtualization Host Management	Add/Remove Virtual Host to/from Server Pool
	Edit Tags
	Edit Attributes
	Reboot
	Change Routing Configuration
	Change NFS4 Domain
	Change Naming Service
	Change Remote Logging Configuration
Virtualization Host Usage	Create Logical Domains
	Create zones
	Create OVM virtual servers
Virtualization Guest Creation	Create Logical Domains
	Create zones
	Create OVM virtual servers
Virtualization Guest Deletion	Delete Logic Domain
	Delete Zones
	Delete OVM Virtual Servers
Virtualization Guest Usage	Start Guest
	Shutdown Guest
	Migrate Guest
	Clone Guest
Storage Creation	Create Library
Storage Deletion	Delete Library
Storage Usage	Associate Library

Table 7–2 (Cont.) Permissions and Tasks

Permission	Tasks
Network Creation	Create Network Domain
	Create Network(manage network)
Network Deletion	Delete Network Domain
	Delete Network
Network Usage	Assign Network
	Connect Guests
Fabric Creation	Create Fabric
Fabric Deletion	Delete Fabric
Fabric Usage	Fabric Management
Chassis Usage	Chassis Usage
Storage Server Usage	Storage Server Usage
Switch Usage	Switch Usage
Server Usage	Launch LOM Controller
	Edit Tags
Operating System Usage	Edit Tags
	Edit Attributes
Rack Creation	Create Rack
Directory Server Management	Directory Server Management
Power Distribution Unit Usage	Power Distribution Unit Usage
Power Distribution Unit Management	Power Distribution Unit Management
Rack Creation	Rack Creation
Rack Deletion	Rack Deletion
Rack Management	Rack Management
Rack Usage	Rack Usage
OVM Manager Usage	OVM Manager Usage
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 Assign Roles and Privileges to a User

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.

To Replicate a User

1. Select **Administration** in the Navigation pane.
2. Click either **Local Users** or a directory server.

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

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

Configuring a Notification Profile

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

Eight levels of notification can be sent:

- **None**: No notifications are sent to the destination.
- **Incident Severity >= Critical**: Incidents of critical severity are sent to the destination.
- **Incident Severity >= Warning**: Incidents of critical or warning severity are sent to the destination.
- **Incident Severity >= Info**: Incidents of any severity are sent to the destination.
- **Incident updates and all severities**: Incidents of any severity and incident updates 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, Groups, or top-level Smart 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.

To Configure a Notification Profile

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

1. Select **Administration** in the Navigation pane.
2. Select **Local Users** in the Navigation pane.

   The Users tab is displayed.
3. Select the user for whom you want to configure notifications.
4. Click the **Configure Notification Profile** icon.

   The Configure Notification Profile Wizard is displayed.

   If a Notification Profile has already been configured for the user, the existing profile is displayed.
5. Select either **Subscribe to All Messages** or **Subscribe to Custom List of Messages**.
   - If you select Subscribe to All Messages, you receive notifications for all assets.

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

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

     Use the Pager drop-down list to select the severity of messages to be received through a pager.
   - If you select Subscribe to Custom List of Messages, the Configure Group Notifications page is displayed. You receive the specified priority of notifications for each Virtualization Pool and Group.

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

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

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

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

   The Summary page is displayed.
8. Click **Update Notification Profile**.

   The new notification profile is applied.

Deleting a Notification Profile

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

To Delete a Notification 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 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.

8

Backup and Recovery

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

The following features and topics are covered in this chapter:

Introduction to Backup and Recovery

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 `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. You can specify the name and location of the backup file and the log file. The `ecadm backup` command does not back up software and storage library contents. Run the `ecadm backup` command regularly and save the backup file on a separate system.

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

Some of the procedures described in this section use the `ecadm` and `proxyadm` commands. See the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about this command.

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

Backing Up 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/images/os` directory. This is because the size of some of the OS image files in this directory can be prohibitively large.

In addition to running the `ecadm backup` command, you should back up the `/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.

To Back Up an Enterprise Controller

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. If you are using a customer-managed database, you can back up the database schema using the `--remotedb` option, or you can use the existing backup and recover processes implemented by your database administrator.

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

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

   - **-o | --output <backup file>**: Specify the file in which the backup archive is generated. Do not specify a path inside the `/opt/*xvm*` directories. The default output file is `/var/tmp/sat-backup-<date>-<time>.tar`.
   - **-c | --configdir <dir>**: Specify an alternate backup configuration directory.
   - **-l | --logfile <logfile>**: Save output from command in <logfile>. Log files are stored in the `/var/opt/sun/xvm/logs/` directory.
   - **-d | --description <description string>**: Embed the <description string> as the description of the backup archive.
   - **-r | --remotedb**: If the Enterprise Controller uses a customer-managed database, export the database schema to a file in the `/var/tmp/ocdumpdir` directory on the database server. This does not perform a full database backup, which the database administrator should perform separately.
   - **-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 verbosity level (may be repeated)

   For example:

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

```
ecadm: *** Output in /var/backup/EC-12December.tar
ecadm: *** Log in /var/opt/sun/xvm/logs/sat-backup-2012-12-17-16:21:12.log
```

3. Save the contents of the most recent upgrade installation directory. This directory is a child of the `/var/opt/sun/xvm/update-saved-state/` directory, and is named according to the version number.
4. Copy the backup file to a separate system.

Restoring an Enterprise Controller

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

To Restore an Enterprise Controller

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

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

1. Prepare the Enterprise Controller system.
   - If you are restoring the backup on a new system, then the host name and Enterprise Controller software version of the restored system must match those of the backed up system.
   - If you are restoring the backup on the same system, but the software has become corrupt or an upgrade failed, uninstall the Enterprise Controller software.

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

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

   - If you are restoring the backup on the same system, and the software is functioning normally, unconfigure the Enterprise Controller.
2. Install the Enterprise Controller if it has not been installed, but do not configure the Enterprise Controller, as the `ecadm restore` command restores your configuration settings.
   - Oracle Solaris OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*.
   - Linux OS: See the *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*.
3. Upgrade the Enterprise Controller to the same version that was running when the backup was made, if it is not already running that version. Perform this upgrade from the command line.
4. Run the `ecadm` command with the `restore` subcommand and the `-i <backup directory location and file name>` flag.

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

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

For example:

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

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

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

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

Example: Restoring an Enterprise Controller With an Embedded Database

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

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

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

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

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

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

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

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

9

High Availability

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

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

The following features and topics are covered in this chapter:

Introduction to High Availability

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 the *Oracle Enterprise Manager Ops Center Feature Reference Guide* for more information about this command.

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

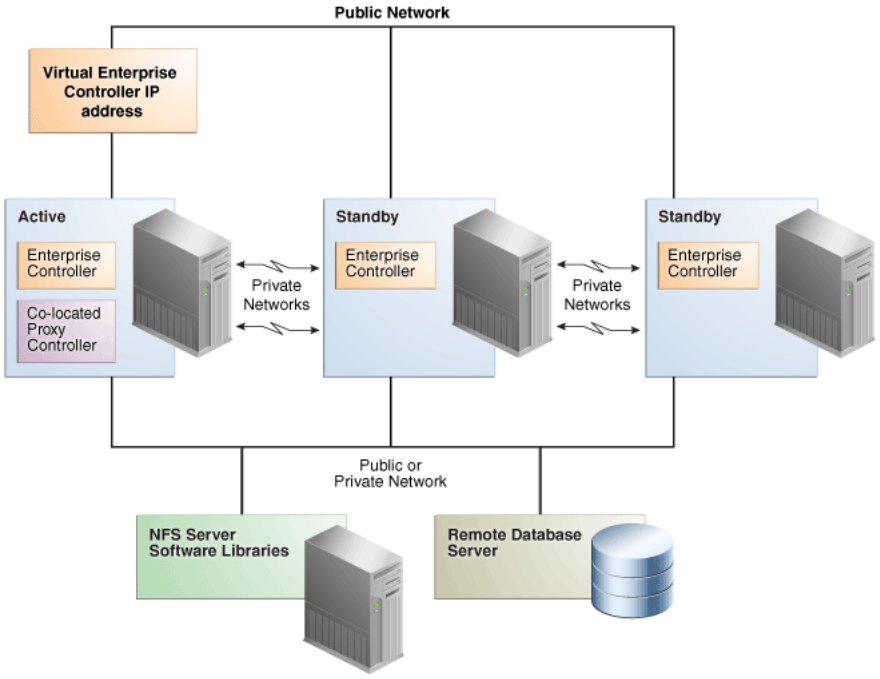
Enterprise Controller High Availability

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

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

Figure 9–1, "Enterprise Controller High Availability Configuration" shows an example Enterprise Controller High Availability configuration.

Figure 9–1 Enterprise Controller High Availability Configuration



Requirements

- 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 `/n1gc-setup/.version.properties` file. The product.version property lists the specific revision level of the installed software. For example:

```
cat /n1gc-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=12.1.2.2161
product.installLocation=/var/opt/sun/xvm/EnterpriseController_installer_
12.1.2.2161
#
```

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

Limitations

- 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 and its co-located Proxy Controller and not to other standalone Proxy Controllers.

Proxy Controller High Availability

Each asset, such as a server or operating system, is managed by a specific Proxy Controller. If a Proxy Controller fails or is uninstalled, you are prompted to migrate assets to another Proxy Controller if one is available.

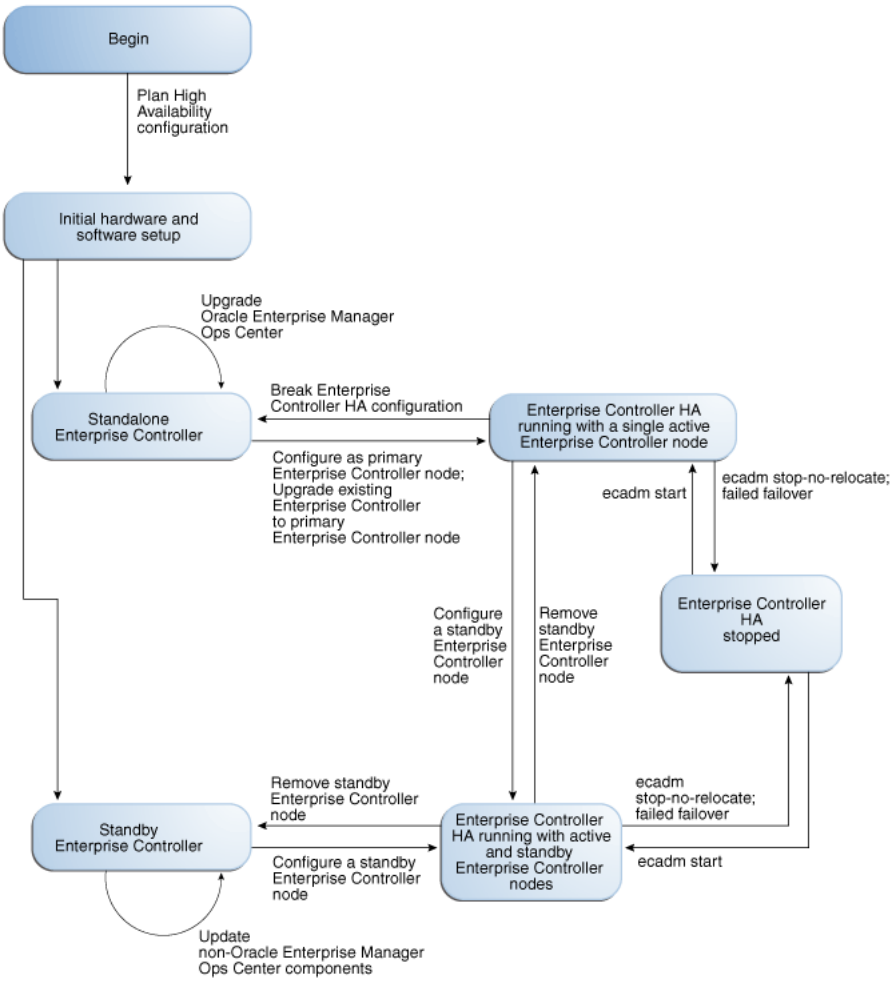
You can also manually move assets to a new Proxy Controller.

Using Enterprise Controller High Availability

You can use Oracle Clusterware and Oracle Real Application Cluster software to create a High Availability configuration. A High Availability configuration includes one active Enterprise Controller node and one or more standby Enterprise Controller nodes, all using an external database. If the active Enterprise Controller node fails, a standby node is made active, and a notification is sent to notify the user that the relocate has occurred.

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

Figure 9–2 Enterprise Controller High Availability States



Converting a Single Enterprise Controller to High Availability

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

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

Preparing for High Availability with Oracle Clusterware

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

Installing Oracle Clusterware

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

Making the Current Enterprise Controller the Active Node

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

To Make the Current Enterprise Controller the Active Node

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

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

   For example:

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

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 using the following format:
   - `http_proxy: <protocol>://<host>:<port>`: This variable specifies the proxy server to use for HTTP.
   - `https_proxy: <protocol>://<host>:<port>`: This variable specifies the proxy server to use for HTTPS.
2. If you are installing on Oracle Solaris 11, configure root as a normal user using the following command:

```
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.i386.12.1.2.2140.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.i386.12.1.2.2140.zip
# ls
enterprise-controller.Solaris.i386.12.1.2.2140.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.i386.12.1.2.2140.tar.zip | tar xf -
# ls
enterprise-controller.Solaris.i386.12.1.2.2140.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.

   For example:

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

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 12.1.2.2140 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=nge1
```

```
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 a High Availability Configuration to a Single Enterprise Controller

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

   The node is removed from the cluster.
3. As root, log on to the active Enterprise Controller node.
4. Use the `ecadm` command with the `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 Cause a Relocate

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.

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

Managing HA Network Resources

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

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

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

Adding a Network Resource

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

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

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

The following options are included in this format:

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

Modifying a Network Resource

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

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

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

The following attributes can be modified:

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

- `PLACEMENT=favored`

Removing a Standby Enterprise Controller Node

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

To Remove a Standby Enterprise Controller Node

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 Enterprise Controller Cluster

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 Temporarily Shut Down the Active Enterprise Controller Without a Relocate

1. As root, log on to the active Enterprise Controller node.
2. Use the `ecadm` command with the `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 `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 Access the Cluster Management UI

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.

Using Proxy Controller High Availability

Each asset is managed by a specific Proxy Controller. 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. 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.

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.

To Migrate Assets from a Failed Proxy Controller

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. Select the destination Proxy Controller from the list of Proxy Controllers, or select **Auto Balance across Proxy Controllers** 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.

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

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. Select the destination Proxy Controller from the list of Proxy Controllers, or select **Auto Balance across Proxy Controllers** 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.

10

Upgrading

You can upgrade to the latest version of Oracle Enterprise Manager Ops Center 12*c* if you are currently using Oracle Enterprise Manager Ops Center 12*c*, or upgrade to Oracle Enterprise Manager Ops Center 12c if you are currently using Oracle Enterprise Manager Ops Center 11*g* Release 1 Update 3.

The following features and topics are covered in this chapter:

Introduction to Upgrading

You can upgrade to the latest version of Oracle Enterprise Manager Ops Center from Oracle Enterprise Manager Ops Center 12*c*. If you are using Oracle Enterprise Manager Ops Center 11*g* Update 3, you must upgrade to version 12.1.1.0.0 before upgrading to the latest version.

Some of the procedures described in this section use the `ecadm`, `proxyadm`, and `agentadm` commands. See the Oracle Enterprise Manager Ops Center Feature Reference Guide 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.

> **Note:** If you are currently using Oracle Enterprise Manager Ops Center 11*g*, you must use the `satadm` command in place of the `ecadm` command. These commands serve the same purpose and use the same syntax for the purposes of these procedures.

Planning The Upgrade

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

- Review the *Oracle Enterprise Manager Ops Center Release Notes* for pre-installation requirements and known issues.
- Verify that your system meets the system requirements outlined in the *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System* or *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*, since some system requirements have changed.

  You can use the OCDoctor to check system requirements. See `http://java.net/projects/oc-doctor` for more information about the OCDoctor.
- If you made changes to the uce.rc file, the upgrade erases your changes. Copy your changes to the .uce.rc file before beginning the upgrade.
- If you replaced the self-signed web server certificate for the Enterprise Controller, the upgrade erases your web server configuration changes, and might erase the certificate. Copy the certificate to a safe location before beginning the upgrade. After the upgrade, reapply your configuration changes and copy the certificate to its original location.
- If you are upgrading from version 11g to version 12c, changes to several features require you to make several changes to your environment:
  - Discovery criteria from version 11g are converted to discovery profiles, but you must create new credentials and associate them with the new discovery profiles before you can use them to discover assets.
  - Any assets that were discovered but not managed by a version 11g Enterprise Controller must be rediscovered in version 12c.
  - You must create and assign management credentials to assets if the credentials used by a Proxy Controller to reach them have changed.
  - Reports from version 11g must be re-run.
  - Solaris Update Compliance reports are no longer supported in version 12c, and Solaris Update Compliance report templates are not migrated.

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. If you are upgrading from version 11g, you can switch to either database configuration. If you are upgrading from version 12c, 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

You can perform upgrades through the user interface or from the command line. If you are upgrading from version 11g and intend to use the embedded Oracle database, you can perform the upgrade from the user interface or from the command line. If you

are upgrading from version 11g and intend to use a customer-managed database, you can perform the upgrade from the command line.

> **Note:** The upgrade process creates a backup file for the Enterprise Controller. If the upgrade fails, the Enterprise Controller is uninstalled, the initial version of the Enterprise Controller is reinstalled, and the system is automatically restored from the backup file.

Upgrade your systems in the following order.

1. Download the upgrade bundles for your environment.
2. Upgrade the Enterprise Controller. This also upgrades the co-located Proxy Controller.

   If you have a High Availability configuration, upgrade your Enterprise Controllers as described in Upgrading the Enterprise Controllers in an HA Configuration.
3. Upgrade the separate Proxy Controllers.
4. Upgrade the Agent Controllers through the UI or manually.

If your data center is large, you can upgrade your Proxy Controllers one at a time. To do so, upgrade your systems in the following order.

1. Download the upgrade bundles for your environment.
2. Upgrade the Enterprise Controller.

   If you have a High Availability configuration, upgrade your Enterprise Controllers as described in Upgrading the Enterprise Controllers in an HA Configuration.
3. Upgrade one Proxy Controller.
4. Upgrade the Agent Controllers managed by the upgraded Proxy Controller.
5. Upgrade the next Proxy Controller.
6. Upgrade the Agent Controllers managed by the upgraded Proxy Controller.
7. Repeat steps 5 and 6 for each Proxy Controller.

In either scenario, once you have begun the upgrade, complete it as soon as possible. Do not allow the Enterprise Controller or Proxy Controllers to be restarted before all systems have been upgraded.

Downloading Upgrades

You can download upgrades for Oracle Enterprise Manager Ops Center. This includes upgrades for the Enterprise Controller, Proxy Controllers, and Agent Controllers. Downloading an upgrade does not install it on managed assets.

You can download the upgrade bundles through the user interface, from the Oracle Technology Network, or from e-Delivery.

Each upgrade bundle contains the previous upgrade bundles, so you only need to download and apply the most recent upgrade in order to upgrade your system.

Downloading Upgrades From Ops Center Downloads

You can download upgrades for Oracle Enterprise Manager Ops Center through the user interface.

Upgrades are downloaded to these directories:

- Enterprise Controller upgrades: `/var/opt/sun/xvm/images/productUpdate`
- Proxy Controller upgrades: `/var/opt/sun/xvm/images/productUpdate`
- Agent Controller upgrades: `/var/opt/sun/xvm/images/agent`

To View and Download Upgrades

1. Click the **Enterprise Controller** in the Administration section of the Navigation pane.
2. Click **Ops Center Downloads**.

   The Ops Center Downloads Wizard is displayed.
3. (Optional) Hover over the details icon for a download to view more information about it.
4. Select one or more downloads and click **Next**.

   The View License page is displayed.
5. Read the license and click **Accept**.

   The Download Status page is displayed.
6. Check **I wish to download the remaining upgrades in the background**, or wait for the downloads to complete.
7. Click **Next**.

   The Summary page is displayed.
8. Click **Finish**.

   The upgrades are now available.

Downloading Upgrades From the Oracle Technology Network

You can download upgrade bundles for the Enterprise Controller and Proxy Controller from the Oracle Technology Network.

1. Log in to the Oracle Technology Network Oracle Enterprise Manager Ops Center page at `http://www.oracle.com/technetwork/oem/ops-center/index.html`.
2. Click **Enterprise Manager Ops Center** in the Enterprise Manager Downloads sidebar.
3. Select **Accept License Agreement**.
4. Download the appropriate bundle.
   - Click the Enterprise Controller bundle with the correct operating system and architecture to download the full bundle. This bundle contains the Enterprise Controller and Proxy Controller files for the selected architecture and operating system, and Agent Controller files for every supported operating system and architecture.

- Click the Proxy Controller bundle with the correct operating system and architecture to download the Proxy Controller installation bundle. This bundle is used to manually install remote Proxy Controllers.

Downloading Upgrades From e-Delivery

You can download upgrade bundles for the Enterprise Controller and Proxy Controller from e-Delivery.

To Download Upgrades From e-Delivery

1. Log in to the Oracle e-Delivery website at http://edelivery.oracle.com.
2. Read and accept the Software License Agreement and Export Restrictions, then click **Continue**.
3. Select the Oracle Enterprise Manager product pack and the correct platform for your environment, then click **Go**.

   The list of download packs is displayed.
4. Select the Oracle Enterprise Manger Ops Center 12*c* Release 1 Media Pack and click **Continue**.

   The list of available bundles is displayed.
5. Download the appropriate bundle.
   - Click **download** next to the Enterprise Controller bundle with the correct operating system and architecture to download the full bundle, then save the downloaded bundle locally. This bundle contains the Enterprise Controller and Proxy Controller files for the selected architecture and operating system, and Agent Controller files for every supported operating system and architecture.
   - Click **download** next to the Proxy Controller bundle with the correct operating system and architecture to download the Proxy Controller installation bundle, then save the downloaded bundle locally. This bundle is used to manually install remote Proxy Controllers.

Upgrading the Enterprise Controllers

Once you have downloaded an upgrade bundle, you can upgrade your Enterprise Controllers.

You can perform upgrades through the user interface or from the command line. If you are upgrading from version 11g and intend to use the embedded Oracle database, you can perform the upgrade from the user interface or from the command line. If you are upgrading from version 11g and intend to use a customer-managed database, you can perform the upgrade from the command line.

Upgrading the Enterprise Controllers in an HA Configuration

If you have multiple Enterprise Controllers in a high availability configuration, you can upgrade them together.

Before You Begin

Perform the following tasks before you upgrade the Enterprise Controller:

- Download the Enterprise Controller upgrade.

- Review pending and scheduled jobs before updating the Enterprise Controller. The upgrade shuts down the Enterprise Controller, which causes running jobs to fail.
- Use the OCDoctor to verify that there are no outstanding issues on the Enterprise Controller systems. Log in to each Enterprise Controller system, then run the OCDoctor with the `--update` option, then run the OCDoctor script with the `--troubleshoot` option. See the OCDoctor chapter for more information about the OCDoctor.

To Upgrade the Enterprise Controllers in an HA Configuration

1. If one of the Enterprise Controller nodes has a co-located Proxy Controller, make it the primary node using the `ecadm` command with the `ha-relocate` subcommand.
2. If multiple Enterprise Controller nodes have co-located Proxy Controllers, migrate all of the assets from these Proxy Controllers to a remote Proxy Controller or to the Proxy Controller of the primary node as described in Migrating Assets Between Proxy Controllers.
3. On each standby node, use the `ecadm` command with the `ha-unconfigure-standby` subcommand to unconfigure the standby nodes from the HA configuration.
4. Uninstall the Enterprise Controller software on the standby nodes as described in Uninstalling and Unconfiguring the Enterprise Controller, then reboot the systems.
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. On the remaining Enterprise Controller system, update the `start/exec` property in the the `svc:/application/scn/satellite-enable` SMF service.

   a. Change the `start/exec` property for the `svc:/application/scn/satellite-enable` service to `:true`. For example:

   ```
   # /usr/sbin/svccfg
   svc:> select svc:/application/scn/satellite-enable
   svc:/application/scn/satellite-enable> setprop start/exec = :true
   svc:/application/scn/satellite-enable> end
   ```

   b. Refresh the `svc:/application/scn/satellite-enable` service. For example:

   ```
   # /usr/sbin/svcadm refresh svc:/application/scn/satellite-enable:default
   ```

   c. Confirm that the property has been changed. For example:

   ```
   # svcprop -p start/exec svc:/application/scn/satellite-enable:default
   :true
   ```
7. Use the `ecadm` command with the `start` subcommand and the `-w` option to start the active node.

   The Enterprise Controller is restarted.
8. Upgrade the active node using the Upgrading a Single Enterprise Controller from the User Interface procedure or the Upgrading a Single Enterprise Controller from the Command Line procedure.
9. Convert the upgraded standalone Enterprise Controller to an HA configuration as described in Converting a Single Enterprise Controller to High Availability. This

procedure includes installing the latest Enterprise Controller version on the standby nodes.

Upgrading a Single Enterprise Controller from the User Interface

The following procedure describes how to upgrade the Enterprise Controller. You can view and install upgrades from the user interface.

Upgrade log files are stored in the `/var/opt/sun/xvm/update-saved-state` directory on the Enterprise Controller.

Note: If you are currently using Oracle Enterprise Manager Ops Center 11g, you must upgrade your systems from the command line.

Before You Begin

Perform the following tasks before you upgrade the Enterprise Controller:

- Download the Enterprise Controller upgrade bundle.
- Review pending and scheduled jobs before updating the Enterprise Controller. The upgrade shuts down the Enterprise Controller, which causes running jobs to fail.
- Use the OCDoctor to verify that there are no outstanding issues on the Enterprise Controller system. Log in to the Enterprise Controller, then run the OCDoctor with the `--update` option, then run the OCDoctor script with the `--troubleshoot` option. See the OCDoctor chapter for more information about the OCDoctor.
- When you are using an embedded database, verify that the Oracle Database 11g Enterprise Edition version 11.2.0.3 installation files used during the Oracle Enterprise Manager Ops Center installation are present in the `/var/tmp/downloads` directory on the Enterprise Controller system. Follow this procedure to download the installation files if they are missing:

Note: The download procedure requires a valid My Oracle Support (MOS) account, which must be associated with a Customer Service Identifier (CSI) with a software contract.

---

a. Create a `/var/tmp/downloads` directory on the Enterprise Controller system.

b. Navigate to `http://support.oracle.com`, click Sign In, and sign in with your MOS credentials.

c. Click the Patches & Updates tab.

d. Enter 10404530 in the field next to Patch Name or Number.

e. Click the Add Filter icon, then select your Enterprise Controller system's operating system and architecture in the drop-down menu next to Platform.

f. Click Search.

The Oracle Database 11g Enterprise Edition version 11.2.0.3 patch set is displayed.

g. Click Download.

The file download popup is displayed.

h. Download the first two files. For Oracle Solaris, these files end with `_1of6.zip` and `_2of6.zip`. For Linux, these files end with `_1of7.zip` and `_2of7.zip`

i. Copy or move the downloaded installation bundles to the `/var/tmp/downloads` directory on the Enterprise Controller system.

To Upgrade the Enterprise Controller

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

   The Upgrade Enterprise Controller Wizard is displayed. All available Enterprise Controller upgrades are displayed.
3. (Optional) Mouse over the details icon for an upgrade to view more information about it.
4. Select an upgrade and click **Next**. If the current Oracle Enterprise Manager Ops Center installation file cannot be found, the Install Path Verification page is displayed. If the upgrade fails, the installation file is used for rollback.
5. If the Install Path Verification page is displayed, enter the path to the Oracle Enterprise Manager Ops Center installer and click **Next**. By default, the upgrade process uses the `/var/opt/sun/xvm/update-saved-state/` directory to back out the changes if the upgrade fails. If this directory is not present, the installer for the previous version is used to reinstall the older version and restore the system.
6. The Job Details page is displayed. When the upgrade shuts down the Enterprise Controller, any jobs that are running fail. View the job details, then click **Next**. The Summary page is displayed.
7. Click **Finish**.

   The upgrade is launched. The upgrade can take up to an hour, during which time the Enterprise Controller is not accessible. Reload the browser regularly, and the login page displays normally when the upgrade is complete.
8. If you are upgrading from version 12c to version 12c update 1, and your environment uses a customer-managed database, update the database privileges.

   a. Copy the `refactorOCPrivs_12.1.1.0.sql` script, from the Enterprise Controller system to the customer-managed database system.

      On Oracle Solaris systems, this script is in the `/opt/ORCLsysman-db/sql/update/delta-update1/oracle/` directory.

      On Linux systems, this script is in the `/opt/orcl-sysman-db/sql/update/delta-update1/oracle/` directory.

   b. Run the SQL script as the SYS User. When you are prompted, provide the schema names for the Ops Center database login and Read-Only Ops Center database login for the appropriate prompts. These parameters were provided when the inital Ops Center logins were created using the `createOCSchema_remote.sql` script. These parameters are visible in the `/opt/sun/xvm/db.properties` file as `mgmtdb.appuser` and `mgmtdb.roappuser`.

      For example:

      ```
      sqlplus / as sysdba @refactorOCPrivs_12.1.1.0.sql

      Enter username for Ops Center database login: OC
      Enter username for read only Ops Center database login: OC_RO
      ```

9. Clear the browser cache and refresh the browser before you log in to the newly upgraded Enterprise Controller.
10. Back up your Oracle Enterprise Manager Ops Center data using the `ecadm` command and the `backup` subcommand.

Upgrading a Single Enterprise Controller from the Command Line

The following procedures describe how to upgrade the Enterprise Controller, with either an embedded database or a customer-managed database. If you are running Oracle Enterprise Manager Ops Center in Disconnected Mode, you must upgrade from the command line. The co-located Proxy Controller is upgraded as well, even if it is not enabled.

The Enterprise Controller upgrade log is saved locally as `/var/opt/sun/xvm/update-saved-state/update_satellite_bundle_<version number>/updatelog.txt`.

Upgrade log files are stored in the `/var/opt/sun/xvm/update-saved-state` directory on the Enterprise Controller.

If an error occurs during this process, the system is restored to the prior version.

Before You Begin

Perform the following tasks before you upgrade the Enterprise Controller:

- Verify that the Enterprise Controller has at least five (5) GB of free space for the upgrade bundle.
- Acquire the upgrade bundle from Oracle and transfer it to the Enterprise Controller system.
- Review pending and scheduled jobs before updating the Enterprise Controller. The upgrade shuts down the Enterprise Controller, which causes running jobs to fail. Scheduled jobs cannot be launched while the upgrade is being applied.
- Use the OCDoctor to verify that there are no outstanding issues on the Enterprise Controller system. Log in to the Enterprise Controller, then run the OCDoctor with the `--update` option, then run the OCDoctor script with the `--troubleshoot` option. See the OCDoctor chapter for more information about the OCDoctor.
- If you upgrading from Oracle Enterprise Manager Ops Center 11g and you plan to use a customer-managed database, you must identify a system with an Oracle Database Enterprise Edition database that serves as the Oracle Enterprise Manager Ops Center repository.
- When you are using an embedded database, or are upgrading from Oracle Enterprise Manager Ops Center 11g and you plan to use an embedded database, verify that the Oracle Database 11g Enterprise Edition version 11.2.0.3 installation files are present in the `/var/tmp/downloads` directory on the Enterprise Controller system. Follow this procedure to download the installation files if they are missing:

  Note: This procedure requires a valid My Oracle Support (MOS) account, which must be associated with a Customer Service Identifier (CSI) with a software contract.

  a. Create a `/var/tmp/downloads` directory on the Enterprise Controller system.

b. Navigate to http://support.oracle.com, click Sign In, and sign in with your MOS credentials.

c. Click the Patches & Updates tab.

d. Enter 10404530 in the field next to Patch Name or Number.

e. Click the Add Filter icon, then select your Enterprise Controller system's operating system and architecture in the drop-down menu next to Platform.

f. Click Search.

   The Oracle Database 11g Enterprise Edition version 11.2.0.3 patch set is displayed.

g. Click Download.

   The file download popup is displayed.

h. Download the first two files. For Oracle Solaris, these files end with `_1of6.zip` and `_2of6.zip`. For Linux, these files end with `_1of7.zip` and `_2of7.zip`

i. Copy or move the downloaded installation bundles to the `/var/tmp/downloads` directory on the Enterprise Controller system.

Upgrading the Enterprise Controller With an Embedded Database

This procedure describes how to upgrade an Enterprise Controller with an embedded database. If you are using version 11g, this procedure installs and configures the embedded database.

1. As root, log in to the Enterprise Controller.
2. Verify that the Enterprise Controller is online.
   - If you are currently using Oracle Enterprise Manager Ops Center 12c, use the `ecadm` command to verify that the Enterprise Controller is online. If necessary, use the `ecadm start` command to start the Enterprise Controller.

     ```
     # /opt/SUNWxvmoc/bin/ecadm status
     online
     ```

   - If you are currently using Oracle Enterprise Manager Ops Center 11g, use the `satadm` command to verify that the Enterprise Controller is online. If necessary, use the `satadm start` command to start the Enterprise Controller.

     ```
     # /opt/SUNWxvmoc/bin/satadm status
     online
     ```

3. Create a temporary directory within the directory where you installed Oracle Enterprise Manager Ops Center, then copy or move the upgrade bundle to the new directory. For example:

   ```
   # mkdir /var/tmp/OC/update
   # cp enterprise-controller.Solaris.sparc.12.1.0.2001.tar.zip /var/tmp/OC/update
   ```

4. Change to the directory containing the upgrade bundle.

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

5. Unzip and un-tar the 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. For example:

```
# unzip enterprise-controller.Solaris.i386.12.1.0.2001.tar.zip | tar xf -
# ls
enterprise-controller.Solaris.i386.12.1.0.2001.tar.zip
xvmoc_full_bundle
#
```

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

```
# unzip enterprise-controller.Solaris.i386.12.1.0.2001.zip
# ls
enterprise-controller.Solaris.i386.12.1.0.2001.zip
xvmoc_full_bundle
#
```

6. Change to the `xvmoc_full_bundle` directory and run the install script.

```
# cd xvmoc_full_bundle
# ./install
```

The following option can be used with the install script:

--verbose or -v: Increases verbosity of output from upgrade program. Without this option, non-verbose output is given.

When the upgrade is complete, the install script indicates that all Oracle Enterprise Manager Ops Center components have been upgraded to the latest version.

7. Clear your browser cache and refresh your browser before you log in to the newly upgraded Enterprise Controller.
8. Back up your Oracle Enterprise Manager Ops Center data using the `ecadm` command and the `backup` subcommand.

Upgrading the Enterprise Controller With a Customer-Managed Database

This procedure describes how to upgrade an Enterprise Controller with a customer-managed database. If you are using version 11g, this procedure configures Oracle Enterprise Manager Ops Center to use a customer-managed database.

1. As root, log in to the Enterprise Controller.
2. Verify that the Enterprise Controller is online.
   - If you are currently using Oracle Enterprise Manager Ops Center 12c, use the `ecadm` command to verify that the Enterprise Controller is online. If necessary, use the `ecadm start` command to start the Enterprise Controller.

```
# /opt/SUNWxvmoc/bin/ecadm status
online
```

   - If you are currently using Oracle Enterprise Manager Ops Center 11g, use the `satadm` command to verify that the Enterprise Controller is online. If necessary, use the `satadm start` command to start the Enterprise Controller.

```
# /opt/SUNWxvmoc/bin/satadm status
online
```

3. Create a temporary directory within the directory where you installed Oracle Enterprise Manager Ops Center, then copy or move the upgrade bundle to the new directory. For example:

```
# mkdir /var/tmp/OC/update
# cp enterprise-controller.Solaris.sparc.12.1.0.2001.tar.zip /var/tmp/OC/update
```

4. Change to the directory containing the upgrade bundle.

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

5. Unzip and un-tar the 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. For example:

```
# unzip enterprise-controller.Solaris.i386.12.1.0.2001.tar.zip | tar xf -
# ls
enterprise-controller.Solaris.i386.12.1.0.2001.tar.zip
xvmoc_full_bundle
#
```

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

```
# unzip enterprise-controller.Solaris.i386.12.1.0.2001.zip
# ls
enterprise-controller.Solaris.i386.12.1.0.2001.zip
xvmoc_full_bundle
#
```

6. If you are upgrading from version 11g, copy the `createOCschema_remote.sql` script from the `/var/tmp/OC/xvmoc_full_bundle/<Enterprise Controller OS>/Product/installer/scripts` directory on the Enterprise Controller to the customer-managed database server. As the customer-managed database administrator, run the 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.
   - **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.

When you enter all of the required information, the `createOCschema_remote.sql` script indicates completion and exits.

For example:

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

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

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


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

Enter username for Ops Center database login: TESTSCHEMA
Enter password for Ops Center database login:
Enter username for read only Ops Center database login: TESTSCHEMA_RO
Enter password for read only Ops Center database login:
Enter default tablespace for Ops Center user: USERS
Enter temporary tablespace for Ops Center user: TEMP
Enter Oracle Data Pump destination directory: /var/tmp/ocdumpdir

"Done creating OC_SYSTEM_ROLE and OC_RO_ROLE"
"Done creating Schema 'TESTSCHEMA'. Roles and privileges have been granted."
"Done creating Schema 'TESTSCHEMA_RO'. Roles and privileges have been granted."
"Done creating OC_DUMP_DIR at /var/tmp/ocdumpdir"
"Done granting privs to users and profiles"
"Testing connectivity to the new schema: 'TESTSCHEMA'"
Connected.
"Testing connectivity to the new read only schema: 'TESTSCHEMA_RO'"
Connected.

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


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

7. If you are upgrading from version 11g, create a database properties file on the Enterprise Controller system. The database properties file must contain the location of the customer-managed database and the same user and read-only user credentials supplied in the schema creation script.

   For example:

   ```
   # vi /var/tmp/OC/DB/RemoteDBProps.txt
   mgmtdb.appuser=user
   mgmtdb.password=userpass
   mgmtdb.roappuser=user
   mgmtdb.ropassword=userpass
   mgmtdb.dburl=jdbc:oracle:thin:@<database host name>:<port>/<database service
   name>
   ```

8. Change to the `xvmoc_full_bundle` directory and run the `install` script. If you are upgrading from version 11g, use the `-remoteDBprops=<credentials file>` option.

The following option can be used with the install script:

--verbose or -v: Increases verbosity of output from upgrade program. Without this option, non-verbose output is given.

For example, to upgrade from version 12c to version 12c update 1:

```
# cd xvmoc_full_bundle
# ./install
```

For example, to upgrade from version 11g to version 12c update 1:

```
# cd xvmoc_full_bundle
# ./install -remoteDBprops=/var/tmp/OC/DB/RemoteDBProps.txt
```

When the upgrade is complete, the install script indicates that all Oracle Enterprise Manager Ops Center components have been upgraded to the latest version.

9. If you are upgrading from version 12c to version 12c update 1, and your environment uses a customer-managed database, update the database privileges for the OC system schema and OC_SYSTEM_ROLE.

   a. Copy the `refactorOCPrivs_12.1.1.0.sql` script, from the Enterprise Controller system to the customer-managed database system.

      On Oracle Solaris systems, this script is in the `/opt/ORCLsysman-db/sql/update/delta-update1/oracle/` directory.

      On Linux systems, this script is in the `/opt/orcl-sysman-db/sql/update/delta-update1/oracle/` directory.

   b. Run the SQL Script as the SYS User. When you are prompted, provide the schema names for the Ops Center database login, Read-Only Ops Center database login, and default tablespace for the appropriate prompts. These parameters were provided when the inital Ops Center logins were created using the `createOCSchema_remote.sql` script. The database login and read-only database login parameters are visible in the `/opt/sun/xvm/db.properties` file as `mgmtdb.appuser` and `mgmtdb.roappuser`. The default tablespace is visible in the `/opt/ORCLsysman-db/etc/llocalOracleConfig.properties` file as `remote_default_ts`.

      For example:

      ```
      sqlplus / as sysdba @refactorOCPrivs_12.1.1.0.sql

      Enter username for Ops Center database login: OC
      Enter username for read only Ops Center database login: OC_RO
      Enter default tablespace for the Ops Center database login: USERS
      ```

10. Clear your browser cache and refresh your browser before you log in to the newly upgraded Enterprise Controller.

11. Back up your Oracle Enterprise Manager Ops Center data using the `ecadm` command with the `backup` subcommand and the `-r` option.

Upgrading Proxy Controllers

Once you have downloaded an upgrade bundle, you can upgrade your Proxy Controllers.

Upgrading a Proxy Controller from the User Interface

You can remotely upgrade Proxy Controllers to the latest available version.

Proxy Controller files are stored in the `/var/opt/sun/xvm/images/productUpdate` directory. If you are using Connected Mode, use the Ops Center Downloads action to download Proxy Controller files. If you are using Disconnected Mode, you must add the Proxy Controller files to the `/var/opt/sun/xvm/images/productUpdate` directory before they can be used.

To upgrade a Proxy Controller through the UI, the Enterprise Controller must be able to reach the Proxy Controller with an SSH connection using port 22 during the upgrade process. This connection is used to transfer Proxy Controller bundles and execute commands on the Proxy Controller system. If your security restrictions do not allow this connection, upgrade the Proxy Controller from the command line.

Before You Begin

Perform the following tasks before you upgrade the Proxy Controller:

- Upgrade the Enterprise Controller.
- Download the Proxy Controller upgrade.

To Upgrade a Proxy Controller

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

   Proxy Controller information is displayed.
3. Select one or more Proxy Controllers.
4. Click the **Upgrade to Latest Available Version** icon in the center pane.

   The Upgrade Wizard is displayed.
5. Select a method for providing SSH credentials for the Proxy Controller or Proxy Controllers.
   - Re-use the SSH credentials used during discovery
   - Apply the same SSH credentials to all
   - Enter SSH credentials for each
6. Click **Finish**.

   A job is launched to update the Proxy Controllers.

Upgrading a Proxy Controller from the Command Line

You can manually update Proxy Controllers to the latest available version to gain access to new and updated features.

The Proxy Controller upgrade log is saved locally as `/var/opt/sun/xvm/update-saved-state/update_proxy_bundle_<version number>/updatelog.txt`.

If an error occurs during this process, the system is restored to the prior version.

Note: During the upgrade process, the Proxy Controller is shut down. However, the Proxy Controller must be online at the beginning of the process.

Before You Begin

Proxy Controller files are stored in the `/var/opt/sun/xvm/images/productUpdate` directory on the Enterprise Controller. If you are using Connected Mode, use the Ops Center Downloads action to download Proxy Controller files, then move them to the Proxy Controller system. If you are using Disconnected Mode, Proxy Controller files must be downloaded outside of Oracle Enterprise Manager Ops Center and moved to the Proxy Controller system.

To Upgrade a Proxy Controller

1. As root, log in to the Proxy Controller system.
2. Back up the contents of the following directory:
   - `/etc/opt/sun/cacao2/instances/scn-proxy/security/` on a Linux Proxy Controller
   - `/etc/cacao/instances/scn-proxy/security/` on an Oracle Solaris Proxy Controller
3. Run the `proxyadm` command with the `status` subcommand to verify that the Proxy Controller is online. If the Proxy Controller is offline, start it using the `proxyadm` command with the `start` subcommand.

   For example:

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

4. Change to the directory containing the upgrade bundle.
5. Uncompress and un-tar the installation archive, then list the contents of the temporary directory.
   - For example, on a Linux Proxy Controller:

     ```
     # unzip proxy-controller.Linux.i686.12.1.0.2001.tar.zip
     # tar xf proxy-controller.Linux.i686.12.1.0.2001.tar
     # ls
     xvmoc_full_bundle
     proxy-controller.Linux.i686.12.1.0.2001.tar
     #
     ```

   - On an Oracle Solaris Proxy Controller:

     ```
     # gzcat proxy-controller.Solaris.i386.12.1.0.2001.tar.zip | tar xf -
     # ls
     xvmoc_full_bundle
     proxy-controller.Solaris.i386.12.1.0.2001.tar.zip
     ```

6. Change to the `xvmoc_full_bundle` directory.
7. Run the install script.

   ```
   # ./install
   ```

   The following options may be used with the install script:

--install <version 11g install bundle path>or-i <version 11g install bundle path>: If you removed the `/var/opt/sun/xvm/update-saved-state/` directory, you must use this option to specify the location of the Oracle Enterprise Manager Ops Center 11g install bundle. If the directory is present, this option is unnecessary.

The upgrade is installed on the Proxy Controller. When the upgrade is complete, the install script indicates that all components have been upgraded.

Upgrading Agent Controllers

Once you have upgraded your Enterprise Controllers and Proxy Controllers, you can upgrade your Agent Controllers.

Upgrading Agent Controllers from the User Interface

You can remotely upgrade Agent Controllers to the latest available version.

Agent Controller files are stored in the `/var/opt/sun/xvm/images/agent` directory. If you are using disconnected mode, you must add Agent Controller files to the `/var/opt/sun/xvm/images/agent` directory before they can be used.

To Upgrade Agent Controllers

1. Select one or more assets with Agent Controllers.
   - Select an asset from the All Assets section of the Assets tab.
   - Select a group that contains operating systems.
2. Click **Upgrade Agent Controller** if you selected one asset, or **Upgrade All Agent Controllers** if you selected a group.

   The Upgrade Agent Controllers page is displayed.
3. Select an upgrade option for the system or systems to be upgraded, then click **Next**.
   - The Automatic upgrade option lets you upgrade Agent Controllers without using SSH credentials. The Agent Controllers must be running for an automatic upgrade.
   - The SSH upgrade using one set of credentials for all targets option prompts you for a single set of SSH credentials for all systems to be upgraded.
   - The SSH upgrade using individual credentials for each target option prompts you for a separate set of credentials for each system to be upgraded.

   The Summary page is displayed.
4. Click **Finish**.

   The Agent Controller upgrade job is launched.

Upgrading Agent Controllers from the Command Line

You can upgrade Agent Controllers manually. Before you upgrade an Agent Controller, you must upgrade the Proxy Controller that manages it.

If you are manually upgrading Agent Controllers running in non-global zones, complete these upgrade steps for any Agent Controller running in the global zone before upgrading all of the non-global zones. The global zone and the non-global zones must all use the same Agent Controller version.

This procedure requires root access.

1. Copy the new Agent Controller bundle from the Enterprise Controller to the client, remove the existing Agent Controller directory, and extract the new Agent Controller bundle.

   For example, on Oracle Solaris Agent Controllers:

   ```
   # scp <IP of Enterprise
   Controller>:/var/opt/sun/xvm/images/agent/SunConnectionAgent.`uname -s`.`uname
   -p`.12.0.0.2001.zip /var/tmp
   # cd /var/tmp
   # rm -r SunConnectionAgent
   # unzip SunConnectionAgent.`uname -s`.`uname -p`.12.1.0.2001.zip
   ```

   On Linux Agent Controllers:

   ```
   # scp -p <IP of Enterprise
   Controller>:/var/opt/sun/xvm/images/agent/SunConnectionAgent.`uname
   -s`.i686.12.1.0.2001.zip /var/tmp
   # cd /var/tmp
   # rm -r SunConnectionAgent
   # unzip SunConnectionAgent.`uname -s`.i686.12.1.0.2001.zip
   ```

2. Use the `agentadm` command with the `stop` subcommand to stop the Agent Controller.

   For example:

   ```
   ./agentadm stop
   ```

3. Install the Agent Controller upgrade.

   ```
   # cd /var/tmp/SunConnectionAgent
   # ./install
   ```

4. Use the `agentadm` command with the `configure` subcommand and the `--keep-connection` option to configure the new Agent Controller.

   For example:

   ```
   # ./agentadm configure --keep-connection
   ```

   This step also starts the Agent Controller.

   Note: The following errors may safely be ignored. These refer to the addition of two sysidcfg scripts, which are already present from a prior `agentadm configure` step, such as from the original version 11g agent installation and configuration. The correct sysidcfg scripts are called properly by sysidcfg.

   ```
   Failed to add the zone configuration automation.
   Failed to add the service tags recreate script.
   ```

5. Verify the connection.

   ```
   # sc-console list-connections
   scn-agent https://172.25.14.21:21165
   urn:scn:clregid:1234567-aaaa-bbbb-cccc-123456789abc:YYYYMMDDHHMMSSss
   ```

Downgrading Agent Controllers

You can remotely revert Agent Controllers to a previously installed version.

To Downgrade Agent Controllers

1. Select a group that contains operating systems with Agent Controllers, then click the Summary tab.
2. Click the **Agent Controllers** tab.

   Agent Controller information is displayed.
3. Select one or more Agent Controllers.
4. Click the **Downgrade to Previously Installed Version** icon in the center pane.

   The Downgrade Wizard is displayed.
5. Select an option for providing credentials.
   - Downgrade without requiring credentials
   - Use an existing set of credentials
   - Create a new set of credentials
6. Click **Submit**.

   A job is launched to downgrade the Agent Controllers.

11

Uninstalling and Unconfiguring

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

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

The following features and topics are covered in this chapter:

Introduction to Uninstalling and Unconfiguring

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

Some of the procedures described in this section use the `ecadm`, `proxyadm`, and `agentadm` commands. See the Oracle Enterprise Manager Ops Center Feature Reference Guide for more information about these commands.

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

Uninstalling and Unconfiguring Agent Controllers

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

Uninstalling and Unconfiguring Agent Controllers from the User Interface

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

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

To Uninstall and Unconfigure Agent Controllers from the User Interface

1. Select **Assets** from the Navigation pane.
2. In the All Assets pane, click the **Managed Assets** tab.

   The list of currently managed assets are displayed in the Managed Assets section.
3. From the Managed Assets list, select the managed OS instance from which you want to remove the Agent Controller.
4. Click the **Delete Assets** icon (*X* icon placed above the list header).

   The Management Credentials page of the Unmanage Assets Wizard is displayed.
5. Provide a set of credentials to access the Agent Controller, then click **Next**.
   - **New**: Click New to create a new set of credentials.

     Enter a name and the credential information, then click Ok.
   - **Select**: Click Select to select an existing set of credentials.

     Select a set of credentials from the list, then click Ok.

   The Summary page is displayed.
6. Click **Finish**.

   A job is launched to uninstall and unconfigure the Agent Controllers.

Uninstalling and Unconfiguring Agent Controllers from the Command Line

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

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

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

To Uninstall and Unconfigure Agent Controllers from the Command Line

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.

   ```
   # ./agentadm unconfigure
   ```

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

Uninstalling and Unconfiguring a Proxy Controller

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

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

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

Unconfiguring and Uninstalling a Proxy Controller from the User Interface

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

To Unconfigure and Uninstall 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. 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.

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.

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.

To Uninstall a Proxy Controller from the Command Line

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 `/n1gc-setup/installer/install` command with the `-e` option to uninstall the Proxy Controller software components from your system. For example:

```
# cd /n1gc-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 12.1.1.2064 on SunOS)

1. Restore file system configuration. [Not Uninstalled]
2. Uninstall Expect. [Not Uninstalled]
3. Uninstall IPMI tool. [Not Uninstalled]
4. Uninstall Agent components. [Not Uninstalled]
5. Uninstall application packages. [Not Uninstalled]
6. Uninstall Core Channel components. [Not Uninstalled]
7. Uninstall Proxy Core components. [Not Uninstalled]
8. Uninstall UCE Http proxy. [Not Uninstalled]
9. Uninstall OS provisioning components. [Not Uninstalled]
10. Stop and delete services. [Uninstalled]
(1 of 10 Uninstalled)

Executing current step: Uninstall OS provisioning components...
```

When complete, the install script indicates that the Proxy Controller has been uninstalled.

Uninstalling and Unconfiguring the Enterprise Controller

Unconfiguring an Enterprise Controller removes user, authentication, and configuration data and unregisters the Enterprise Controller from Oracle. Data about Proxy Controllers and managed systems is retained. If you unconfigure your Enterprise Controller, you must reconfigure it before using Oracle Enterprise Manager Ops Center.

Uninstalling the Enterprise Controller removes the Enterprise Controller software and all Oracle Enterprise Manager Ops Center data.

Unconfiguring the Enterprise Controller

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

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.

Note: Uninstalling the Enterprise Controller does not uninstall a customer-managed database or remove the Oracle Enterprise Manager Ops Center schema.

To Uninstall the Enterprise Controller

1. If the Enterprise Controller is part of an HA configuration and is currently the active note, 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 `/n1gc-setup/installer/install` command with the `-e` option to uninstall the Enterprise Controller software components from your system.

   For example:

   ```
   # cd /n1gc-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 12.1.1.2064 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.

A

Command Line Administration

This chapter explains how to manage the Oracle Enterprise Manager Ops Center Enterprise Controller, Proxy Controller, and Agent Controller from the command line.

The following information is included:

Configuring the Enterprise Controller: ecadm

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

Synopsis

Oracle Solaris OS

```
/opt/SUNWxvmoc/bin/ecadm -V
/opt/SUNWxvmoc/bin/ecadm [ -h | --help ]
/opt/SUNWxvmoc/bin/ecadm subcommand [ options ]
```

Linux OS

```
/opt/sun/xvmoc/bin/ecadm -V
/opt/sun/xvmoc/bin/ecadm [ -h | --help ]
/opt/sun/xvmoc/bin/ecadm subcommand [ options ]
```

Options

The following common options are supported:

`-h| --help`: Displays the usage synopsis for `ecadm`.

`-V| --version`: Displays the version of Oracle Enterprise Manager Ops Center.

Subcommands

The subcommands of ecadm are as follows:

start
Starts the Enterprise Controller services running on the host.

stop
Stops the Enterprise Controller services running on the host.

status
Displays the status of the Enterprise Controller services. Displays either online or offline to the standard output and sets the exit status to reflect the Enterprise Controller service state.

configure
Performs configuration tasks for the Enterprise Controller services. Registers the Enterprise Controller with My Oracle Support.

unconfigure
Performs the inverse operation of configuring the Enterprise Controller. Deregisters the Enterprise Controller.

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

restore
Restores the state data of an Enterprise Controller from a backup archive. If a new system is being used, the system must have the same host name as the original Enterprise Controller. After the successful completion of this command, the Enterprise Controller is in the same operational state that existed at the time of the backup.

If the registration of the Enterprise Controller to My Oracle Support is invalidated with the `ecadm unconfigure` command, any backup archives created during the time the Enterprise Controller was registered become unusable. The Enterprise Controller is no longer able to communicate with My Oracle Support, and the asset data shared between the Enterprise Controller and the hosted servers lose their synchronization.

verify-db
Verifies that the database used for the Enterprise Controller data persistence is available, reachable, and the schemas are setup 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.

maintenance
Changes the state of the database to maintenance state.

migrate
Moves Enterprise Controller data persistence from a local database to a customer-managed database, then removes the local database and the local database server binaries from the Enterprise Controller. The database must be installed in the destination location before beginning this procedure. The Enterprise Controller is shutdown and is restarted on successful completion.

sqlplus
Opens a sqlplus console to the underlying database.

ha-status
Checks the status of the Oracle Clusterware Enterprise Controller resource.

ha-configure-primary
Configures the system as the primary Enterprise Controller in an Oracle Clusterware framework.

ha-configure-standby
Configures the system as a standby Enterprise Controller in an Oracle Clusterware framework.

ha-modify-resource
Modifies the Enterprise Controller Clusterware resource attributes. To modify the Clusterware resource attributes, edit the `/var/opt/sun/xvm/ha/EnterpriseController_HA_clusterware.properties` file with the appropriate changes, and run this command to take effect.

ha-relocate
Switches from the currently active Enterprise Controller node to a different node.

ha-start
Starts the Enterprise Controller Clusterware resource on one of the Clusterware nodes. Starting the Enterprise Controller Clusterware resource causes the Enterprise Controller services to start.

ha-stop-no-relocate
Stops the Enterprise Controller Clusterware resource. Stopping the Enterprise Controller resource causes the currently active node hosting the Enterprise Controller services to be stopped.

ha-unconfigure-primary
Removes the last node hosting the Enterprise Controller in an Oracle Clusterware framework.

ha-unconfigure-standby
Removes a Enterprise Controller node from the Oracle Clusterware framework.

Subcommand options

Common options for all subcommands:

`-h| --help`: Displays the usage synopsis for the subcommand.

`-v| --verbose`: Displays verbose error and informational messages.

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

start
Enter `ecadm start [ -h | --help ] [ -v | --verbose ] [ -c | --cluster ] [ -t | --temporary ] [ -w | --wait ] [ -l | --logfile <logfile> ]`.

`-c|--cluster`: Cluster environment.

`-w| --wait`: ecadm does not exit until all services have been started.

`-t| --temporary`: The state change is made temporary until next reboot.

stop
Enter `ecadm stop [ -h | --help ] [ -v | --verbose ] [ -c | --cluster ] [ -t | --temporary ] [ -w | --wait ] [ -l | --logfile <logfile> ]`.

`-c|--cluster`: Cluster environment.

`-w| --wait`: ecadm does not exit until all services have been stopped.

`-t| --temporary`: The state change is made temporary until next reboot.

status
Enter `ecadm status [ -h | --help ]`.

configure
Enter `ecadm configure [ -h | --help ] [ -f | --config <config-file>] [ -p | --proxy ] [ -P | --noproxy ] [ -v | --verbose ] [ -l | --logfile <logfile> ]`.

`-f| --config <config-file>`: Uses the contents of `<config-file>` to register the Proxy Controller with My Oracle Support.

`-p| --proxy`: By default, enables the local Proxy Controller after the Enterprise Controller is configured.

`-P| --noproxy`: The local control proxy is not enabled.

Note: Ensure that the file permission for the configuration file properties is set to 400 because it contains the Online Account user name and password. The configuration file must not be accessible to unauthorized users.

---

unconfigure
Enter `ecadm unconfigure [ -h | --help ] [ -v | --verbose ] [ -l | --logfile <logfile> ]`.

backup
Enter `ecadm backup [ -o | --output <backup-file> ] [ -t | --tag <tag> ] [ -d | --description <description> ] [ -r | --remotedb ] [ -c | --configdir <config-dir>] [ -T | --tempdir <temp-dir> ] [ -h | --help ] [ -v | --verbose ] [ -l | --logfile <logfile> ]`.

`-o | --output <backup-file>`: Stores the backup archive in tar format in `<backup-file>`. Do not specify the path inside the xvm install directories (`/opt/*xvm*`). Default: `/var/tmp/sat-backup-<date>-<time>.tar`

`-t | --tag <tag>`: Stores the string `<tag>` as a property of the backup archive which is displayed by restore operation when referencing the `<backup-file>`.

`-d | --description <description>`: Stores the string `<description>` as a descriptive property of the backup archive (the description is informational and it is displayed during restore operation).

`-r|--remotedb`: If Enterprise Controller uses a remote database, export the schema to a file on the database server. This option must be specified if the Enterprise Controller uses a remote database, otherwise data is not exported from the database.

`-c | --configdir <config-dir>`: `<config-dir>` is an alternative collection of backup modules when performing the backup. ecadm backup is modular in design and executes a set of backup tasks in the configuration directory. This option provides a means to use an alternate set of modules to produce a backup archive in a specialized way.

`-T | --tempdir <temp-dir>`: Uses `<temp-dir>` instead of the temporary directory in `/var/tmp` for intermediate storage needs during the backup. This temporary directory is required to hold a large quantity of data during the backup operation.

restore
Enter `ecadm restore -i | --input <backup-file> [ -c | --configdir <config-dir>] [ -r | --remotedb ] [ -d | --tempdir <temp-dir> ] [ -h | --help ] [ -v | --verbose ] [ -l | --logfile <logfile>] .`

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

`-r|--remotedb`: If EC uses a remote database, export the schema to a file on the database server. This option must be specified if the Enterprise Controller uses a remote database, otherwise data is not exported from the database.

`-c | --configdir <config-dir>`: `<config-dir>` is an alternative collection of restore modules when performing the backup. ecadm restore is modular in design and executes a set of restore tasks in the configuration directory. This option provides a means to use an alternate set of modules to restore a backup archive in a specialized way.

`-d | --tempdir <temp-dir>`: Uses `<temp-dir>` instead of the temporary directory in /var/tmp for intermediate storage needs during the restore. This temporary directory is required to hold a large quantity of data during the restore operation.

verify-db
Enter `ecadm verify-db [ -v | --verbose ]`.

change-db-password
Enter `ecadm change-db-password -p| --passwordfile <password-file> [ -v | --verbose ]`.

`-p| --password-file <password-file>`: Specifies the file containing the new password.

`-r| --as_read_only_user`: Specifies if the operation is done for a read only user. If this option is used, the password for the read only user is specified in the `<password file>`, and the read only user is the target of the change.

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 dabatase properties. The default location of db.properties file is /var/opt/sun/xvm/db.properties

-p| --propfile <dbpw.properties file>: Contains the passwords for the schema names in db.properties. The dbpw.properties file is found by default in /var/opt/sun/xvm/dbpw.properties

-d| --directory <directory to run in>: Uses the directory passed in as the working directory for the sqlplus session.

ha-status

Enter ecadm ha-status [-h | --help] [-v | --verbose] [-d | --display] [-l | --logfile <logfile>].

-d| --as_read_only_user: Displays full High Availability status info.

ha-configure-primary

Enter ecadm ha-configure-primary [-h | --help] [-v | --verbose] [-l | --logfile <logfile>].

ha-configure-standby

Enter ecadm ha-configure-standby [-h | --help] [-p | --credentialsfilename <credentials-file>] [-v | --verbose] [-l | --logfile <logfile>].

-p| --credentialsfilename<credentials-file>: Specifies the file containing the user name and password for privileged access. The first line of the file must contain the user name in this format: username=<user>. The second line of the file must contain the password in this format: password=<password>.

ha-modify-resource

Enter ecadm ha-modify-resource [-h | --help] [-p | --credentialsfilename <credentials-file>] [-v | --verbose] [-l | --logfile <logfile>].

-p| --credentialsfilename <credentials-file>: Specifies the file containing the user name and password for privileged access. The first line of the file must contain the user name in this format: username=<user>. The second line of the file must contain the password in this format: password=<password>.

ha-relocate

Enter ecadm ha-relocate [-h | --help] [-n | --node <standby node>] [-v | --verbose] [-l | --logfile <logfile>].

-n| --node <standby node>: Relocates to node in <standby node>.

ha-start

Enter ecadm ha-start [-h | --help] [-n | --node <standby node>] [-v | --verbose] [-l | --logfile <logfile>].

-n| --node <standby node>: Relocates to node in <standby node>.

ha-stop-no-relocate

Enter ecadm ha-stop-no-relocate [-h | --help] [-v | --verbose] [-l | --logfile <logfile>].

ha-unconfigure-primary
Enter `ecadm ha-unconfigure-primary [ -h | --help ] [ -v | --verbose ] [ -l | --logfile <logfile> ]`.

ha-unconfigure-standby
Enter `ecadm ha-unconfigure-standby [ -h | --help ] [ -n | --node <standby node>] [ -v | --verbose ] [ -l | --logfile <logfile>]`.

`-n| --node <standby node>`: Unconfigures the standby node when run from another cluster node. Use this option when the standby node is down.

Exit status

The exit status displays the status of the Enterprise Controller services. The status currently displays either offline or online to the standard output. The exit status displays one of the following codes:

0: Online

2: Offline (only for status subcommand)

1: Error occurred during processing

Configuring the Proxy Controller: proxyadm

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

Synopsis

Oracle Solaris OS

```
/opt/SUNWxvmoc/bin/proxyadm -V
/opt/SUNWxvmoc/bin/proxyadm [ -h | --help ]
/opt/SUNWxvmoc/bin/proxyadm subcommand [ options ]
```

Linux OS

```
/opt/sun/xvmoc/bin/proxyadm -V
/opt/sun/xvmoc/bin/proxyadm [ -h | --help ]
/opt/sun/xvmoc/bin/proxyadm subcommand [ options ]
```

Options

The `proxyadm` command supports the following options:

`-h| --help`: Displays the usage synopsis for proxyadm.

`-V`: Displays the version of Oracle Enterprise Manager Ops Center.

Subcommands

The `proxyadm` command includes the following subcommands:

start
Starts the Proxy Controller services running on the host.

stop
Stops the Proxy Controller services running on the host.

status
Displays the online or offline status of the Proxy Controller services to the standard output, and sets the exit status to reflect the Proxy Controller service state.

configure
Performs configuration tasks for the Proxy Controller services.

You can set the following classes of configuration information:

- Registering the Proxy Controller with the Enterprise Controller.
- Configuring the type of DHCP server that the Proxy Controller runs and the parameters for that DHCP server.

unconfigure
Performs the inverse operation of configuring the Proxy Controller. Deregisters and unconfigures the connection between the Proxy Controller and the Enterprise Controller it is associated with.

Subcommand options

The following common options are supported for all the subcommands:

`-h| --help`: Displays the usage synopsis for that subcommand.

`-v| --verbose`: Displays verbose error and informational messages.

start
Enter `proxyadm start [ -h | --help ] [ -v | --verbose ] [ -w | --wait ] [ -t | --temporary ] [ -l | --logfile <logfile> ].`

`-w| --wait`: proxyadm does not exit until all the services are started.

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

`-t| --temporary`: The state change is made temporary until next reboot.

stop
Enter `proxyadm stop [ -h | --help ] [ -v | --verbose ] [ -w | --wait ] [ -t | --temporary ] [ -l | --logfile <logfile> ].`

`-w| --wait`: proxyadm does not exit until all the services are stopped.

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

`-t| --temporary`: The state change is made temporary until next reboot.

status
Enter `proxyadm status [ -h |--help ].`

configure
Enter `proxyadm configure [-h | --help] [-v | --verbose] [-a | --proxy-ip] [-u | --user <user name>] [-p | --passwordfile] [-t | --tokenfile <password-file>] [-x | --proxy <host name>[:<port>]] [-U | --proxy-user <proxy user name>] [-P | --proxy-passwordfile <password-file>] [-a | --proxy-ip].`

`-u | --user <user name>`: Specifies the Enterprise Controller administrator user name.

`-p| --passwordfile <passwordfile>`: Specifies a filename containing the password for the Enterprise Controller administrator.

(Optional) -t| --tokenfile <autoregistration_tokenfile>: Specifies an autoregistration token stored in a file. This is used as an alternative for Enterprise Controller administrator user name and password.

(Optional) -x| --proxy <host name>[:<port>]: If an HTTPS proxy is required to reach the Enterprise Controller, specify the <host name> for that proxy. Specifying the IP port is optional. The default proxy port is 8080.

(Optional) -U | --proxy-user <proxy user name>: Use this option if a proxy requires a user name for authentication.

(Optional) -P | --proxy-passwordfile <password-file>: Uses the password in <password-file> for proxy authentication.

(Optional) -a | --proxy-ip: Explicitly enter the IP address of the control proxy.

> **Note:** The password file must be secured to prevent unauthorized users from examining the file. The file permission must be set to 400.

unconfigure

Enter proxyadm unconfigure [-h | --help] [-k| --keep].

-k|--keep: Keeps the local Proxy Controller database.

Exit status

The exit status displays the status of the proxy services. The states currently display either offline or online on the standard output. The exit status displays one of the following codes:

0: Online

2: Offline (only for status subcommand)

1: Error occurred during processing

Configuring the Agent Controller: agentadm

The agentadm command helps to manage the Oracle Enterprise Manager Ops Center agents such as registering the Agent Controller to the proxy and unconfiguring the agents.

Synopsis

Oracle Solaris OS

```
/opt/SUNWxvmoc/bin/agentadm
/opt/SUNWxvmoc/bin/agentadm [ -h | --help ]
/opt/SUNWxvmoc/bin/agentadm subcommand [ options ]
```

Linux OS

```
/opt/sun/xvmoc/bin/agentadm -V
/opt/sun/xvmoc/bin/agentadm [ -h | --help ]
/opt/sun/xvmoc/bin/agentadm subcommand [ options ]
```

Usage

```
agentadm [-V | --version ] [ -K | --property-keys <file>] [ -q | --quiet ]
[ -v | --verbose ] [ -f | --force ] [ -n | --norefresh ] [ -o |
--output-file ] [ -h | --help]

agentadm subcommand [ options ]
```

Options

The following common options are supported:

`-K| --property-keys <file>`: The properties filename for the subcommands.

`-V| --version`: Displays the version number of the Agent Controller software.

`-h| --help`: Displays the usage synopsis for all configuration steps supported by agentadm.

`-v| --verbose`: Display verbose error and informational messages. Use multiple occurrences of this option to increase the verbosity level.

`-q| --quiet`: Does not display anything and returns only the return code.

`-f| --force`: Ignores non critical errors during steps operations.

`-n| --norefresh`: Does not overwrite the existing operation.

`-o| --output-file`: Sends the output to the specified logfile.

Subcommands

The subcommands of agentadm are as follows:

start
Starts the Agent Controller services running on the host.

stop
Stops the Agent Controller services running on the host.

configure
Performs configuration tasks for the Agent Controller services.

unconfigure
Performs the inverse operation of configuring the Agent Controller.

usage
Equivalent to `[ -h | --help ]`

Subcommand options

start
Enter `agentadm start`.

stop
Enter `agentadm stop`.

configure
The configuration step consists of:

- sc-console registration of the agent to proxy.

- scn-agent cacao instance creation.
- uce-agent cacao instance creation.
- Registration of the agent's products to the proxy.

The registration of the agent to the proxy is as follows: `agentadm configure [ -u | --user <user name> ] [ -p | --passwordfile<password-file> ] [ -a | --agent-ip <IP address> ] [ -t | --token <tokenfilename> ] [ -x | --proxy <URI> ] [ -I | --non-interactive ] [ -k | --keep-connection ]`

`-u | --user <user name>`: The Online Account user name.

`-p | --passwordfile <passwordfile>`: Filename with the Online Account credentials.

`-a | --agent-ip <IP address>`: Specify the IP address to be used during registration.

`-t | --token <tokenfilename>`: Filename containing auto registration token.

`-x | --proxy <URI>`: URI of the proxy to be registered.

`-I | --non-interactive`: Launch sc-console in non-interactive mode (without -i). Default is interactive mode.

`-k | --keep-connection`: Do not re-register to proxy if the connection exists.

unconfigure
Enter `agentadm unconfigure`

Index

A

B

C

D

E

H

I

L

M

N

O

P

R

S

T

U

V

W